

MARTIN HUSOVEC

PRINCIPLES OF **THE DIGITAL SERVICES ACT**



OXFORD

Principles of the Digital Services Act

Principles of the Digital Services Act

MARTIN HUSOVEC

OXFORD
UNIVERSITY PRESS

OXFORD
UNIVERSITY PRESS

Great Clarendon Street, Oxford, OX2 6DP,
United Kingdom

Oxford University Press is a department of the University of Oxford.
It furthers the University's objective of excellence in research, scholarship,
and education by publishing worldwide. Oxford is a registered trade mark of
Oxford University Press in the UK and in certain other countries

© Martin Husovec 2024

The moral rights of the author have been asserted

This is an open access publication, available online and distributed under the
terms of a Creative Commons Attribution-Non Commercial-No Derivatives 4.0
International licence (CC BY-NC-ND 4.0), a copy of which is available at
<http://creativecommons.org/licenses/by-nc-nd/4.0/>.
Subject to this license, all rights are reserved.



Enquiries concerning reproduction outside the scope of this licence should be sent
to the Rights Department, Oxford University Press, at the address above.

Public sector information reproduced under Open Government Licence v3.0
(<http://www.nationalarchives.gov.uk/doc/open-government-licence/open-government-licence.htm>)

Published in the United States of America by Oxford University Press
198 Madison Avenue, New York, NY 10016, United States of America

British Library Cataloguing in Publication Data
Data available

Library of Congress Control Number: 2024936306

ISBN 978–0–19–288245–5

DOI: 10.1093/law-ocl/9780192882455.001.0001

Printed and bound by
CPI Group (UK) Ltd, Croydon, CR0 4YY

Foreword

‘We should write a book together about the DSA.’

In 2020, I already knew Martin too well to know that he was not joking. I had met him in 2014, when he was already an expert on intermediary liability and its impact on fundamental rights, and I had just taken up a new position in this fascinating area within the European Commission’s services. By 2020, we were already good friends. I had just been appointed Deputy Head of Unit in the service responsible for the E-Commerce Directive, and at that time focused on the preparations of the proposal for the Digital Services Act Package, including the Digital Services Act (DSA) and the Digital Markets Act. In this role, I led the legal work around the conception, negotiation, and, later, implementation of the DSA.

The DSA represents a huge milestone in the history of digital regulation in the European Union, and at the Commission we expected to set a global gold standard. Martin refers to the DSA in this book as the ‘EU Digital Rights Charter’. I had gathered so many insights, views, interpretations, and anecdotes about historical moments (at least for legal nerds) from my experience during the conception and negotiation process that I felt that there was just so much I could write about it.

In this context, writing a monograph about the DSA (and with one of the most authoritative experts in the area!) was not only an amazingly attractive idea, but also a project which I knew would be a very useful contribution to the practical implementation of this landmark piece of law.

As with any legal instrument, the legislative history is a key interpretative guidance of the ‘intention of the legislator’. Way too often in the European Commission, however, after successfully negotiating a piece of law, the negotiation team moves on to the next policy challenge. Unfortunately—and also too often—this happens even before there is a clear written record of the rationale behind this or that agreed text. This memory gap is something I am particularly motivated to avoid.

Leading the drafting and negotiation team gave me an incomparable opportunity to document and trace the what, the who, and the why (or why not) of each provision. Martin’s tempting offer to co-author a book would allow me to keep this record—to the extent that it was not confidential information—for the implementation stage.

As nicely as this idea fitted in my mind, I soon faced some difficulties. The first is that, apparently unlike Martin’s, my days have only 24 hours, and they were all already taken by the negotiations and busy implementation plans. The short application deadline made us work day and night on delegated and implementing acts, first designations of very large online platforms and very large online search engines, and building a strong DSA enforcement team in the Commission.

The second one is more important: as a European civil servant, I am proudly bound by high ethical standards; moreover, as a leading negotiator, I feel strongly about the policy choices made, which I could not easily distance myself from and criticise. Already with the first drafting exercises of the book, I noticed that I did not want to test the limits of these external and internal boundaries. Furthermore, an academic work like the one the reader has in her hands requires a much-needed critical perspective and open mind.

As a solution to this, we agreed that, in a series of interviews and memorable conversations in Brussels, Valencia, Alicante, and online, we would collect the history and the stories behind the negotiation of the DSA. Our lengthy discussions on the legal choices, legal techniques, or the relationship between the DSA and other Union law instruments or national laws are clearly the inspiration of some chapters of this book. I am very proud of having contributed to it, as much as Martin, as other leading scholars, influenced policymakers' choices with their publications and research.

Martin masters this critical academic role and enjoys a distant and independent position from rule-makers that I could not offer. In this work, Martin keeps a critical approach, but he also recognises the DSA's genuine effort to find that difficult 'sweet spot' in balancing users' rights and the providers' accountability in the society they influence and shape.

I would like to stress three particular elements of this book that I am particularly keen on.

First of all, the exemption of liability, or 'safe harbours', is a central element of both the DSA and this book. Indeed, the DSA 'renovates the democratic mandate of the safe harbours'. The rules established under the E-Commerce Directive were often accused of being 'old' and 'unfit' for the current internet. A clear case of legal ageism. Now, these rules are anchored in the DSA, almost unchanged, and stronger than ever. Fun fact: Article 8 ('no general monitoring obligations') is the only article, out of 74 in the Commission proposal, that was not modified at all during the legislative process. Co-legislators agreed with the Commission that this rule is a cornerstone of the internet regulation. Martin dedicates to these rules the importance that they deserve, and explains very clearly how the liability regime under the DSA is closely bound to, but independent from, a full set of due diligence obligations.

Secondly, this work represents the first deep and complete overview of the backbone of the DSA: Chapter III on 'Due diligence obligations'. Martin successfully analyses the long list of due diligence obligations imposed on service providers, in particular platforms, spread alongside around 30 articles. He categorises them under three logical clusters: obligations on 'fair process', 'fair design', and 'transparency and oversight'. He also recognises that the focus of the due diligence obligations is on procedures—not on the content itself. The DSA does not determine what is illegal, or what can or cannot be accepted by platforms. It does not provide any administrative oversight of content.

Thirdly, this book acknowledges a point of key importance to the policy objective that justifies the legal intervention: the single market. Martin dedicates an important part of this book to explain the harmonisation needs and effects of the DSA. During

the making of the DSA, the Commission designated respect for the single market as a ‘red line’ that could not be crossed. In a way, this was embodied by the country-of-origin principle that reflects mutual trust: if a provider decides to establish themselves in Europe, it can choose where—and it will be subject to compliance requirements in that Member State only. National laws that now overlap with, or even contradict, the DSA will need to be repealed. Legal fragmentation is not only bad for business, it also harms legal certainty, as the internet user does not know which rights he or she has. The single market element is also central in the main novelty of the DSA: the centralisation (or mutualisation) of its enforcement around the Commission and the national regulators. The country of establishment will still be the main Member State responsible for ensuring compliance, together with the Commission.

But there is also room for further assessment: with this book being a frontrunner in presenting the DSA to the general practitioner by the time it enters into application, it cannot anticipate whether the enforcement toolbox (very much inspired by competition rules) will work in practice. Time will tell whether the DSA will tame the very large online platforms’ societal role. Time will tell the tangible results that the risk-based approach of the DSA will bring. Secondary legislation, in particular in the field of audits, access to data for vetted researchers, or the collection of the supervisory fee, will need to be analysed. The vast array of information that the DSA will facilitate—from the database of statements of reasons to the detailed transparency reports or the ad repositories—will allow for future judgement on whether the DSA is a success or not.

Maybe, one day, Martin and I should write that book together?

Irene Roche Laguna
Visiting Professor, College of Europe
Head of Unit, European Commission
December 2023

Preface

Dear readers,

In the summer of 2020, before the first draft of the Digital Service Act (DSA) was even proposed, I first thought about writing a book about the DSA for a brief moment. Within hours, I killed the thought. What a terrible idea! The legislation is going to be too big and complex. It cannot be done by a single person.

Several months later, I started writing the book. The sudden change of heart was entirely the fault of my friend, Irene Roche Laguna, who assured me that we could do it together. Irene has been at the forefront of the E-Commerce Directive liability debates for years from her office at the European Commission, and now she was stewarding the DSA proposal through the legislative process. Irene's willingness to join forces made all the difference for my decision to start. We embarked on the project together, discussing interpretations as the DSA was passing legislative milestones.

While I wrote, the DSA was constantly changing. We exchanged ideas, comments, and interpretations. Our efforts became more focused once the law was published and the hours-long debates continued. However, Irene eventually had to step down from the project several months into this joint effort. I had to run the rest of the marathon without my sparring partner. At this point, I was too deep in writing to abandon it. I had too many ideas that I wanted to share with the world. Thus, while the final project is a monograph, Irene's important role must be acknowledged. In many ways, she paved the way for the project. You will see that I sometimes cite from our discussions to credit her ideas directly. I certainly do not exaggerate when I say that this book would not have been possible without her.

Being an academic, I eventually slightly changed the project's soul. Initially, the book was going to be a deep, all-encompassing commentary informed by academic debates. The main idea was to give readers a useful text before the DSA enters into force. Ultimately, the deep commentary was cut in scope to give space to something else: ideas about what to do next. I realised that the DSA is packed with incredible tools that might do a lot of good, especially to protect our liberal democracies. However, exactly because we are at a very fragile moment in history, I felt it necessary to caution against its abuse. I decided to ground the DSA by a set of principles that could guide its application going forward. You can judge the result.

As with any big book, this one too required many personal sacrifices. It would not have been possible without the support of my closest family members, who tolerated my lonely days with my tablet, laptop, and books. Their love and support always gave me the energy to continue. I also owe thanks to many other people whom I interviewed for the book, or who read the earlier versions of the manuscript and shared their comments. You know who you are. You are incredible. My deep gratitude also extends to my

two talented research assistants—Cham Mikhaeil and Genevieve Heng—who helped with editing and visuals. They did an incredible job improving my initial text and sketches. Finally, I also want to thank my employer, the London School of Economics, for being such a great environment that supports free creativity. In times when academics around Europe are increasingly asked to subject their academic creativity to the whims of almighty funders, the LSE Law School's approach is a breath of fresh air.

I hope that the book will serve as a resource for academics, civil society, companies, and officials. I would not have written it if I was not convinced that the DSA can do good. However, to achieve it, a lot of work must be put into its application and understanding. In 2023, we are still only at the very start.

If you find something useful in this book, take it and run with it. That very fact already makes me happy. If you have any observations, criticism, or suggestions for improvement, just email me. For the latest developments, visit my dedicated website at www.husovec.eu/dsa.

Happy reading!

Martin
Alicante, Košice, London
December 2023

Contents

<i>List of Figures</i>	xv
<i>List of Tables</i>	xvii
<i>List of Abbreviations</i>	xix

PART I INTRODUCTION

1	Introduction: Taming the Powers	3
1.1	Introduction	3
1.2	European Regulation of Digital Services	4
1.3	Private and State Power	9
1.4	Delegated Enforcement	12
1.5	Using the Right Metaphors and Principles	14
1.6	Outline of the Book	17
2	Overview of the DSA	19
2.1	Introduction	19
2.2	Scope and Institutions	20
2.3	Liability Exemptions	21
2.4	Due Diligence Obligations	22
2.5	Co-regulation and Enforcement	30
2.6	The Concept of Illegal Content	31
2.7	Conclusion	31
3	Human Rights	33
3.1	Introduction	33
3.2	Strasbourg Jurisprudence	35
3.3	Luxembourg Jurisprudence	47
3.4	Institutional Blind Spots	53

PART II LIABILITY

4	Introduction to Liability Framework	57
4.1	Introduction	57
4.2	History of the ECD	61
4.3	Two Generations of Rules	63
5	Prohibition of General Monitoring Obligations	67
5.1	Introduction	67
5.2	Scope of the GMOP	69
5.3	Origins of the GMOP: From the ECD to the DSA	81
5.4	The GMOP as a Balancing Tool	83
5.5	The GMOP as a Harmonisation Tool	87
5.6	The GMOP vs the Member States	90

6	Liability Exemptions: General Requirements	93
6.1	Introduction	93
6.2	General Requirements	95
6.3	Emerging Difficult General Issues	116
7	Liability Exemptions: Specific Services	123
7.1	Introduction	123
7.2	Mere Conduits	123
7.3	Caching	126
7.4	Hosting	128
7.5	Search Engines	136
7.6	Liability Exemptions Overlaps and Voids	143
8	Injunctions and Orders	145
8.1	Introduction	145
8.2	Scope of Permitted Injunctions	146
8.3	DSA Rules on Orders Issued by Authorities	151
8.4	Content Orders (Article 9)	153
8.5	Information Orders (Article 10)	156
8.6	Conclusion	157
PART III ACCOUNTABILITY		
9	Introduction to Accountability Framework	161
9.1	The EU Landscape of Digital Services	161
9.2	Determining Regulatory Layers	167
9.3	Judicial Review of VLOP/VLOSE Designation Decisions	178
9.4	Separation of Liability and Accountability	181
10	Content Moderation: Outline	185
10.1	Evolution of Practices	185
10.2	Regulation as Division of Powers	188
10.3	Rule-Setting and Its Legitimacy	189
10.4	User-Empowerment and Customisation	192
10.5	Due Process and Its Criticisms	193
11	Fair Moderation Process	202
11.1	The DSA's Approach to Content Moderation	202
11.2	Step 1: Notice Handling (Article 16)	209
11.3	Step 2: Statement of Reasons (Article 17)	221
11.4	Step 3: Internal Appeals (Article 20)	229
11.5	Step 4: External Appeals (Article 21)	234
11.6	Conclusion	248
12	Fair Content Rules	249
12.1	Introduction	249
12.2	General Explainability of Content Moderation (Article 14(1))	249
12.3	Fairness of Content Rules (Article 14(4))	253
12.4	Safeguards Against Abuse by Users and Notifiers (Article 23)	265
12.5	Conclusions	268

13	Risk-Based Approach to Digital Services	270
13.1	Regulatory Moment	270
13.2	A Risk-Based Approach	274
13.3	The Regulator's Powers	276
13.4	Precautionary Principle and Rule of Law	279
13.5	The Bigger Cycle of Risk Mitigation	282
14	Fair Design Practices	285
14.1	Introduction	285
14.2	Design of Recommender Systems	288
14.3	Design of Advertising	296
14.4	Design of User Experience	305
14.5	Business-to-Consumer Marketplaces	313
14.6	Conclusion	314
15	General Risk Management	316
15.1	Introduction	316
15.2	Relevant Risks	318
15.3	Risk Management Cycle	322
15.4	A Theory of the DSA's Limited Risk Management	333
16	Transparency	347
16.1	Introduction	347
16.2	Access to Data of VLOPs/VLOSEs (Article 40)	349
16.3	Transparency Reports	359
16.4	Conclusion	367

PART IV THE DSA AS A POLICY TOOL

17	The DSA as a Cornerstone of the EU Single Market	371
17.1	Introduction	371
17.2	Five Main Pillars of the Digital Single Market	372
17.3	The Period 1995–2022	374
17.4	National Experimentation Post-DSA	376
17.5	Pre-emption by the DSA	380
17.6	Conclusion	389
18	The DSA as a Digital Rights Charter	391
18.1	Introduction	391
18.2	Piecing Together the Big Picture	392
18.3	Copyright Law	396
18.4	Data Protection Law	401
18.5	Audiovisual Media Regulation	407
18.6	Platform to Business Regulation	410
18.7	Terrorist Content Regulation	413
18.8	Conclusion and Outlook	415
19	The DSA as a Mixed Enforcement System	417
19.1	Introduction	417
19.2	Public Enforcement	420

19.3 Private Enforcement	428
19.4 Conclusion	442
20 The DSA as a Co-regulatory System	443
20.1 Introduction	443
20.2 Codes of Conduct as European Benchmarks (Articles 45–48)	445
20.3 A Theory of the DSA’s Regulatory Design	456
20.4 DSA’s Global Spillover Effects	459
20.5 Conclusion	461

PART V OUTLOOK

21 Principles	465
21.1 Introduction	465
21.2 Statutory Design Principles	470
21.3 Interpretative Principles	473
21.4 Conclusion	476
<i>Index</i>	479

Figures

1.1 Redistribution of power	12
2.1 The DSA's regulatory coverage	22
2.2 The DSA's layered structure	23
3.1 ECtHR intermediary liability constraints	47
4.1 Timeline of intermediary liability rules	61
4.2 The internet tech stack	65
6.1 Functionality and its primacy	96
6.2 Neutrality of services	107
9.1 Scope of digital services: online marketplace	172
9.2 Scope of digital services: streaming service	173
10.1 Redistribution of power	188
11.1 Content moderation rules	203
11.2 Notice and takedown choreography	212
13.1 The DSA framework in one picture	273
13.2 The DSA's bigger cycle of risk mitigation	283
14.1 Parts of services	287
14.2 Redistribution of power	297
15.1 Scope of risk mitigation and risk assessment	326
15.2 Risk distribution under risk management	344
17.1 The DSA's regulatory coverage	381
18.1 The DSA as a Digital Rights Charter	392
20.1 The DSA's regulatory architecture	458
21.1 DSA Principles	471

Tables

5.1	GMOP in the ECD and DSA	81
5.2	Recital 47 ECD vs. Recital 30 DSA	82
5.3	Keys risks for general monitoring	84
6.1	Situations leading to the loss of neutrality	111
6.2	Legal concepts and their consequences	122
8.1	EU law limits on orders issued by authorities	150
9.1	Designations as VLOPs and VLOSEs	162
9.2	Runners-up online platform services	163
9.3	Infrastructure services	166
9.4	Overview of due diligence obligations	184
11.1	Types of content restrictions	223
11.2	Statement of reasons requirements	226
11.3	Content moderation steps	231
11.4	List of VLOPs/VLOSEs	237
13.1	DSA's elements according to regulatory approach	272
14.1	Applicability of Article 25 DSA	309
15.1	General risk management: overview	319
15.2	Limits of the general risk management approach	340
16.1	Types of data access	351
16.2	Universal transparency reports (Article 15 DSA)	360
16.3	Examples of transparency reports	362
16.4	Platform transparency reports	364
17.1	Limits on regulation of digital services	381
19.1	Competence for national regulators	422
19.2	Other enforcement actors	441

Abbreviations

ADR	alternative dispute resolution
AG	Advocate General
API	Application programming interface
AVMSD	Audiovisual Media Services Directive
BEUC	European Consumer Organisation
Board	European Board for Digital Services
CDA	Communications Decency Act
CDN	Content Delivery Network
CDSM Directive	Copyright in the Digital Single Market Directive
CFR	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
COO	Country of origin
DG CONNECT	Directorate-General for Communications Networks, Content and Technology
DMA	Digital Markets Act
DMCA	Digital Millennium Copyright Act
DNS	Domain Name System
DPI	Deep Packet Inspection
DSA	Digital Services Act
DSC	digital services coordinator
DSC-COO	Digital Service Coordinator of the Country of the establishment of the provider
DSM	Digital Single Market
ECD	E-Commerce Directive
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EU	European Union
FRA	European Agency for Fundamental Rights
GDPR	General Data Protection Regulation
GMOP	Prohibition on General Monitoring
ICANN	The Internet Corporation for Assigned Names and Numbers
InfoSoc Directive	Information Society Directive
IP	Internet Protocol
NGO	non-governmental organisation
OCSSP	online content sharing service providers
ODS	Out-of-Court Dispute Settlement
P2BR	Platform-to-Business Regulation
RSS	Really Simple Syndication
SDOs	Standard Developing Organisations
TCR	Terrorist Content Regulation

XX ABBREVIATIONS

TFEU	Treaty on the Functioning of the European Union
ToS	Terms of Service
UCPD	Unfair Commercial Practices Directive
UDRP	Uniform Domain-Name Dispute-Resolution Policy
UGC	User-generated content
UK	United Kingdom
US	United States
VLOP	very large online platforms
VLOSE	very large online search engines
VPN	Virtual Private Network

PART I
INTRODUCTION

1

Introduction: Taming the Powers

1.1 Introduction	3	1.4 Delegated Enforcement	12
1.2 European Regulation of Digital Services	4	1.5 Using the Right Metaphors and Principles	14
1.3 Private and State Power	9	1.6 Outline of the Book	17

1.1 Introduction

The internet is a technology that continues to change humanity as only a few others have done before. It has tremendously enhanced our capabilities and improved our everyday lives. It plays to our special skill as a species—our ability to cooperate.¹ The speed and scale of communication in the network is the key ingredient. The permissionless dimension of the ecosystem—the fact that there are no editors—expands the grandeur of its possibilities. The ability of anyone to join the network, express themselves, and find an audience taps deep into human potential.

Today, an absolute majority of the top visited websites rely on user-generated content.² There is no doubt that decentralised non-editorial content continues to rule the internet. People cannot resist connecting with other people by sharing information. Aristotle was convinced that humans are social animals.³ The modern social sciences argue that imitation is the glue that makes us inherently social.⁴ The internet compounds the opportunity for such imitation because it largely reduces restrictions of time and space.

But the abundance of information produced by other humans, coupled with increasingly capable machines that can manufacture impressions of everything from conversations to facts, pushes us to rethink how to separate the wheat from the chaff. People are unsure what to trust.

¹ Yuval N Harari, *Sapiens: A Brief History of Humankind* (1st US edn, Harper 2015).

² 'List of Most Visited Websites', *Wikipedia* (2023) <https://en.wikipedia.org/w/index.php?title=List_of_most_visited_websites&oldid=1168840226> accessed 8 August 2023.

³ Aristotle, *Politics* (Benjamin Jowett tr, Batoche Books 1999) 5.

⁴ Ap Dijksterhuis, 'Why We Are Social Animals: The High Road to Imitation as Social Glue' in Susan Hurley and Nick Chater (eds) *Perspectives on Imitation From Neuroscience to Social Science – Volume 2: Imitation, Human Development, and Culture* (MIT Press 2005) 207 ff.

Moreover, the crowd-like characteristics of the internet invite abuse. As argued by Gustave Le Bon, even a cultivated individual can become a barbarian in a crowd.⁵ People online feel similarly unaccountable and less disposed to check themselves, because ‘a crowd being anonymous, and in consequence irresponsible, the sentiment of responsibility which always controls individuals disappears entirely.’⁶ People can be swayed by others to do things which they would otherwise never contemplate. Online abuse then undermines the trust of victims and onlookers that they can safely express themselves and participate.

Fundamentally, the common question raised by many emerging social problems online, ranging from hate speech and disinformation to consumer protection and cyberbullying, is whether an information ecosystem that lacks editors can recreate trust by other means; for example, trust in safety from illegal content, and trust in quality of legal content. In this book, I argue that laws and regulations have an important role in both preserving the existing shape of the internet and helping to find solutions to problems associated with distrust. The DSA is an example of a law that tries to recreate a trustworthy digital environment by suppressing illegal modes of expression and promoting decentralised trust-enhancing institutions.

1.2 European Regulation of Digital Services

The first European comprehensive internet-related law, the E-Commerce Directive (ECD), was drafted at a time when the internet was used by few. In 1998, long before the dot-com bubble had burst, Paul Krugman provocatively speculated about the prospects of the internet on the pages of the *Red Herring* magazine:

The growth of the Internet will slow drastically, as the flaw in ‘Metcalfe’s law’—which states that the number of potential connections in a network is proportional to the square of the number of participants—becomes apparent: most people have nothing to say to each other! By 2005 or so, it will become clear that the Internet’s impact on the economy has been no greater than the fax machine’s.⁷

While Krugman was being intentionally provocative,⁸ his quotation did capture the sentiment of some people in the industry, that the internet was simply the latest hype, or that people will not transact with strangers. When Pierre Omidyar started eBay in

⁵ Gustave Le Bon, *The Crowd* (first published 1895, T Fisher Unwin Ltd tr, Standard Ebooks 2022) <<https://standardebooks.org/ebooks/gustave-le-bon/the-crowd/t-fisher-unwin-ltd/text/single-page>> accessed 10 August 2023.

⁶ *ibid.*

⁷ Paul Krugman, ‘Why Most Economists’ Predictions Are Wrong’ *Red Herring* (10 June 1998) <<https://web.archive.org/web/19980610100009/https://www.redherring.com/mag/issue55/economics.html>> accessed 8 August 2023.

⁸ Jay Yarow, ‘Paul Krugman Responds To All The People Throwing Around His Old Internet Quote’ *Business Insider* (30 December 2013) <<https://www.businessinsider.com/paul-krugman-responds-to-internet-quote-2013-12>> accessed 8 August 2023.

1995, everyone told him that strangers will not trade with strangers online.⁹ What the public did not always appreciate at the time was the fact that digital platforms were to become the hitherto missing means that would enable people anywhere around the world to start trusting complete strangers.¹⁰

It is partly the trust-enhancing quality of their services that catapulted platforms to the top of our stock markets. Before 2005, the top five technology companies by market capitalisation were hardware and software companies—Microsoft, Intel, IBM, Cisco, and Oracle. The true internet firms started entering the top five after 2005—Google (2005), Apple (2008), Amazon (2013), Alibaba (2014), and Facebook (2015).¹¹

While by the late 1990s, many people *knew* what the internet was, not everyone *used* it. In his speech on 10 October 1996, former US President Bill Clinton joked to the crowd at the Knoxville Auditorium Coliseum in Texas, '[w]hen I took office [in January of 1993], only high energy physicists had ever heard of what is called the Worldwide Web ... Now even my cat has its own Web page.'¹² The number of actual internet users at the time was less than 1% worldwide and 16% in the US.¹³

Even by 2000, only about half of the US population was using the internet. In Europe, the situation was even less developed. While in countries like the Netherlands, almost every second person used the internet at the end of the millennium, in Germany, it was only every third, in Spain every seventh, and in Slovakia every tenth person.¹⁴ Twenty years later, nine out of ten people use the internet in all these countries. The worldwide usage is around 69%.¹⁵

The internet legislation developed in the European Union (EU) and the United States (US) between 1996 and 2000 was written at a time when less than 5% of the world's population was online.¹⁶ The EU Member States had no local champions or articulated economic interests. Social problems were only starting to emerge. The industry to lobby against or for regulation, with the notable exception of the content and telecommunications industries, was largely missing.

Section 230 of the US Communications Decency Act (CDA), section 512 of the US Digital Millennium Copyright Act (DMCA), and section 4 of the EU ECD¹⁷ can be

⁹ Adam Cohen, 'Meanwhile: Pierre Omidyar's perfect store' *New York Times* (8 September 2005) <<http://www.nytimes.com/2005/09/07/opinion/07iht-edcohen.html>> accessed 21 September 2023.

¹⁰ For the discussion of the trust mechanisms, Mitchell Watt and Hubert Wu, 'Trust mechanisms and online platforms: A regulatory response' (2018) M-RCBG Associate Working Paper Series No 97 <https://www.hks.harvard.edu/sites/default/files/centers/mrcbg/files/97_final.pdf> accessed 24 September 2023.

¹¹ See a nice visualisation in Visual Capitalist, 'How the Biggest Tech Companies Have Changed in Size Over 23 Years' (18 March 2019) <<https://www.youtube.com/watch?v=RSuloaATQRA>> accessed 8 August 2023.

¹² Bill Clinton and Al Gore, 'Remarks by the President and the Vice President to the People of Knoxville on Internet for Schools' (Speech at Knoxville Auditorium Coliseum, Knoxville, Tennessee, 10 October 1996) <<https://govinfo.library.unt.edu/npr/library/speeches/101096.html>> accessed 8 August 2023.

¹³ The World Bank, 'Individuals Using the Internet (% of Population)—United States (1990–2021)' (World Bank Open Data) <<https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=US>> accessed 8 August 2023.

¹⁴ The World Bank, 'Individuals Using the Internet (% of Population) (1990–2021)' (World Bank Open Data) <<https://data.worldbank.org/>> accessed 8 August 2023.

¹⁵ Internet World Stats, 'Internet Growth Statistics 1995 to 2023—the Global Village Online' <<https://www.internetworldstats.com/emarketing.htm>> accessed 8 August 2023.

¹⁶ *ibid.*

¹⁷ Martin Husovec, 'Rising Above Liability: The Digital Services Act As a Blueprint for the Second Generation of Global Internet Rules' [2023] *Berkeley Technology Law Journal* (forthcoming).

labelled as the first generation of rules for the internet.¹⁸ The true boldness of the ECD was its horizontal regime—a single rulebook applicable across the entire legal system, even more so than section 230 of the US CDA. This horizontal nature, combined with the concept of liability exemptions and supported by the economic heft of the EU and the US, led to the export of the conditional liability model around the world.¹⁹

The European adaptation of the DMCA system of liability exemptions is to a large extent the product of the desire to pre-emptively coordinate regulation of the internet by the Member States. The European Commission's unit working on the ECD had previously dealt with many other areas where the change was difficult because various differing interests were already deeply entrenched, and stakeholders were vocal about defending the status quo in their Member States. The internet offered a unique possibility to act quickly to control future hindrances to the internal market. Thus, the ECD was drafted as an enabling instrument 'to encourage the vigorous growth of electronic commerce in Europe'²⁰ and reap its benefits, by avoiding regulatory barriers at the national level.²¹ The main impetus was thus to regulate the Member States, not the technology firms.

This explains why so much early legislation concerned regulatory coordination—the provisions were simply directing Member States to notify national rules, to not be stricter than national rules in the provider's state of establishment, to not impose liability on some services in some cases, and to facilitate national injunctions but not allow them to go too far.²² It also explains why all rules were horizontal. Information about specific concerns arising from the Internet did not exist yet, so the EU only tried to coordinate and learn from the national regulatory experiments as they arose.

It is worth noting that the European rules were born out of a surprisingly geographically broad political consensus. The Bonn Declaration on 'Global Information Networks' that culminated in European regulation brought together the Member States of the European Communities and the European Economic Area, then-candidate countries from Central, Eastern, and Southern Europe, and representations from the US, Canada, Japan, and Russia.²³ Thus, in the very early days, the countries were really trying to achieve convergence of rules.

The DSA, as a second generation of internet rules, has been prepared in a different environment than the ECD. Twenty years later, some of the digital tech companies are

¹⁸ For a broader argument, *ibid.*

¹⁹ *ibid.*

²⁰ Commission, 'A European Initiative in Electronic Commerce' (Communication) COM (97) 157 final.

²¹ In *ibid* 13, the Commission argued: 'The development of divergent legislative approaches is not only ineffective given the transfrontier nature of electronic commerce but also risks fragmenting the Single Market and thus inhibiting the development of electronic commerce in Europe.' Twenty-three years later, Rec 2 of the DSA reads: 'Member States are increasingly introducing, or are considering introducing, national laws on the matters covered by this Regulation ... Those diverging national laws negatively affect the internal market, which, pursuant to Article 26 of the Treaty, comprises an area without internal frontiers in which the free movement of goods and services and freedom of establishment are ensured, taking into account the inherently cross-border nature of the internet, which is generally used to provide those services.'

²² Ch 17 (notification and country-of-origin principle), chs 6–7 (liability exemptions), and ch 5 (the prohibition of general monitoring obligations) of this book.

²³ European Ministerial Conference, 'Global Information Networks: Realising the Potential' (6 July 1997) <http://web.mclink.it/MC8216/netmark/attach/bonn_en.htm> accessed 5 August 2023.

the richest companies in the world. Digital services are everywhere. They continue to stir countless new controversies and disrupt or even wipe out older businesses. They are at the centre of political scandals, ranging from hate speech distribution to election manipulation. Countries increasingly regulate them as they see fit.

The DSA combines prescriptive and open-ended regulation. It intervenes more prescriptively where problems have already crystallised and less prescriptively where too little is known about the cause and effect, and new practices continue to emerge. For instance, it intervenes *prescriptively* to improve due process online because it is informed by two decades of content moderation failures. It builds on top of some limited experimentation by the Member States and the industry, but also on the insight that self-regulation cannot guarantee the appropriate solution—a conclusion that not everyone will obviously accept even now, though the past 20 years have given us some evidence of its credibility. But it intervenes less prescriptively where the evidence is thinner or the industry practices are too much in flux, such as on the question of amplification through recommender systems, advertising, and the overall design of services.

The overall message of the DSA, especially for Big Tech, is clear. Facebook’s ‘move fast and break things’ wrongly prioritises innovation over people. Google’s ‘Don’t be Evil’ is insufficient to protect people from digital risks. The DSA asks designers of bigger services to seriously think about people and their rights upfront, and it appoints regulators to chair that discussion. This is not antithetical to start-up culture and encouragement of innovation because the seriousness of obligations grows with the popularity of the service. No one expects scrappy garage start-ups to immediately start thinking about their commitments to humanity. However, in tandem with valuation milestones, the leadership of companies is asked to prepare for regulatory milestones—the moment when the company starts employing over 50 employees, earning over €10 million, or serving 45 million Europeans. The bigger the operation, the more accountable to the public it is.

Despite the focus on the risks, the DSA’s rules are as much about scaling of businesses. The rules are designed with the logic of the EU single market in mind. Harmonisation improves future market entry, even if it puts some regulatory milestones in place. Moreover, many small businesses are built on top of large digital services. The EU is legislating for their benefit because the joint action of Member States is likely to have more impact than the sum of the individual interventions by all states. The DSA rules often try to build the EU’s single market *and* protect people at once. The two goals inform the instrument equally.

Market concentration is another important backdrop for the EU regulation of digital services. While the DSA does not directly address the economic power of companies, it is adopted in tandem with the Digital Markets Act (DMA)²⁴ which regulates some of the same digital services.

²⁴ European Parliament and Council Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 [2022] OJ L265/1 (Digital Markets Act (DMA))

The two acts regulate different sides of the externalities imposed by some of the same digital services. One could say that the DSA deals with the micro-level fairness of how providers treat their users, including how safe they are from various risks. The DMA, in contrast, deals with fairness on the macro-level—that is, how providers of the core digital services use their economic power to reduce the contestability of their positions going forward.²⁵ The DMA's focus is mostly on self-preferencing, tying, bundling, enabling data portability, and interoperability. In some cases, these two types of fairness rules overlap. For instance, the DSA requires fair content moderation rules and the DMA fair service-termination rules²⁶ and fair access;²⁷ both demand dispute settlement mechanisms,²⁸ and regulate parts of the recommender engines.²⁹

The DSA and DMA both take the approach of asymmetric regulation where 'bigness' attracts more responsibility.³⁰ If a platform or a search engine is designated as a gatekeeper under the DMA, it is very likely that it will also be designated as one of the DSA's very large online platforms or very large search engines. However, the DMA is narrower in scope: from the outset, it is likely to apply to fewer companies than the DSA because it applies exclusively to the largest gatekeepers. Its thresholds also include the extent of economic market power.³¹

The regulatory goal of the DMA is that macro-fairness will help to improve the competitiveness of services and thus eventually, through competition, improve the quality of the user experience—micro-fairness—for individuals. For instance, interoperability can allow better competition in user experiences, and push providers to improve trust and safety. The DMA thus aims to reinforce the goals of the DSA, in particular its emphasis on user's choice.

The history of regulation of the internet is a great case study for Collingridge's dilemma,³² which posits that '[w]hen change is easy, the need for it cannot be foreseen; when the need for change is apparent, change has become expensive, difficult, and time-consuming.'³³ Thus, the earlier you regulate, the less you know about what the problems are, but the more you can control the technology, and vice versa. As the technology matures, more information about it becomes available; however, change becomes more difficult due to the entrenchment of power of various players. Information about technology's pros and cons and our ability to intervene against them are inversely

²⁵ Pierre Larouche and Alexandre de Streel, 'The European Digital Markets Act: A Revolution Grounded on Traditions' (2021) 12(7) *Journal of European Competition Law & Practice* 542.

²⁶ DMA, art 6(13).

²⁷ DMA, art 5(12).

²⁸ DMA, art 6(12).

²⁹ DMA, art 6(5).

³⁰ Tim Wu, *The Curse of Bigness: Antitrust in the New Gilded Age* (Columbia Global Reports, 2018); Vestager's motto was 'great power comes with great responsibility' (like Spiderman). See for instance Margrethe Vestager, 'Shared Objectives for Framing the Tech Economy' (Speech at the Riesenfeld Award ceremony, Berkeley, California, 22 February 2022) <https://ec.europa.eu/commission/presscorner/detail/en/speech_22_8025> accessed 9 August 2023.

³¹ DMA, art 1(a) and 1(c).

³² David Collingridge, *The Social Control of Technology* (St Martin's Press 1980).

³³ *ibid* 11.

related. The DSA and the DMA come late in the regulation cycle. Inevitably, they will struggle more to reshape a system that has evolved over two decades.

1.3 Private and State Power

The DSA and DMA share a common foundational principle that the state should constrain private power for the sake of individual freedom. Accordingly, both are arguably predicated on the ordoliberal tradition. This has been acknowledged for DMA³⁴ but is less often stressed for the DSA.³⁵

Ordoliberals like Eucken objected to the laissez-faire liberalism of the 19th century due to its inability to thwart anti-competitive practices.³⁶ Eucken warned against state and private power alike.³⁷ He emphasised that private power is an important threat to individual freedom and must be kept in check—ideally through market competition. Private power, if not disciplined by competitive pressures, can lead to dependency and lack of individual freedom. Individual freedom is ‘not just a doctrine, but the only possible form of human existence.’³⁸ Any system must be measured against its ability to assure it.³⁹

The DSA’s focus on abuses of power by digital services against individuals is best explained as state power stepping in to assure the minimum ‘rules of the game’ in situations where competitive pressure fails to protect, or even endangers, fundamental rights and civil liberties. It is by no means a substitute for competition.

The example of app stores is quite illustrative. App stores are an important lever for content moderation. By imposing basic rules on their apps, they de facto regulate content moderation practices on other services. Some apps that have tried to offer unmoderated experiences, such as Parler, a social network, were temporarily removed from Apple’s app store due to their failure to take ‘adequate measures to address the proliferation’ of threats of violence and illegal activity.⁴⁰ Because of Apple’s market power, Parler could not afford to ignore its requests. In softening the economic grip of big app stores on the distribution of apps, the DMA weakens this power to regulate. This means that individual app providers will regain some of the control from the app stores designated as gatekeepers. This is where the DSA’s standards become key.

³⁴ Manuel Wörsdörfer, ‘The Digital Markets Act and E.U. Competition Policy: A Critical Ordoliberal Evaluation’ (2023) 22 *Philosophy of Management* 149.

³⁵ An exception in this regard is a recent article by Benjamin Farrand, ‘The ordoliberal internet? Continuity and change in the EU’s approach to the governance of cyberspace’ (2023) 2(1) *European Law Open* 106.

³⁶ Daniel Nientiedt and Ekkehard A Köhler, ‘Liberalism and Democracy—a Comparative Reading of Eucken and Hayek’ (2016) 40(6) *Cambridge Journal of Economics* 1743, 1744.

³⁷ Walter Eucken, *Grundsätze der Wirtschaftspolitik* (K Paul Hensel and Edith Eucken eds, 7th edn, Mohr Siebeck 2004) 176–77; Wörsdörfer (n 34) 157.

³⁸ *ibid* 176.

³⁹ Nientiedt and Köhler (n 36) 1744.

⁴⁰ Kim Lyons and Jay Peters, ‘Apple Removes Parler from the App Store’ *The Verge* (10 January 2021) <<https://www.theverge.com/2021/1/9/22221730/apple-removes-suspends-bans-parler-app-store>> accessed 9 August 2023.

The DSA introduces the minimum content moderation rules for service providers like Parler (and app stores). If providers fail to live up to them, action can be taken by public and private enforcers. Instead of praising Apple and relying on its economic power over the ecosystem to enforce the rules of diligence, the DMA tries to weaken it, and the DSA shifts it back to the state and individuals. The basic insight is that while economic power can be useful for enforcement, as it supplements the state's power, too much of it is corrosive in the long run. Thus, the state sometimes reasserts itself and takes back some of the responsibilities from the private sphere to protect its own people.

The reason for the need for such reassertion is that digitisation seems to create a gravitational pull that accumulates power on the side of platforms and other providers of such technologies.

As pointed out by Julie Cohen:

Platforms are not the only powerful entities with interests in shaping flows of information, and logics of intermediation are not the only kinds of logics that networked digital information infrastructures enable. Such infrastructures also offer new possibilities for interrupting and blocking information flows, and those capabilities can be deployed to serve a variety of interests.⁴¹

While digital communication is decentralised in terms of its production and immediate dissemination, it is largely dependent on the subsequent support and sympathy of private actors to be uploaded, kept 'alive' or found. If public, semi-public, and private spaces are all operated privately by companies, the rules of such services are then effectively the rules of what can be said online.⁴² Companies, responding to legislation passed by parliaments, not only moderate their 'product experiences' but create and enforce rules about what we find, read, upload, and share online. Search engines influence what we find;⁴³ social media companies, what we can share; app stores, what tools are distributed to us; payment providers, which content creators can receive our money; content delivery networks, who will be safe from third-party attacks; and internet providers, what websites are available to us, slowed down, or entirely blocked.⁴⁴

⁴¹ Julie E Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (OUP 2019) ch 4.

⁴² James Grimmelman, 'The Virtues of Moderation' (2015) 17 *Yale Journal of Law and Technology* 42; Luca Belli and Nicolo Zingales (eds), *Platform Regulations: How Platforms Are Regulated and How They Regulate Us* (FGV Direito Rio 2017); Tarleton Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media* (Yale University Press 2018); Nicolas P Suzor, *Lawless: The Secret Rules That Govern Our Digital Lives* (CUP 2019); Sarah T Roberts, *Behind the Screen: Content Moderation in the Shadows of Social Media* (Yale UP 2019).

⁴³ Emily B Laidlaw, 'Private Power, Public Interest: An Examination of Search Engine Accountability' (2009) 17 *International Journal of Law and Information Technology* 113; Joris van Hoboken, *Search Engine Freedom: On the Implications of the Right to Freedom of Expression for the Legal Governance of Web Search Engines* (Kluwer Law International 2012).

⁴⁴ Jonathan Zittrain, 'Internet Points of Control' (2003) 44 *Boston College Law Review* 653; Christopher S Yoo, 'Free Speech and the Myth of the Internet as an Unintermediated Experience' (2010) 78 *George Washington Law Review* 697; Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (OUP 2006); Liudmila Sivetc, 'State Regulation of Online Speech in Russia: The Role of Internet Infrastructure Owners' (2019) 27 *International Journal of Law & Information Technology* 28.

Moreover, technical architecture makes deviation from the prescribed rules much more difficult.⁴⁵

Digital tools are very powerful as levers of control because they are embedded in our lives as much as public services, such as roads and sewerage systems. Tim Wu and others have argued that the state is likely to realise this and that the new frontier of speech control techniques will originate from the exercise of private power, sometimes acting on its own in the interest of profit, and sometimes in concert with governments using self- or co-regulation.⁴⁶ It is for a reason that privatisation of the governance of speech has been thematised for years by academics,⁴⁷ and why the governance of information exchange between people has been a key concern.⁴⁸

Simply swinging the pendulum of power from companies back to the state is no solution either. Digital services have at times appropriated power that was previously in the hands of individuals because such regulatory possibilities did not exist before digitisation. In other cases, the power might have vested with the state, but digitisation has now created a new possibility for individuals to gain new agency. Regulation of digital services should therefore give some of those newly found powers back to individuals, and not only move it on the axis between the state and private actors (see Figure 1.1).

Regulation in liberal democracies should compel the state to reassert the power of individuals wherever possible. To do so, the regulation needs to pay attention to how it empowers people, and not just the state. The regulatory approaches that put too much emphasis on the authorities, as opposed to individuals or civil society, only shift from the private-power-dominated model to the state-dominated model.

Seen from this perspective, one of the additional important reasons why content moderation arguably needs positive safeguards against abuse is that in the absence of regulation, state power and private power easily conspire against individuals and redistribute power over them based on mutual convenience.⁴⁹

⁴⁵ Lawrence Lessig, 'What Things Regulate Speech: CDA 2.0 vs. Filtering' (1998) 38(4) *Jurimetrics* 629; Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books 1999); Paul S Berman, 'Cyberspace and the State Action Debate: The Cultural Value of Applying Constitutional Norms to "Private" Regulation' (2000) 71 *University of Colorado Law Review* 1263.

⁴⁶ Tim Wu, 'Is the First Amendment Obsolete?' [2017] *Columbia Public Law Research Paper* No 14-573 <<https://ssrn.com/abstract=3096337>> accessed 10 August 2023; Damian Tambini, Danilo Leonardi, and Chris Marsden, 'The Privatisation of Censorship? Self-Regulation and Freedom of Expression' in Damian Tambini, Danilo Leonardi, and Chris Marsden (eds), *Codifying Cyberspace* (Routledge 2007).

⁴⁷ Lessig (n 45); Jack M Balkin, 'Free Speech and Hostile Environments' (1999) 99(8) *Columbia Law Review* 2295; Christina Angelopoulos and others, 'Study of Fundamental Rights Limitations for Online Enforcement through Self-Regulation' (Institute for Information Law (IViR) 2015) <<https://hdl.handle.net/11245.1/7317bf21-e50c-4fea-b882-3d819e0da93a>> accessed 10 August 2023; Kate Klonick, 'The New Governors: The People, Rules, and Processes Governing Online Speech' (2018) 131 *Harvard Law Review* 1598.

⁴⁸ Michael Meyerson, 'Authors, Editors, and Uncommon Carriers: Identifying the Speaker within the New Media' (1999) 71 *Notre Dame Law Review* 79; Emily B Laidlaw, *Regulating Speech in Cyberspace: Gatekeepers, Human Rights and Corporate Responsibility* (Cambridge University Press 2015); Jan-Hinrik Schmidt and others, 'How Do Intermediaries Shape News-Related Media Repertoires and Practices? Findings From a Qualitative Study' (2019) 13 *International Journal of Communication* 853; Yochai Benkler, 'A Free Irresponsible Press: Wikileaks and the Battle Over the Soul of the Networked Fourth Estate' (2011) 46 *Harvard CR-CL Law Review* 311; Jack M Balkin, 'Old-School/New-School Speech Regulation' (2014) 127 *Harvard Law Review* 2296; Jack Balkin, 'Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation' (2018) 51 *University of California, Davis Law Review* 1149.

⁴⁹ On the concept of 'invisible handshake', Angela Daly, *Private Power, Online Information Flows and EU Law: Mind the Gap* (Hart Publishing 2016); Michael D Birnhack and Niva Elkin-Koren, 'The Invisible

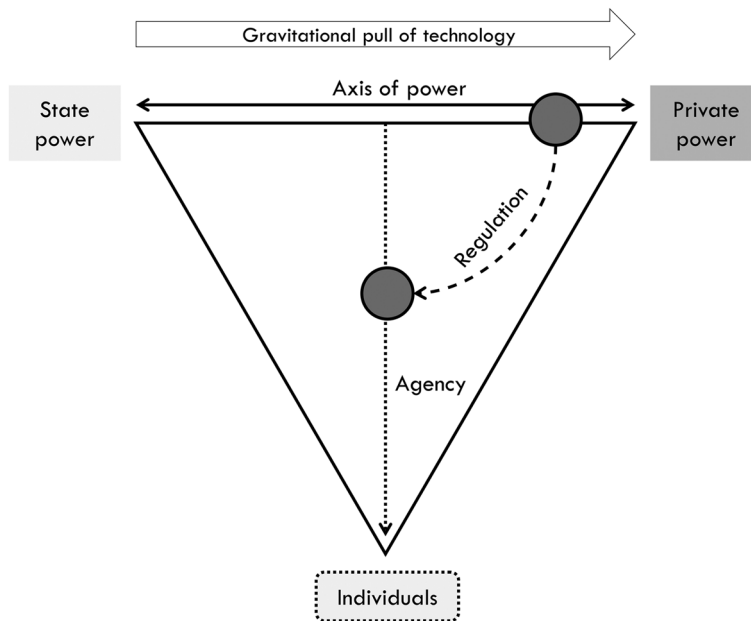


Figure 1.1 Redistribution of power

Controlling digital intermediaries ultimately means controlling the state behind the scenes. Regulations like the DSA act as a legal tool that creates a system of checks and balances between state, providers, and individuals, under which individuals can better rein in the state and private actors, private actors can push against the overreach of the state, and state actors can keep tabs on whether private actors abuse their power. Everyone keeps everyone else in check. Many components of the DSA thus can be described as a form of ‘responsive regulation.’⁵⁰

1.4 Delegated Enforcement

Thus, to understand the risks posed by private and state power, the concept of delegated enforcement is key. Delegated enforcement describes a situation where the law expects private companies to act as enforcers of the law, by entrusting them with various tasks, such as the removal of content.⁵¹

Providers often moderate content because legislation expects them to do so under the threat of sanctions, or because the state is requesting compliance in individual cases

Handshake: The Reemergence of the State in the Digital Environment’ (2003) 8 *Virginia Journal of Law & Technology* 6.

⁵⁰ See especially ch 20 discussing the work of Ian Ayres and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (OUP 1992) and applying it to the DSA.

⁵¹ Martin Husovec, ‘Mandatory Filtering Does Not Always Violate Freedom of Expression: Important Lessons from *Poland v. Council and European Parliament*’ (2023) 60(1) *Common Market Law Review* 173.

through orders. In such cases, while providers of digital services work to internalise these mandates, their actions are not entirely voluntary. The hands of providers are forced by states that grant companies discretion only in terms of *how* to apply resources to problems at hand, as opposed to *whether* to do so in the first place. Such delegated enforcement is completely rational and understandable; however, from a fundamental rights perspective, it raises many problems.

Delegated enforcement shows that our paradigm of the exercise of public power on people is partly outdated—and not only in the digital environment.⁵² Balkin makes this point most clearly⁵³ when he argues that while in the past speech control took the form of the government directly regulating individuals (‘old school speech regulation’), today’s novel approach is indirect—that is, government regulating private power for the end goal of regulating individuals (‘new school speech regulation’).⁵⁴ This means that governments pressure private entities to regulate the behaviour of other private parties (individuals), instead of directly intervening against them. After all, when trying to control protesters, why painstakingly confiscate their phones if one can simply call on wireless internet service providers to cut off their access to the internet?⁵⁵

Often, states try to disclaim any responsibility for how legislation is internalised by firms, arguing that those actions cannot be attributed to the lawmaker (or an authority). The recent case law of the CJEU and the ECtHR tries to tackle this problem by shifting some of the responsibility back to parliaments (and authorities) when they are formulating their legislation (or its interpretation). This principle is key for the application and understanding of the DSA.

In one of the recent cases, Advocate General Øe concluded that ‘[t]he legislature cannot delegate ... a task and at the same time shift all liability to those providers for the resulting interferences with the fundamental rights of users.’⁵⁶ In the Advocate General’s view, the state is responsible for the failings of firms which are legally expected to enforce the law, and so is the EU legislature in this case. He also eloquently formulates a general heuristic to assess when the risks of over-blocking are present as follows:

a risk of an ‘over-blocking’ exists, generally, where public authorities hold intermediary providers liable for illegal information provided by users of their services. In order to avoid any risk of liability, those intermediaries may tend to be overzealous and excessively block such information where there is the slightest doubt as to its lawfulness.⁵⁷

⁵² Timothy Garton Ash, *Free Speech: Ten Principles for a Connected World* (Yale University Press 2016) 365; David Kaye, *Speech Police: The Global Struggle to Govern the Internet* (Columbia Global Reports 2019) 16.

⁵³ Jack M Balkin, ‘Free Speech Is a Triangle’ (2018) 118 Columbia Law Review 2011.

⁵⁴ Ash refers to this as ‘P²’ situations, Ash (n 52) 365.

⁵⁵ Gabe Rottman, ‘Shutting Down Cell Service During Protests: The Constitutional Dimension’ (*American Civil Liberties Union*, 30 April 2012) <<https://www.aclu.org/news/national-security/shutting-down-cell-service-during-protests-constitutional-dimension>> accessed 10 August 2023.

⁵⁶ Case C-401/19 *Republic of Poland v European Parliament and Council of the European Union* ECLI:EU:C:2021:613, Opinion of AG Øe, para 84.

⁵⁷ *ibid* para 142.

Delegated enforcement is a lens through which we can look at interference with fundamental rights. Over-blocking is just one of the types of abuse, but also the most common. The principle underlying the above passage is, however, universal: legislatures must control the ‘beast’ that they have created. They ought to show commitment to do so through various safeguards to prevent abuse. For instance, if legislation tasking banks to fight money-laundering or implement sanctions leads to the constant blocking of savings of innocent people by risk-averse banks, then clearly, the legislature and relevant authorities bear part of the burden to safeguard against overreach.

To complicate things further, state power often pushes companies to act where there is no legal mandate. More than a decade ago, Yochai Benkler identified ‘a major potential vulnerability’ in the existing legal system—‘the ability of private infrastructure companies to restrict speech without being bound by the constraints of legality, and the possibility that government actors will take advantage of this affordance in an extra-legal public-private partnership for censorship.’⁵⁸

In the absence of transparency about why companies make what decisions, such ‘regulation by raised eyebrow’ extends restrictions on the freedoms of individuals without a legal mandate. As pointed out by some, the phenomenon is ‘well known from the broadcast-era efforts to pressure old radio and TV outlets to bring their programming choices in line with the desires of politicians and bureaucrats.’⁵⁹

The DSA is thus in part a positive regulation for the benefit of information exchange.⁶⁰ The DSA curtails the rising private power by subjecting it to accountability to individuals (and the state) to counter the previous situation of ‘power without responsibility.’⁶¹

1.5 Using the Right Metaphors and Principles

At the time of writing, many countries around the world are considering how to regulate lawful but harmful content—that is, content that does not violate the letter of the law but can lead to societal harm. The typical examples are vulgar content, self-harm content, disinformation, some types of pornography, or spam. While some forms of such content can be illegal, a lot of it is not. The key question that parliaments around the world are facing is how to govern such content. The UK, for instance, originally planned to include a clause tasking providers to police content that is harmful to adults.⁶² The DSA, with its focus on a broad set of risks, *de facto* prescribes that even

⁵⁸ Benkler (n 48).

⁵⁹ Adam Thierer and Andrea O’Sullivan, ‘The White House Social Media Summit and the Return of “Regulation by Raised Eyebrow”’ (*Mercatus Center George Mason University*, 12 July 2019) <<https://www.mercatus.org/economic-insights/expert-commentary/white-house-social-media-summit-and-return-regulation-raised>> accessed 10 August 2023.

⁶⁰ Advocating for this type of regulation: Kaye (n 52); Ash (n 52).

⁶¹ Rebecca Tushnet, ‘Power Without Responsibility: Intermediaries and the First Amendment’ (2008) 76 *George Washington Law Review* 986.

⁶² The relevant clause was dropped in favour of an empowerment obligation under the system known as triple lock in the later versions of the Bill—s 12 of the Online Safety HC Bill (2021–22, 2022–23) (creating a duty for some services to ‘include in a service ... features which adult users may use or apply if they wish to increase their

lawful content must be considered for the risks that it poses to others. The public debates about such regulation often quickly slip into ideological conversations. Part of the problem is the use of metaphors and the principles behind them.

Some thinkers analogise risks from digital services to those arising from cars, chemicals, workplace design, or other physical products. Lorna Wood and William Perrin's 2019 proposal which inspired the UK's Online Safety Bill⁶³ argued for an overarching duty of care of providers to prevent a wide range of harms, including psychological harms. They envisaged regulators' ability to limit 'harmful behaviour'⁶⁴ prophylactically when regulators see 'good reasons' to do so.⁶⁵ Graham Smith, a leading English internet lawyer, criticised the proposal in the UK legislative debate, arguing that '[s]peech is not a tripping hazard'.⁶⁶ I tend to agree; but what is it then?

This book tries to show that more apt analogies for the regulation of digital services may be found in the safety rules that were developed around the right to protest in public. Digital providers that distribute user-generated content to the public share many of the same characteristics as public protests. Most of the digital services are tools used by people to communicate. While the place where crowds gather might differ, the psychology and dynamics of crowds exhibits some of the same problems. As argued by Gustave Le Bon, 'the crowd is always intellectually inferior to the isolated individual'⁶⁷ because of the 'disappearance of the conscious personality, the predominance of the unconscious personality, the turning by means of suggestion and contagion of feelings, and ideas in an identical direction'.⁶⁸ Whether the direction is heroic or criminal then depends on the 'nature of the suggestion to which the crowd is exposed'.⁶⁹ The key ingredient is that the crowd as an environment reduces the perception of accountability of individuals who become its members.⁷⁰

The state even faces similar questions about whose speech should be prioritised, given the scarcity of prominent spaces where public expressions can take place. The main public square of a city is as important to protesters as placement on recommender systems is to content creators. While not all public communication will have the qualities of crowds, a lot of collective expressions, whether positive or negative, can gain them as their distribution grows. Therefore, regulation of digital services cannot be treated as some matter-of-fact regulation of chemicals or cars. Communication

control over content' that 'reduce[s] the likelihood of the user encountering' or 'alert' users to some types of content, such as hate speech, self-harm or eating disorders).

⁶³ Lorna Woods and William Perrin, 'Online Harm Reduction—a Statutory Duty of Care and Regulator' (Carnegie UK Trust 2019) 7 and 13 <<https://carnegieuktrust.org.uk/publications/online-harm-reduction-a-statutory-duty-of-care-and-regulator/>> accessed 10 August 2023.

⁶⁴ *ibid.* 48. For a discussion of consequences, Graham Smith, 'Speech Is Not a Tripping Hazard – Response to the Online Harms White Paper' (28 June 2019) <<https://www.cyberleagle.com/2019/06/speech-is-not-tripping-hazard-response.html>> accessed 10 August 2023.

⁶⁵ Woods and Perrin (n 63) 11.

⁶⁶ Smith (n 64).

⁶⁷ Le Bon (n 5).

⁶⁸ *ibid.*

⁶⁹ *ibid.*

⁷⁰ *ibid.*

tools are as sensitive for liberal democracy as the ability of people to publicly protest. Freedom of speech considerations must be at the core of every trade-off with safety.

Public protest is the soundtrack of democracy,⁷¹ and a crucial form of self-expression of individuals.⁷² It is a bedrock of the system of *liberal* democracy and closely related to human dignity and the right to think. Sometimes such self-expression only has value for individuals but in many other cases, it has value for society. It is impossible to task the government to tell the two apart. The government can draw boundaries for expressions that are not *peaceful*, but not for expressions that do not contribute to social welfare, because the *utility* of speech is impossible to settle. Only future generations can judge its utility when looking back at our times.

Thus, while comparisons to other areas, such as food safety, should not be dismissed, the reliance on such analogies should be treated with utmost caution. Moreover, even food regulation teaches us that the scientific consensus about the true nature of alleged harm is constantly evolving, and even where it is settled, parliaments do not always simply impose it on individuals as a strict limit on their freedoms. Doing so can rob people of their sense of agency and dignity. People are trusted to make the right choices with unhealthy food.

As such, liberal democracies usually do not ban most unhealthy food even though it clearly increases the cost of everyone's health care and insurance, and shortens our individual lifespans. At best, they try to make the choice of eating unhealthy food less appealing, constrain it in some sensitive settings (eg, schools), or generally make it more costly to consume. But commanding people to follow the newest scientifically approved diets does not strike us as the most obvious thing to do. This is despite the fact, as will be shown, that the constitutional limits on the distribution of food are much weaker than those for the distribution of information (Chapter 13).

Public gatherings offer a more apt analogy. Such gatherings can also lead to damage, noise, disruption, loss of business, or inflict other costs on innocent onlookers. People living near public squares might die if ambulances cannot reach them on time due to someone who is exercising his or her right to protest. Keeping gatherings safe can cost sizeable sums of money that are partly paid from the public purse. For society, such gatherings can be incredibly important, and utterly useless at the same time. However, they remain a crucial form of self-expression for individuals.

It is clear that the solution is not to ban or limit people's right to protest or pre-approve their contents according to the government's estimated social utility or risks. Instead, liberal democracies around the world decide which expressions to pronounce illegal and put additional guardrails on the right of public protest by managing its risks to others and the protesters themselves, while guaranteeing the substance of the right to self-expression.⁷³ The illegal actions of individual protesters can invite intervention by police or authorities. Organisers of protests can be deputised to help guarantee orderly

⁷¹ Timothy Zick, *Managed Dissent: The Law of Public Protest* (CUP 2023) 11.

⁷² *ibid.*

⁷³ For ECtHR, *Fromkin v Russia* App No 74568/12 (ECHR, 5 January 2016); for the US, *Ward v Rock Against Racism* 491 US 781 (1989).

assemblies but they are not liable for illegal actions of protesters. No one wants the police to approve the speakers, speeches, or posters, or to dictate to people how to conduct their right to protest. As long as assemblies are conducted lawfully, the state stands by and manages the risks.

The DSA aims to create ‘a safe, predictable and trusted online environment’ (Article 1(1)). States are thus tasked to maximise, and sometimes mutually balance the concepts of safety and trust of individuals. They offer different starting points: while safety can be imposed, trust can only be earned.

1.6 Outline of the Book

This book tries to provide a reader with a map and a compass concerning the DSA. The map takes the form of an extensive analysis of all the mechanisms of the regulation, and how they fit together into one whole. The compass is the set of principles developed throughout the theoretical chapters and summarised in the final chapter.

The book is divided into five parts.

Part I maps the question of power in the digital ecosystem and gives a bird’s-eye overview of the DSA and a broader European human rights framework. Part II is devoted to the question of liability which the DSA inherits from the ECD. It explains where the rules were amended, and how they have developed over two decades. Moreover, it offers numerous conceptual proposals regarding key undefined concepts, such as neutrality, general monitoring, and the notion of knowledge.

Part III explores the concept of accountability without liability for content that is imposed by statutory duties labelled as due diligence obligations. It explains why increasing accountability rather than liability is the right regulatory approach. Separate chapters are devoted to all due diligence obligations, from content moderation to risk management and transparency. The content moderation chapters speculate about the likely effect of the DSA on how platforms regulate content. The risk management chapters grapple with the question of why digital services cannot be regulated as other areas of laws, and how to operationalise a risk-based approach in such a sensitive area.

Part IV looks at the effects that the DSA is likely to have on the whole legal system. It explains why the DSA presents a minimum level of safeguards that are likely to enrich other areas as a digital rights charter. It also speculates that post-DSA, platform-specific rulemaking in Europe is likely to shift even more to the EU level. The chapters offer a vision of how a mixed enforcement system that blends public and private enforcement can advance some of the goals of the DSA in practice, and also offer suggestions for the regulators.

Part V condenses the insights into a set of principles that should help to guide us when facing the inevitable tension between acting upon digital risks and protecting individual freedoms. Increased accountability of providers should result in the appropriate allocation of decision-making capabilities between states and individuals.

Wherever possible, the interpretation of the DSA should help individuals to make decisions, rather than tell them what decisions to make.

The overall assessment of the DSA as a law is that it has the right ingredients to become a balanced piece of internet regulation. The envisaged regulatory system has the potential to rebuild trust in the digital environment and empower individuals. The regulation's goal of a trustworthy environment can be firmly aligned with respect for individual liberties. Indeed, with the help of the right principles, the DSA can become a blueprint for the second generation of regulation of digital services around the world. I offer the first sketch of such principles.

2

Overview of the DSA

2.1	Introduction	19	2.4.3	Advanced obligations for online platforms that are not small firms	25
2.2	Scope and Institutions	20	2.4.4	Special obligations for VLOPs	28
2.3	Liability Exemptions	21	2.4.5	Special obligations for VLOSEs	30
2.4	Due Diligence Obligations	22	2.5	Co-regulation and Enforcement	30
2.4.1	Universal due diligence obligations for all services in scope	24	2.6	The Concept of Illegal Content	31
2.4.2	Basic obligations for all hosting services	25	2.7	Conclusion	31

2.1 Introduction

The Digital Services Act (DSA) is a European Union (EU) Regulation aiming to assure fairness, trust, and safety in the digital environment. It preserves and upgrades the liability exemptions for online intermediaries that have existed in the European framework since 2000. It exempts providers of digital infrastructure-layer services, such as internet access providers, and content-layer services, such as social networks and file-hosting services, from liability for third-party content.

Simultaneously, the DSA imposes due diligence obligations concerning the design and operation of such services, in order to ensure a safe, transparent, and predictable online ecosystem. These due diligence obligations aim to regulate the general content moderation practices and design practices concerning advertising, and transparency, and regarding children and everyone's user experience. The due diligence obligations focus mainly on the *fairness of the process* rather than the content itself, and usually increase with the size and social relevance of the various services. Very large online platforms (VLOPs) and very large online search engines (VLOSEs) are subject to the most extensive risk management responsibilities, which must undergo independent auditing.

The DSA's major regulatory contribution is in *splitting* due diligence obligations from the liability for underlying content. Prior to the DSA, most of the laws tried to influence the providers' behaviour by threatening them with joint liability for what their users do. Save for some areas of law, the courts often faced a binary decision: impose a duty of care, or deny it and confirm a liability exemption. The DSA ends this binary. It comes up with its own self-standing expectations formulated as due diligence obligations. Providers violating them can be held to account. These legal obligations are

separate from those of their users (Chapter 9). Even providers who are not liable for users remain accountable for their own failings to be diligent. Violations of the DSA have no bearing on the provider's preservation of the liability exemptions.

2.2 Scope and Institutions

The DSA takes the form of an EU Regulation with a broad scope.¹ Regulations are directly applicable and do not need to be incorporated into national law. This means that all authorities in the Member States must immediately set aside any national laws that conflict with it. Being a 'horizontal' instrument (a rulebook applicable across the legal system), it will coexist with and be complemented by existing sector-specific legislation (consumer protection, intellectual property, security, home affairs, etc).

The DSA applies from 17 February 2024, across the EU. However, VLOPs and VLOSEs started being regulated earlier, from August 2023.² By February 2024, EU Member States were required to designate the agencies responsible for enforcement of the rules, including their primary agency—an independent national digital services coordinator (DSC).

Despite harmonisation, national laws remain important on many levels.

Providers that do not offer Europeans their digital services are not subject to the DSA. If they do, their lack of establishment in Europe is irrelevant; the DSA applies to providers only if they target EU markets or have a significant number of users from Europe (Chapter 9). In this sense, the DSA is very similar to the General Data Protection Regulation. The providers of relevant digital services that are established in Europe are subject to primary supervision by a national DSC of the state in which they have their main establishment. If they have no establishment in the EU, they are subject to supervision by a DSC of the state of their designated legal representative. If they failed to appoint one, they are supervised by any national DSC. In addition, the European Commission has extensive competencies to supervise and facilitate supervision in the area. VLOPs and VLOSEs, in particular, are subject to the European Commission's exclusive competence for special due diligence obligations.

The obligations imposed by the DSA are also enforceable through private actions (Chapter 19). Individuals and firms affected by breaches of the DSA's due diligence obligations can seek injunctions and claims for compensation before national courts. Such claims are often provided in national law, such as unfair competition law, contract law, consumer law, intellectual property law, or general tort law. Consumer organisations are equally empowered to seek injunctions and other redress remedies, including compensation, for violations of DSA due diligence obligations that harm the collective interests of consumers. National law can also extend collective redress to business

¹ DSA, ch I: arts 1–3, chs 4 and 17–20.

² Four months after the designation, which took place in April 2023, was delivered to companies, European Commission, 'DSA: Very Large Online Platforms and Search Engines' (*Shaping Europe's digital future*, 25 April 2023) <<https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops>> accessed 10 August 2023.

organisations. These legal claims are again distinct from liability for the underlying content. Thus, a social network can violate the DSA and be subject to injunctions to remedy this failing, but it will remain exempted from liability for a particular violation committed by one of its users (eg their hate speech or defamatory content).

2.3 Liability Exemptions

The DSA builds upon the two-decades-old rulebook of the E-Commerce Directive. It preserves and upgrades its basic liability rules.³ The DSA's reincorporation of the liability exemptions means that they receive renewed support through the democratic process, as rules that have withstood the test of time and remain fit for purpose.

The DSA continues to single out the three most common technical activities for liability exemptions. The liability exemptions prevent all the state actors, including national and Union agencies, from imposing liability for third-party content and obligations to generally monitor third-party content. The three relevant technical activities are as follows:

- Mere conduit services cover any services that 'transmit' information in a 'communication network' or provide 'access' to a 'communication network.' To the extent that providers remain neutral, they are not liable even if they are notified about illegal information.
- Caching services cover 'automatic, intermediate and temporary' storage of third-party information. To the extent that providers remain neutral, they are not liable unless the illegal content is removed from the source, and they are notified about it.
- Hosting services cover any services that 'store' information at the request of third parties. To the extent that they remain neutral, providers are in principle not liable unless they are notified.

This triad of activities together is referred to as 'intermediary services.' They cover most of the digital ecosystem. Although the system largely copies the E-Commerce Directive, the scope of mere conduit services is partly expanded. While the difference between content-layer and infrastructure-layer services is not explicitly spelled out in the text of the DSA, it is implicit in its various provisions. Mere conduit services, which mostly cover infrastructure, have exemptions that cannot be lost even when providers are notified about illegal content (eg a website they give access to). Even among hosting services, requests should in principle be directed to the providers, who are closer to the content because they have superior technical and operational ability to act. This means that webhosting firms should usually be expected to act when the hosted websites

³ DSA, ch II: arts 4–10, chs 4–8.

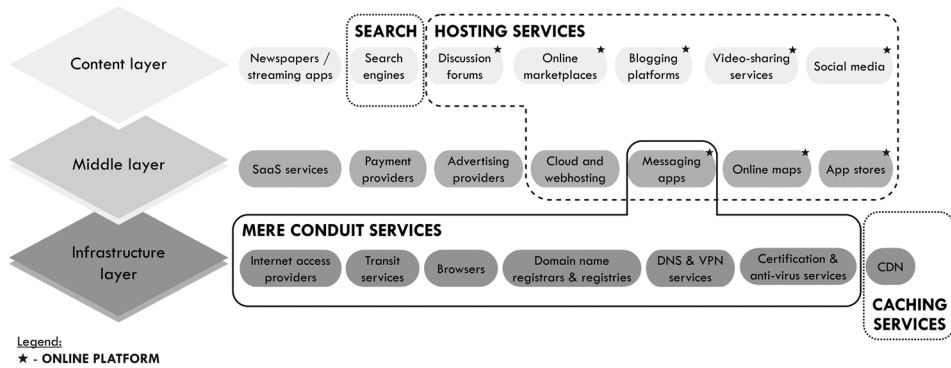


Figure 2.1 The DSA's regulatory coverage

which store the illegal content fail to do so. Figure 2.1 depicts the regulatory coverage of the entire digital ecosystem.

2.4 Due Diligence Obligations

The real novelty of the DSA lies in the creation of fully fledged tiers of due diligence obligations.⁴ Instead of 'liability', the DSA insists on the 'responsibility' that grows with the service's size and societal impact. These obligations are *not* preconditions of liability exemptions. However, they are clearly meant to legislatively balance the liability assurances with some societal responsibilities as to trust, safety, and fairness in these services. Like all due diligence obligations, they relate more to the process rather than substance. Their goal is to strengthen the fundamental rights of all stakeholders and increase fairness of individuals' dealings with providers of digital services.

The tiers of due diligence obligations apply depending on the type and size of the service. Some services are only subject to the universal layer of obligations, while other services are subject to all four layers. For VLOPs, the most regulated of all services, due diligence obligations have a layer-cake structure, with special obligations on the very top and universal obligations at the bottom.

Chapter III of the DSA is structured around the following four basic tiers of due diligence obligations, which I have labelled with four adjectives for ease of navigation (see Figure 2.2):

- **Universal obligations** apply to all services that could benefit from a liability exemption (mere conduit, caching, and hosting). With the notable exception of annual reporting, the obligations apply irrespective of the size of the firm.

⁴ DSA, ch III: arts 11–48, chs 9–16.

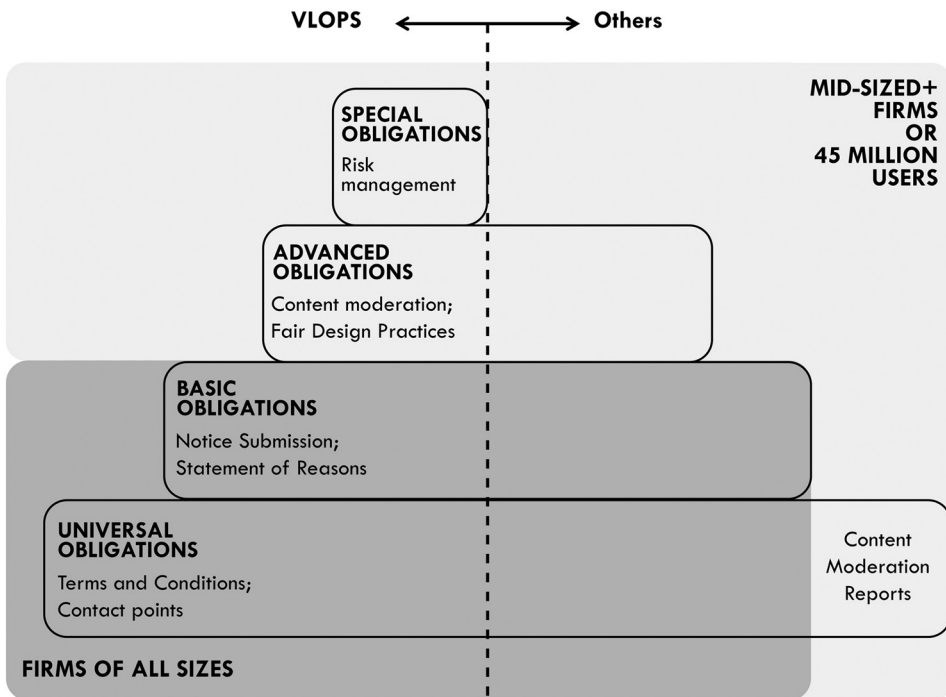


Figure 2.2 The DSA's layered structure

- **Basic obligations** apply to all services that technically perform hosting, irrespective of their size.
- **Advanced obligations** apply to a subset of hosting services, online platforms, which are bigger than small firms and that distribute information to the public as their core function. The category includes a special set of obligations for online marketplaces.
- **Special obligations** apply to online platforms that are very large (ie VLOPs). By extension, they also apply to online search engines that are very large (ie VLOSEs) with minimum modifications in scope. To trigger them, it is not size, but reach that matters. When platforms reach roughly 10% of the population of the EU (ie 45 million monthly average active users), special obligations are triggered.

Due diligence obligations apply irrespective of whether a liability exemption is subsequently lost (Chapter 9). If a service, or part of a service, in its technical description, matches the subject of a liability exemption granted by the DSA (eg hosting), the corresponding due diligence obligations apply. This remains the case even if providers do not meet or subsequently fail to meet the separate conditions for their liability exemptions (eg they stop being neutral with respect to some of the hosted content).

2.4.1 Universal due diligence obligations for all services in scope

Providers of intermediary services are obliged to designate a single point of contact for authorities and users (Articles 11–12). If they are not established in the EU, they must appoint a legal representative, a person, or a company, in one of the EU Member States. The legal representative can be held liable for the provider's non-compliance with the DSA (Article 13).

There is no universal obligation to moderate content, but all intermediary services are under an obligation to explain in their terms and conditions whether and, if so, how they moderate third-party content on their services. The policies must be explainable (Article 14). Content moderation is understood to be any restriction placed on the availability, visibility, and accessibility of information. Providers must describe in detail their content moderation practices, including whether, and if so how and when, they use automation. More importantly, when enforcing these rules, they are under an obligation to do so 'with due regard to' the rights and legitimate interests of all parties involved (Article 14(4)). This amounts to a legal requirement that they assess the fairness of their rules and their impact on human rights of their content-related decision-making.

All intermediary services, unless they qualify as micro- or small firms, are subject to new transparency obligations (Article 15). Small firms are defined as enterprises which employ fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed €10 million. However, if small and micro-firms qualify as VLOPs, they remain under the obligation (Chapter 9). All such providers must publish annual reports concerning what orders they have received from authorities (eg to remove content or provide information), and how they operate their content moderation practices (divided into distinct categories of actions), including the functioning of their internal complaint-handling systems. Hosting providers also must report on how they handle various notifications. Finally, all such providers must explain how they use automation in their content moderation. They must explain what tools they use, for what purposes, with what accuracy, and how they avoid making mistakes (Chapter 16).

In practice, this means that many firms with more than 50 employees that offer intermediary services to European users will have to start preparing and issuing annual reports. The provision will thus apply to many firms which benefit, even if only for part of their service (eg editorial media operating a discussion section), from a liability exemption. It will most definitely apply to many infrastructure services, such as internet access providers, content delivery networks, app stores, or webhosting services, for which it was less customary to publish such reports up until now. Very likely, it will also include domain name authorities, Virtual Private Network (VPN), email, and messaging services. Traditionally, such services are not expected to moderate content—but if they do (as is increasingly the case), they need to be transparent and fair in their decision-making (Article 14(4)).

2.4.2 Basic obligations for all hosting services

In addition, services providing storage of third-party information (hosting) are obliged to comply with some procedural obligations when moderating content. The DSA prescribes how exactly they should receive notifications about illegal content on their services. This ensures that proper notifications cannot be ignored.

Notification specifications (Article 16) only apply to reporting of manifestly *illegal* content. Thus, the violations of terms of use are left unregulated and subject to the providers' rules. If the notice specifications are fulfilled by notifiers (eg victims, non-government organisations (NGOs), or authorities), this often (though not automatically) means that the providers are put on notice (ie if knowledge of the manifest illegality is relevant for their liability exemption, they can lose exemption unless they act against that piece of content). The DSA 'codifies' the latest interpretation by the Court of Justice of the European Union (CJEU) that such notices should not require a 'detailed legal examination' by the provider (Chapters 7 and 11).

Hosting providers must uphold *fair processes* in content moderation, for instance, by keeping the complaining party in the loop. Uploaders will receive an explanation on the grounds and reasons behind providers' actions to affected users, if their content or accounts are restricted or demonetised—be it because the content is illegal, or because it violates its terms of use. Such explanations have prescribed minimum requirements and should include information about potential redress. Thus, takedowns or other restrictions all must be properly justified to users, irrespective of the size of providers (Article 17). The information should be sufficient to seek redress, under the national law as is the case today, and going forward, under the DSA for mid-sized or bigger online platforms.

The DSA also obliges hosting providers to notify the relevant authorities about illegal content that qualifies as a crime involving a threat to human life or safety if they become 'aware of it' (Article 18). This usually happens when they conduct content moderation and process notifications (Chapter 11).

2.4.3 Advanced obligations for online platforms that are not small firms

In addition, the richest tier of the due diligence obligations applies to a subset of 'hosting' services known as 'online platforms'. The term 'online platform' is used globally, but it is the first time that it has been defined in a legal instrument in the EU. While 'hosting' services simply provide a technical function of storage of third-party information, 'online platforms' also disseminate it to the public as their core feature and can be described as 'public-facing hosting providers'. Generally, all due diligence obligations applicable to online platforms carve out small and micro-firms.

The obligations can be divided into the following main categories:

- Content moderation:
 - o fair process;
 - o fair rules.
- Risk management:
 - o fair design practices;
 - o general risk management.
- Transparency and oversight.

2.4.3.1 Content moderation (Chapters 10–12)

To facilitate quality enforcement, the DSCs will certify trusted flaggers (eg NGOs, or associations) whose notifications are known to be of high accuracy. Providers are asked to give them priority in the assessment process. Such status can be revoked if misused. Platforms must operate a free-of-charge internal complaint mechanism which allows users to appeal their decisions within six months. Individuals who frequently incorrectly flag lawful content, or submit manifestly illegal content, shall be suspended. This incentivises good behaviour on all sides and impedes misuse by rogue actors.

Any decision restricting access, visibility, monetisation, or accounts of users, regardless of whether it is based on illegality or terms and conditions, should be reviewable. Both notifiers and affected authors of content can complain. Decisions about restrictions should be fair (ie non-arbitrary and non-discriminatory) and proportionate. Unsuccessful parties should be informed about the out-of-court dispute settlement (ODS) mechanism through which they can file complaints, usually for a fee. ODS can be pursued even when no internal complaint was filed first. However, the zero cost of internal complaints will likely attract many complainants first. ODS providers will have to show independence and expertise before they are certified by the DSCs of their Member State of the establishment. If complainants (content creators or original notifiers) win an ODS case, their fees and reasonable costs shall be reimbursed by providers. While ODS decisions are not binding, unjustified failure to observe them is a violation of the DSA.

2.4.3.2 Risk management (Chapters 13–15)

On top of the universal obligation to fairness in terms of conditions, online platforms must design, organise, and operate their interfaces in a way that avoids deceit, manipulation, and other material distortion or impairment of their users' ability to make free and informed decisions (what is sometimes referred to as 'dark patterns'). Users can be consumers and firms. While the specific rules on consumer-facing practices remain applicable (eg the Unfair Commercial Practices Directive⁵), the DSA effectively legislates

⁵ European Parliament and Council Directive 2005/29/EC of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, European Parliament and Council Directives 97/7/EC, 98/27/EC, and 2002/65/EC and European Parliament and Council Regulation (EC) No 2006/2004 [2005] OJ L 149/22 (Unfair Commercial Practices Directive).

a general clause against misrepresentation and aggressive practices in all horizontal relationships that are not covered in any sector-specific legislation. The only requirement is that the practices must be conducted via apps, websites, or other surfaces operated by online platforms that are not small or micro. Online platforms are also subject to an obligation to ensure a high level of privacy, safety, and security of minors on their services. This is further exemplified by a ban on profiling-based advertising aimed at minors.

Among the design features of services, *advertising* and *recommender systems* are more explicitly regulated. Online platforms are obliged to properly label advertisements and explain who paid for them and why a particular user sees each particular ad. Any content that is shown against payment is understood to be an advertisement. If the parameters for advertisement can be modified, this should be explained. Online platforms should enable content creators to declare advertisements in uploaded content. Finally, while targeted or personalised advertising is not banned as such, advertising to anyone, including adults, shall not be based on profiling using sensitive data as an input. Online platforms operating any recommender systems (eg timelines, suggestion tools, recommended video sections, etc) shall explain clearly the main parameters they use, and in that case, how to modify or influence those parameters. Customisability is not prescribed for regular online platforms. However, if it exists, it must be constantly accessible and modifiable for users.

A special set of mostly transparency-related rules applies to ‘online platforms allowing consumers to conclude distance contracts with traders.’ As a sort of ‘know-your-business-customer’ obligation, such platforms must take various steps to allow the traceability of traders using their services to offer products and services, including by requesting their ID documents and payment details. The collected information is stored on online platforms and can be provided to third parties if they have a legitimate interest (eg to enforce their consumer rights). The provider shall avoid confusion as to who is the trader offering the product or service.

Online platforms must also ensure their traders can provide (through their interface) all necessary information that is required by applicable consumer laws, including on product safety. They shall randomly check if the products and services sold through the platform were identified as illegal in the official databases—a juggling act to avoid imposing a general monitoring obligation. Finally, if online platforms become aware that some products or services sold through their platforms are illegal, they should inform the relevant consumers about the illegality, the identity of traders, and available redress.

2.4.3.3 Transparency (Chapter 16)

In addition to their basic due diligence obligation on transparency, online platforms must report, twice a year (on the 17th of every February and August), the number of average monthly users, and once yearly on the specifics of internal and external (ODS) disputes, and various repeat-infringer suspensions. They are obliged to submit their decisions about content, along with explanations, to a central database maintained

by the European Commission. Additional transparency obligations are foreseen for trusted flaggers, ODS bodies, and regulators.

2.4.4 Special obligations for VLOPs

Online platforms with more than 45 million active average monthly users are very large in terms of reach. Since all online platforms must publish their active monthly user numbers biannually, they will know when they reach the threshold. Although the definition of ‘active recipient of services’ is very broad, and thus invites some discussion about the scope, registered and non-registered users alike qualify (Chapter 9). For instance, this means the following users count: on online marketplaces, both sellers and buyers, including prospective buyers; on social networks, both registered and non-registered users; on short-term rental services, both providers of rental and potential tenants.

The European Commission is the only authority responsible for the supervision and enforcement of special due diligence obligations. Upon obtaining information, it designates an online platform as a ‘VLOP’ or ‘VLOSE’. The list is published in the Official EU Journal. Special obligations enter into force for VLOPs and VLOSEs four months after their designation.

VLOPs must identify, analyse, and assess any systemic risks stemming from the design, functioning, and use made of their services. They shall carry out this exercise at least once a year. The four main focus areas for such regular exercises are:

- Illegal content, including illegal conduct, on their services (eg hate speech, copyright infringements or counterfeits, bullying, stalking, child abuse material, unsafe products, etc).
- Actual or foreseeable negative effects on:
 - o all fundamental rights (eg chilling effects on freedom of speech, media pluralism, data protection, right to information, children’s rights, etc);
 - o pre-defined protected interests: civic discourse, electoral process, public security, gender-based violence, public health, and minors.
- Serious negative consequences to users’ physical and mental well-being.

The typical actions expected to counter these challenges include the redesign of their amplification and moderation tools, such as recommender systems and algorithmic decision systems, adjustment of content moderation rules, advertising rules, an increase of resources for various trust and safety activities, improvement of documentation and handling of incidents, protection measures in favour of vulnerable groups, and data-related practices. Given the known disparity of resource allocation across the world or linguistic communities, VLOPs must consider their actions in the local context (ie for each language and each country).

Risk reports should be submitted at VLOPs' own expense to independent auditors who should assess compliance with all special due diligence obligations, but also universal, basic, and advanced obligations. Codes of Conduct signed by VLOPs can further inform the substance of these obligations. If the audit is not fully positive, VLOPs must consider the suggested operational recommendations of auditors. If they do not implement them, they must justify why in the implementation report, and set out alternatives. The self-assessment, own mitigation measures, external audits, and follow-up implementation reports are transmitted to the European Commission (unredacted) and made available to the public (redacted).

In addition to general risk management that concerns a broad set of risks, the DSA specifies a few other areas of special obligations concerning content moderation systems (crisis protocols, increased reporting, and resource allocation), design of the services (recommender systems and advertising transparency) and oversight (data access and scrutiny by supervisory authorities and vetted researchers):

- Regarding content moderation, VLOPs must maintain a crisis response mechanism for instances of extraordinary circumstances leading to a serious threat to public security or public health in the Union or a part of it. The mechanism grants the European Commission powers to ask VLOPs to implement certain actions. In addition to other transparency obligations, VLOPs must specify what human resources they put into the content moderation per each official language of Member States, how they support other obligations concerning the fairness of content moderation, and how accurate are the procedures.
- Regarding design of services, recommender systems offered by VLOPs must always include at least one option that is not based on the profiling. However, it does not have to be a default. Advertising carried by VLOPs must be accompanied by a publicly accessible archive ('repository') which stores for one year all necessary disclosures about published advertisements, along with a minimum of additional meta information.
- Regarding oversight, VLOPs must provide access to data to supervising authorities and vetted researchers. DSCs and the European Commission shall have access to the necessary data to monitor and assess compliance with the DSA. They should assist with explaining the design and logic of the functioning of their recommendation systems. Vetter researchers, a status granted by a DSC, shall have access to data to conduct research into the detection and understanding of systemic risks, as well as adequacy, efficiency, and impacts of the mitigation measures adopted by the platforms. Finally, VLOPs are obliged to appoint a compliance officer who is an independent senior manager with distinct responsibility for compliance with DSA obligations. The officer should report directly to the management body of the VLOP and have a clear set of tasks and authorisation within the firm.

2.4.5 Special obligations for VLOSEs

Search engines that have more than 45 million active monthly users qualify as VLOSEs. Their special obligations mirror those of VLOPs. However, because the entire product of search engines does not qualify for one unitary hosting exemption, they are not explicitly subject to all universal, basic, and advanced obligations as their online platform counterparts. Search engines are explicitly only subject to a chapter on special obligations. However, many of the special obligations refer to and build upon universal (eg transparency) or advanced (eg recommender systems or advertising) obligations. These obligations thus extend to VLOSEs also.

Moreover, to the extent that parts of their services are covered by one of the liability exemptions (eg storage of keywords in sponsored results or links in the natural search results), they can also be subject to all other due diligence obligations. As extensively debated in Chapter 7 of this book, this is a point that will have to be clarified by the CJEU in the coming years. In my view, search engines in some situations can be regarded as hosting and online platform services. It is therefore still possible that the content moderation of search engines will be subject to the DSA's due diligence obligations.

2.5 Co-regulation and Enforcement

The DSA creates a complex supervisory system.⁶ The DSA's prescriptive rules concerning content moderation can be enforced through a mixture of administrative enforcement and private causes of action. In contrast, the system of risk management applicable to Big Tech—VLOPs and very large search engines (VLSEs)—is only subject to administrative enforcement and additional co-regulation through codes of conduct.

The administrative competencies are distributed between national DSCs and the European Commission. The risk management obligations applicable only to Big Tech are supervised exclusively by the European Commission. Other due diligence obligations of Big Tech, such as those concerning content moderation, are supervised jointly by the Member States of their establishment and the European Commission, with the latter having a priority to enforce. Finally, the due diligence obligations of other providers are supervised only by the authorities of the Member State of their own establishment or that of their legal representative.

National laws continue to outline procedures and powers of national authorities that allow them to issue orders regarding illegal content on digital services. The DSA

⁶ DSA, ch IV: arts 49–88, chs 17–20.

only provides minimum and optional requirements for such orders (Chapter 8). Member States are *not* prohibited from using other forms of requests than the foreseen orders. For instance, Union law allows them to send regular notifications. It is important, however, to distinguish between state-power-based orders of courts or authorities and private-enforcement-related notices, which do not trigger an obligation to remove, but only an obligation to assess, regardless of the public nature of the sender.

2.6 The Concept of Illegal Content

The DSA does *not* harmonise what content or behaviour counts as illegal (Article 3(h)). The DSA basically refers to the entire legal system of its Member States to express what is illegal for the purposes of the DSA. In some areas, such laws can be harmonised, but this remains an exception.

When national laws are largely in sync and only diverge *on margin*, platforms can bridge the differences in the standard of illegality by the least common denominator in the terms and conditions (eg when two countries prohibit the incitement of violence, but they take different views on when behaviour is illegal). But they can also enforce these laws only locally. Both approaches are in line with the DSA, and are legitimate.

The more difficult questions arise when two legal systems prescribe *mutually incompatible* behaviour because they demand contradictory actions (eg disclosure of some facts may be illegal in one country, while prescribed in the other). In cases of such conflicts, the challenge is to find an implementation that satisfies both Member States. Within the EU, the possible moderators of conflicts are the rules of the internal market (Chapter 17) and fundamental rights (Chapter 3).

But this outcome also means that such national content laws do produce immediate effects across the Union with the help of the DSA. A malicious government could adopt legislation and then enforce it through the DSA. The only realistic check on such enforcement is the initial geolocation of such requests by providers and a potential countervailing interim relief obtained from the judiciary. Providers might also decide to push against such legislation and deny the requests or orders, but by doing that, they expose themselves to legal risks of liability for distributing such content.

2.7 Conclusion

The DSA does not regulate content. It regulates the procedures under which online content disputes take place on digital services. Its aim is to create a trustworthy environment by two main mechanisms. The first of these is by making people safe from

illegal content. This is achieved by removing such content quickly and offering means that can bring the original perpetrators of wrongs to account. Second, by giving people more scope to pursue content disputes with platforms, whenever they feel that they have observed the rules but were accused otherwise. Removing such arbitrariness can foster the trust of people in the digital ecosystem in the long run.

3

Human Rights

3.1 Introduction	33	3.2.4 Rights of providers of digital services	40
3.1.1 Horizontal vs vertical situations	34	3.3 Luxembourg Jurisprudence	47
3.2 Strasbourg Jurisprudence	35	3.3.1 Freedom of expression of speakers	48
3.2.1 Speakers, victims, readers, and facilitators	36	3.3.2 Freedoms of providers	50
3.2.2 Internet's specificity and experimentation	38	3.3.3 Freedom of readers to receive information	52
3.2.3 Types of expressions	39	3.4 Institutional Blind Spots	53

3.1 Introduction

The Digital Services Act (DSA) is primarily a fairness regulation guaranteeing fair process, rules, and practices. For big digital services, it is also a risk management regulation. From the individual's standpoint, however, it gives many people the opportunity to understand, articulate, and advance their rights against the providers of digital services who are in a position of influence despite being non-state actors. In other words, the DSA opens the door for the application of individual freedoms.

This chapter maps the scope and interrelationship between the DSA, the European Union (EU) Charter of Fundamental Rights (CFR), and the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR). It provides a high-level overview of the EU regulatory landscape and its relation to the DSA and the relevant fundamental rights. The European human rights system is multi-layered. National constitutions are supplemented by the Convention and other international treaties, developed by the Council of Europe—one of the main bodies of the continents' post-war security architecture.

While the EU Charter, adopted in 2009, is more modern and encompassing, the Convention from 1950 and its subsequent Protocols mostly cover civil and political rights.¹ A simple comparison with the EU Charter shows that some human rights, such as freedom to conduct business (Article 16 CFR), right to consumer protection (Article 38 CFR), access to services of general economic interest (Article 36 CFR), integration of persons with disabilities (Article 26 CFR), and the rights of the children and the elderly (Articles 24–25 CFR) are not present in the Convention. In some cases,

¹ A protocol is generally an annex to a Treaty, supplementing the main Treaty text with details and exemptions. See, eg the right to education in Protocol 1, art 2.

the Convention protects the same interests under conceptually different provisions of its own: freedom of and sciences (Article 13 CFR) falls under freedom of expression under the Convention (Article 10 ECHR); right to data protection (Article 8 CFR) under the right to private life (Article 8 ECHR); protection of intellectual property (Article 17(2) CFR) under the right to peaceful enjoyment of possessions (Article 1 Protocol 1 ECHR).

While the EU Charter's catalogue is broader, its application is conditional upon the exercise of the EU law-making powers. The EU Charter thus shadows EU law (Article 51(1) CFR). If the national laws are not within the remit of the EU law, the EU Charter does not apply.² The application of the Convention, in contrast, is not conditional. Viewed from this perspective, the DSA is a general-purpose instrument that will open doors to the EU Charter's application to digital content disputes. It will offer a springboard for civil, political, economic, and social rights for many new situations.

3.1.1 Horizontal vs vertical situations

The key distinction in human rights law is between horizontal situations (non-state actors interfering with each other's rights among themselves) and vertical situations (state actors interfering with the rights of non-state actors). In digital services, it is sometimes difficult to draw these lines clearly. To an independent observer, it is often unclear if a provider is motivated by profit and acting voluntarily, or due to coercion by law. Due to cost-saving or strategic reasons, platforms moderating content might claim to enforce contracts where the impetus comes from law enforcement. This fluidity between horizontal and vertical complicates things a lot.

If a provider acts voluntarily, it should enjoy broad discretion to run its business. It can draft its contracts to its own liking within the limits of law and, at best, must take the human rights of into account. It can be sloppy, arbitrary, or even capricious. However, in a scenario where a provider acts involuntarily when coerced to do so by the state, it cannot be allowed to exceed the discretion that is allowed to the state. Otherwise, by using a non-state agent, state actors could easily usurp more powers for themselves. Thus, knowing *why* providers do what they do is crucial to understanding the constraints under which they operate. The DSA tries to create more transparency partly to allow us to better understand which framework applies.

In legal theory, Balkin argued that digital speech cases often constitute a triangle.³ That is, the state is regulating providers for the sake of policing the user's speech or behaviour. I prefer to call such situations *delegated enforcement*.⁴ Not because the state is conferring powers but because the state is compelling some outcomes. Delegated enforcement turns horizontal disputes into vertical affairs, although an observer might

² For procedural application, see Case C-617/10 *Åklagaren v Åkerberg Fransson* ECLI:EU:C:2013:105.

³ Jack Balkin, 'Free Speech is a Triangle' (2018) 118(7) *Columbia Law Review* 2011.

⁴ Martin Husovec, '(Ir)Responsible Legislature? Speech Risks under the EU's Rules on Delegated Digital Enforcement' (2021) <dx.doi.org/10.2139/ssrn.3784149> accessed 10 August 2023.

still mistakenly see them as sparring between equals. If a provider removes content because it expects negative legal consequences, the true dispute is between the state that compels the outcome and the individual affected by it, and not with the provider who only gives effect to it. Inherently, there is nothing special about this situation. Very few would think that a government that asks employers to fire employees who hold certain views is not acting vertically. The same would apply to our assessment of sanctions or other interventions. Even if the executioner is a non-state actor who ‘only’ responds to incentives, the actions should be attributed to the state. Otherwise, enforcement by proxy becomes a loophole.

Delegated enforcement situations are increasingly common due to digitisation, which is opening our lives to an ever-increasing number of proxy-regulatory opportunities. Each digital service provides legislatures with a *regulatory platform*. Platforms posing as de facto regulatory vehicles extend the hands of the government. They offer outsourcing of costs along with scale and speed that are hardly matched by administrative bureaucracies or the judiciary.

The DSA tries to address the increased reliance on delegated enforcement in two main ways. First, it introduces universal procedural and other safeguards in the system that apply irrespective of whether the providers act voluntarily or involuntarily. Second, it proclaims very large online platforms and search engines (VLOPs/VLOSEs) as key places for digital gathering. Such places then must manage all sorts of risks posed by their digital spaces. Consequently, for VLOPs/VLOSEs under the DSA, almost every action is a form of delegated enforcement.

Any regulation of digital services can be described as managing conflicts between multiple parties, such as platforms, content creators, their audiences, and potential victims. Each side has a set of fundamental rights working in their favour and wishes to advance them at the expense of the other. For instance, hate speech victims desire faster removals from platforms, citing concerns about their safety and private life, while content creators push back citing free speech interests and the need for due process. The legislatures navigating these multi-party conflicts are often between a rock and a hard place. The courts usually are in an even more difficult position because ‘the most important legal dials and knobs’⁵ require positive legislation and cannot be simply invented by interpretation of human rights law.

3.2 Strasbourg Jurisprudence

The two most significant provisions in digital content disputes are the right to private and family life (Article 8 ECHR) and the right to receive and impart information (Article 10 ECHR). Other important rights include the freedom of assembly (Article

⁵ Daphne Keller, ‘The Three-Body Problem: Platform Litigation and Absent Parties’ (*Lawfare*, 4 May 2023) <<https://www.lawfaremedia.org/article/the-three-body-problem-platform-litigation-and-absent-parties>> accessed 10 August 2023.

11 ECHR),⁶ prohibition of discrimination (Article 14 ECHR),⁷ peaceful enjoyment of possessions (Article 1 Protocol 1 ECHR),⁸ and finally, the right to an effective remedy (Article 13 ECHR).⁹

3.2.1 Speakers, victims, readers, and facilitators

The majority of the European Court of Human Rights (ECtHR)'s digital case law concerns the right to private life and freedom of expression guarantees. The cases are usually brought by speakers (content creators)¹⁰ or their victims¹¹ who are affected by measures imposed on their providers of digital services, such as:

- website blocking imposed on access providers,
- decryption measures imposed on messaging services,¹²
- liability for posting a hyperlink to a third-party video,¹³
- liability for providing a space for other people's comments.¹⁴

Only in a few instances, the cases were brought directly by *providers* of digital services, such as news sites operating comments sections,¹⁵ providers of a messaging service,¹⁶ or owners of piracy websites.¹⁷ All these cases were considered Article 10 ECHR cases. On the other hand, in some cases, the ECtHR rejected complaints by passive readers or

⁶ *Kablis v Russia* App nos 48310/16 and 59663/17 (ECtHR, 30 April 2019) on blocking a social network account of an activist organising a protest.

⁷ *Beizaras and Levickas v Lithuania* App no 41288/15 (ECtHR, 14 January 2020) on the failure to investigate gay-related hate speech by authorities which violates arts 8 and 14 ECHR.

⁸ *Paefgen GmbH v Germany* App nos 25379/04, 21688/05, 21722/05, and 21770/05 (ECtHR, 18 September 2007) on the cancellation of a domain name found to interfere with art 1 Protocol 1 ECHR, though justified.

⁹ *Vladimir Kharitonov v Russia* App no 10795/14 (ECtHR, 23 June 2020); *OOO Flavis and others v Russia* App nos 12468/15, 23489/15, and 19074/16 (ECtHR, 23 June 2020); *Bulgakov v Russia* App no 20159/15 (ECtHR, 23 June 2020); *Engels v Russia* App no 61919/16 (ECtHR, 23 June 2020).

¹⁰ *Ahmet Yıldırım v Turkey* App no 3111/10 (ECtHR 18 December 2012); *Magyar Jeti Zrt v Hungary* App no 11257/16 (ECtHR, 4 December 2018) for the inclusion of hyperlink in an article; *Kablis* (n 6); *Kharitonov* (n 9); *Flavis* (n 9); *Bulgakov* (n 9); and, about an owner of a website with user-generated content: *Engels* (n 9); *Wikimedia Foundation, Inc v Turkey* App no 25479/19 (ECtHR, 1 March 2022); *Ali Ergin Demirhan v Turkey* App no 10509/20 (ECtHR, pending).

¹¹ Art 8 cases, such as *Pihl v Sweden* App no 74742/14 (ECtHR, 7 February 2017) regarding a defamation victim alleging a lack of protection; *KU v Finland* App no 2872/02 (ECtHR, 2 December 2008) regarding the absence of tools in the national law to fight cybercrimes; *Høiness v Norway* App no 43624/14 (ECtHR, 19 March 2019) regarding a defamation victim complaining about lack of protection; *Volodina v Russia (No 2)* App no 40419/19 (ECtHR, 14 September 2019) regarding a cybercrime victim complaining about lack of protection; *Tamiz v UK* App no 3877/14 (ECtHR, 19 September 2017).

¹² *Podchasov v Russia* App no 33696/19 (ECtHR, pending), where a Telegram user complains about being impacted by a de-encryption order.

¹³ *Magyar Jeti Zrt* (n 10).

¹⁴ *Sanchez v France* App no 45581/15 (ECtHR [GC], 15 May 2023).

¹⁵ *Delfi AS v Estonia* App no 64569/09 (ECtHR, 16 June 2015) (Delfi); *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v Hungary* App no 22947/13 (ECtHR, 2 February 2016) (MTE).

¹⁶ *Telegram Messenger LLP and Telegram Messenger Inc v Russia* App no 13232/18 (ECtHR, pending).

¹⁷ *Fredrik Neij and Peter Sunde Kolmisoppi v Sweden* App no 40397/12 (ECtHR, 19 February 2013) (The Pirate Bay (ECtHR)).

listeners using digital services, such as Last.fm,¹⁸ but accepted the complaints by active users, such as academics trying to watch YouTube.¹⁹

Article 10 guarantees the right of *speakers* to impart information as well as the right of *readers and listeners*, being the public, to receive it.²⁰ The protection of Article 10 applies to the *means of dissemination* along with the *content of information* because restrictions imposed on the former undoubtedly interfere with the readers' right to receive and impart information.²¹ The beneficiaries of protection, therefore, range from passive or more active readers (often dubbed as 'users'), content creators (also sometimes confusingly called 'users'), owners of social media accounts, and website operators, to their technical intermediaries, such as internet access providers and platforms hosting their content or comments.

This diversity in beneficiaries clearly poses some difficulties in navigating and developing the contours of case law. Speakers traditionally engage in editorial content (eg journalists employed by media). For editorial speech, the ECtHR's jurisprudence tries to conceptualise 'responsible journalism' and acceptable duties and responsibilities.²² However, platforms and similar digital services *do not* disseminate their own speech. They provide tools that may be closer or further from the content creators; however, these are still only tools for creating and disseminating speech. Therefore, they *facilitate* the expressions of others.²³ This begs the question of how to apply the older standards from the area of media with editorial content to the 'new media'. The ECtHR claims to resolve this by looking for a 'graduated and differentiated response' for actors who fall within the new notion of media, following the Recommendation of the Committee of Ministers.²⁴ As will be explained below, it is not always clear that the ECtHR actually succeeds in 'graduating and differentiating' the applicable standards. However, the case law is in flux.

Article 8 ECHR, on the other hand, protects victims of torts of defamation,²⁵ hate speech²⁶ or other cybercrimes, such as dissemination of child abuse material²⁷ or other types of 'cyberviolence'.²⁸ The ECtHR is conscious of the fact that Articles 8 and 10

¹⁸ *Akdeniz and others v Turkey* App no 20877/10 (ECtHR, 11 March 2014).

¹⁹ *Cengiz and others v Turkey* App nos 48226/10 and 14027/11 (ECtHR, 1 December 2015).

²⁰ See eg *Observer and Guardian v the United Kingdom* App no 13585/88 (ECtHR, 26 November 1991), para 59; *Guerra and others v Italy* App no 14967/89 (ECtHR, 19 February 1998), para 53.

²¹ See eg *Öztürk v Turkey* App no 22479/93 (ECtHR, 28 September 1999), para 49: 'It applies not only to the content of information but also to the means of dissemination since any restriction imposed on the means necessarily interferes with the right to receive and impart information'; *ML and WW v Germany* App nos 60798/10 and 65599/10 (ECtHR, 28 June 2018), para 89: 'the applicants' right to respect for their private life under Article 8 of the Convention and, on the other hand, the radio station's and publishers' freedom of expression and the public's freedom of information under Article 10'.

²² *Amaghlobeli and others v Georgia* App no 41192/11 (ECtHR, 20 May 2022), para 37.

²³ Facilitation was referenced by the ECtHR in the context of search engines, see *ML and WW* (n 21) para 97.

²⁴ Committee of Ministers, 'Recommendation CM/Rec(2011)7 on a New Notion of Media on 21 September 2011' (Council of Europe 2013).

²⁵ *Höiness* (n 11); *Pihl* (n 11); *Magyar Jeti Zrt* (n 10).

²⁶ *Delfi* (n 15); *Sanchez* (n 14); *Beizaras* (n 7).

²⁷ *KÜ* (n 11).

²⁸ *Volodina* (no 2) (n 11) paras 17, 18, and 20: the publication of her intimate photographs without consent, impersonation through the creation of fake social-media profiles, and tracking her with the use of a GPS device.

cases represent similar complaint zones and therefore tries to synchronise its case law in the two areas.²⁹

3.2.2 Internet's specificity and experimentation

The starting point of the Strasbourg (and even Luxembourg) case law seems to be the specificity of the internet. As mentioned above, for the ECtHR, digital services facilitating user-generated content must be subject to 'graduated and differentiated'³⁰ regulation that differs from the regulation of editorial media. For top European judges, the special attributes of the internet are its 'accessibility', 'capacity to store and communicate vast amounts of information', its ability to support 'user-generated expressive activity', and its role in 'facilitating the dissemination of information in general'.³¹ At the same time, as emphasised by the Fifth Section of the ECtHR in *ML and WW v Germany*:

Internet sites are an information and communication tool particularly distinct from the printed media, especially as regards the capacity to store and transmit information, and that the risk of harm posed by content and communications on the Internet to the exercise and enjoyment of human rights and freedoms, particularly the right to respect for private life, is *certainly higher* than that posed by the press.³²

The ECtHR is, on the one hand, very sensitive to measures such as whole website blocking, but on the other, so far less willing to be prescriptive with respect to hate speech on digital platforms. In the latter case, it gives the Member States a broader margin to experiment than would be the case in the context of traditional media. The existing case law does not prescribe how to deal with hate speech online, but only how to not deal with it. However, such a position may only be temporary because the Convention is a 'living instrument', and nothing prevents the ECtHR from tightening the noose on the legislatures' choices in the future.³³ If the Court starts with the articulation of minimum standards under Article 8, it must be careful not to clash directly with the complex system envisaged by the DSA.

²⁹ *ML and WW* (n 21) para 92.

³⁰ Committee of Ministers (n 24), Appendix, para 7: 'A differentiated and graduated approach requires that each actor whose services are identified as media or as an intermediary or auxiliary activity benefit from both the appropriate form (differentiated) and the appropriate level (graduated) of protection and that responsibility also be delimited in conformity with Article 10 [ECHR] and other relevant standards developed by the Council of Europe', cited by the ECtHR in *Delfi*, para 113.

³¹ Case C-401/19 *Republic of Poland v European Parliament and Council of the European Union* ECLI:EU:C:2022:297, para 46; The Grand Chamber is citing the ECtHR decision in *Cengiz* (n 19) para 52; and *Kharitonov* (n 9) para 33.

³² *ML and WW* (n 21) para 91 (emphasis mine).

³³ George Letsas, 'The ECHR as a Living Instrument: Its Meaning and its Legitimacy' (2014) <<https://dx.doi.org/10.2139/ssrn.2021836>> accessed 10 August 2023; *Tyrer v United Kingdom* App no 5856/72 (ECtHR, 25 April 1978).

In any case, this broader margin of appreciation has thus far supported the Member States' experimentation with policies that tackle the sensitive topic of hate speech. In two important cases involving liability for storing comments containing *hate speech* posted by others, the ECtHR allowed the Member States also to impose post-publication monitoring obligations to avoid civil³⁴ or even monetary criminal liability.³⁵ In *defamation* cases on the other hand, the ECtHR is much more prescriptive and views general content monitoring obligations as incompatible with freedom of expression.³⁶

3.2.3 Types of expressions

Traditionally, the margin of appreciation of the states is very narrow with respect to political speech on the one hand and very broad for cases involving commercial speech³⁷ and matters of intimate personal convictions within the sphere of morals or religion on the other.³⁸ In *Markt intern Verlag GmbH and Klaus Beermann v Germany*, the ECtHR held that '[t]he Court must confine its review to the question whether the [unfair competition] measures taken on the national level are justifiable in principle and proportionate'.³⁹ The same review of 'justifiable in principle and proportionate' was also adopted in the context of commercial advertising.⁴⁰ In some cases, such as *Mouvement Raëlien Suisse v Switzerland*,⁴¹ the speech can find itself 'in-between' two standards of review. In a case involving a promotional campaign of a supposed UFO religious group, the ECtHR's Grand Chamber applied a broader margin:

The poster campaign in question sought mainly to draw the attention of the public to the ideas and activities of a group with a supposedly religious connotation that was conveying a message claimed to be transmitted by extra-terrestrials, referring for this purpose to a website address. The applicant association's website thus refers only incidentally to social or political ideas. The Court takes the view that the type of speech in question is not political because the main aim of the website in question is to draw people to the cause of the applicant association and not to address matters of political debate in Switzerland. Even if the applicant association's speech falls outside the commercial advertising context—there is no inducement to buy a particular product—it is nevertheless closer to commercial speech than to political speech per se, as it has a certain proselytising function. The State's margin of appreciation is therefore broader.⁴²

³⁴ *Delfi* (n 15).

³⁵ *Sanchez* (n 14).

³⁶ *Höiness* (n 11); *Pihl* (n 11); *Magyar Jeti Zrt* (n 10).

³⁷ Comprehensively, Dimitrios Doukas, 'Commercial Speech and Freedom of Expression in EU Law: A Paradigm of a Sliding Scale of Review for the European Court of Justice?' (2019) 44(6) *European Law Review* 739.

³⁸ *Mouvement Raëlien Suisse v Switzerland* App no 16354/06 (ECtHR, 13 July 2012), para 61.

³⁹ *Markt intern Verlag GmbH and Klaus Beermann v Germany* App no 10572/83 (ECtHR, 20 November 1989), para 33.

⁴⁰ *Casado Coca v Spain* App no 15450/89 (ECtHR, 24 February 1994), para 50.

⁴¹ *Mouvement Raëlien Suisse* (n 38).

⁴² *ibid* para 62; *VgT v Switzerland* App no 24699/94 (ECtHR, 28 June 2001) paras 57, 70–72, 75, and 79.

This then results in ECtHR's broader deference, as '[t]he Court cannot interfere with the choices of the national and local authorities, which are closer to the realities of their country, for it would thereby lose sight of the subsidiary nature of the Convention system'.⁴³

However, the ECtHR also held that for the citizen, 'advertising is a means of discovering the characteristics of services and goods offered to him'.⁴⁴ Therefore, in some cases, even the speech interests of corporations can prevail over the state's ability to enforce public morals corresponding to religious sensitivities of some groups. In *Sekmadienis Ltd v Lithuania*,⁴⁵ the ECtHR held that the Lithuanian authorities overstepped the margin of appreciation when they banned commercial advertising for simply invoking the names of Jesus and Mary⁴⁶ on the grounds that it was 'incompatible with the principles of a religious person' and cannot be viewed as 'gratuitously offensive or profane, [inciting] hatred on the grounds of religious belief or [attacking] a religion in an unwarranted or abusive manner'.⁴⁷ Similarly, in *Krone (No 3)*,⁴⁸ an injunction issued by the Austrian courts regarding an unfair competition case which effectively banned price comparison of newspapers was found to violate Article 10 based on 'impairing the very essence of price comparison'.⁴⁹

This case law, therefore, suggests a limited review of speech that does not contribute to the public debate and is merely commercial. While advertising and other purely commercial acts still enjoy Article 10 protection, the states have a broader possibility to regulate it as they see fit. Only a 'soft proportionality test' applies in such cases. On the other hand, political speech and non-commercial speech⁵⁰ are protected under a very rigorous proportionality test. In between these two are the cases of commercial speech that primarily contribute to a public debate. The intensity of the scrutiny also changes depending on whether there is a European consensus on a particular issue. If it exists, then the deviation can be scrutinised more closely.⁵¹

3.2.4 Rights of providers of digital services

Information dissemination is very important to freedom of expression. Article 10 undoubtedly protects 'means of dissemination'. With typical editorial speech, the facilitator's protections usually overlap with the speaker's protection. Organisations behind the newspapers or broadcasters that facilitate and invest in editorial speech would be considered metaphorical speakers, although the protected speech originated

⁴³ *Mouvement Raëlien Suisse* (n 38) para 64.

⁴⁴ *Casado Coca* (n 40) para 51.

⁴⁵ *Sekmadienis Ltd v Lithuania* App no 69317/14 (ECtHR, 30 January 2018).

⁴⁶ *ibid* paras 7, 8, and 9.

⁴⁷ *ibid* para 77.

⁴⁸ *Krone Verlag GmbH & Co KG v Austria (No 3)* App no 39069/97 (ECtHR, 11 December 2003).

⁴⁹ *ibid* para 33.

⁵⁰ *Open Door and Dublin Well Woman v Ireland* App no 14234/88 (ECtHR, 23 September 1992), para 80: Irish ban on information about abortion clinics abroad, including if provided by non-profit counselling services.

⁵¹ *Casado Coca* (n 40) paras 54–55; *Stambuk v Germany* App no 37928/97 (ECtHR, 17 October 2002), para 40.

from their employees. Given that they provide organisational support for creating and sharing of expressions, it was natural to treat them as speakers.

However, even in the offline world, a subset of actors in the ecosystem, such as printers, booksellers, cinema owners, or transport companies, would be harder to categorise as speakers. They do not express *their* views. At most, they help materialise the freedom of expression of other individuals through their commercial services. Yet, their freedom to operate a business is crucial to enabling such freedoms, given their role in facilitating the expression and dissemination of other people's ideas and expressions. They print them and deliver them to customers. In the digital age, the number of such facilitators has skyrocketed. To avoid the creation of loopholes in the effective protection of Article 10, these actors cannot be left unprotected. Otherwise, the governments could target them instead to halt the dissemination of undesirable ideas and expressions.

With the rise of non-editorial speech, which originates from millions of individuals, digital facilitators have multiplied and gained tremendous importance. Ensuring their protection under freedom of expression laws has become a vital concern for digital speech infrastructure because speakers depend on facilitators' support. No content can be published online without a hosting service, nor can it be reached without an internet access provider. However, much like printers and booksellers, web hosting companies storing third-party content or internet access providers channelling consumers to websites are hardly speakers.

Under the Convention, it is unclear if such 'facilitators' enjoy their own protection under Article 10 or whether their protection is only a derivative of speakers' protection. Surprisingly, case law does not address this detail.⁵² Under ECtHR case law, facilitators are simply assumed to be entitled to Article 10 protection for third-party content, often without much explanation from the ECtHR. What is clear, however, is that the facilitators' status as companies does *not* limit the protection offered by Article 10. As noted by the ECtHR in *Autronic AG v Switzerland*, 'neither *Autronic AG*'s legal status as a limited company nor the fact that its activities were commercial nor the intrinsic nature of freedom of expression can deprive *Autronic AG* of the protection of Article 10'.⁵³ Article 10 applies to 'everyone', irrespective of whether they are natural or legal persons.⁵⁴

There are two broad groups of cases concerning digital providers as facilitators: (1) platforms that usually store third-party content or at least provide other tools that

⁵² There has not been a single case grappling with these entities in the relevant case law. In the US, the leading case addresses facilitators' protections concerning booksellers—*Smith v California*, 361 US 147 (1959). Although there is no equivalent case law of the ECtHR on bookseller's liability, there are cases regarding traditional publishers' art 10 rights—*Handyside v the UK* App no 5493/72 (ECtHR, 7 December 1976). *Handyside* is the leading case in which the applicant was a traditional book publisher, and the confiscation of its book was considered an interference with the publisher's art 10 rights. Although the case resulted in a no-violation decision, it is one of the first freedom of expression cases, and it set a high standard for such cases, which is still applied today.

⁵³ *Autronic AG v Switzerland* App no 12726/87 (ECtHR, 22 May 1990), para 47. Prior to this case, the ECtHR had already stated that art 10 applies to profit-making companies. See eg *The Sunday Times v UK* App no 6538/74 (ECtHR 26 April 1979); *Markt intern* (n 39).

⁵⁴ On corporation as rights-bearers, Turkuler Isiksel, 'Corporate Human Rights Claims Under the ECHR' (2019) 17 *Georgetown Journal of Law and Public Policy* 979.

process it, such as search engines, and (2) providers of digital infrastructures, such as the internet access, domain name system, and encrypted messaging services.

The second group of cases is rarely filed by providers directly. The complainants are usually speakers, the owners of the website that was blocked, or readers, the passive users of blocked websites. The only exception to date is the pending case of *Telegram v Russia*, where a messaging service complained against the imposition of encryption backdoors on the basis of Article 10.⁵⁵

The ECtHR's case law contains three leading cases on the liability of websites for comments posted on *platforms*. Rather confusingly, the first Grand Chamber case, *Delfi v Estonia* (2015),⁵⁶ represents 'the hate speech exception' to the general approach underlying the case law. The contents in question were comments under news articles containing hate speech and other 'clearly unlawful speech'.⁵⁷ The authors of these comments were anonymous, and once the comments were posted, only the platform could remove them.

It was common ground between parties that any liability imposed on *the platform* for user-generated content constituted an interference with *its rights* under Article 10.⁵⁸ In its decision, the Grand Chamber set a very broad margin of appreciation for the Member States. It devised a balancing test and ultimately expressed that professional news websites can be held liable under national law if they fail to scrutinise content in the comments even *before* they are notified about such comments by affected victims. In doing so, it accepted the interpretation of the Estonian tort law that imposed civil liability before notification of illegal hate speech as compatible with Article 10, even though this reading would have run afoul of EU statutory laws then, such as the ECD's liability exemptions.⁵⁹ The judgment seemed to have implied that the Council of Europe's Member States, many of whom were also EU members, would be free to impose monitoring obligations on platforms concerning third-party content.

The strong criticism of the judgment led a later president of the ECtHR, Judge Robert Spano, to write extra-judicially about the case in 2017, claiming that 'the case is to some extent unique and unsuitable as a basis for broad interpretive conclusions over and above the facts presented by the case'.⁶⁰ The follow-up case law of the Court proved this to be true, although *Delfi* did not entirely disappear as a framework of reference.⁶¹ The general approach of the Court is now represented by numerous section decisions that apply the *Delfi* test. The most important of them is *MTE v Hungary* (2016).⁶² In this case, the Court acted much more prescriptively to give effect to Article 10 rights. It

⁵⁵ *Telegram Messenger LLP* (n 16).

⁵⁶ *Delfi* (n 15).

⁵⁷ *ibid* 110.

⁵⁸ *Delfi* (n 15) para 181: 'The Court notes that it was not in dispute between the parties that the applicant company's freedom of expression guaranteed under Article 10 of the Convention had been interfered with by the domestic courts' decisions. The Court sees no reason to hold otherwise.'

⁵⁹ The Member States of the EU were constrained then by the ECD and its liability provisions and, today, by similar provisions under the DSA.

⁶⁰ Robert Spano, 'Intermediary Liability for Online User Comments under the European Convention on Human Rights' (2017) 17(4) Human Rights Law Review 665, 679.

⁶¹ *Sanchez* (n 14).

⁶² *MTE* (n 15).

endorsed as constitutionally necessary the liability model (but not the details), which both the E-Commerce Directive (ECD) and the DSA adopt, based on the idea of shared responsibility for the harms and wrongs in the digital ecosystem. For platforms hosting content, this shared responsibility is known as the notice and takedown (or action) choreography.

In *MTE*, the Fourth Section of the Court rejected far-reaching monitoring duties due to their chilling effect on the freedom of expression on the internet. It ruled that ‘the notice-and-take-down-system could function in many cases as an appropriate tool for balancing the rights and interests of all those involved’.⁶³

In contrast with *Delfi*, the comments in *MTE* did not amount to speech inciting hate and violence. More importantly, the users were able to modify their comments once they were published. The authors of comments thus had more agency to do the right thing on their own. In addition, the for-profit criterion that weighted against the provider in *Delfi* remained unaddressed.⁶⁴ In *Delfi*, the case concerned a large, professionally managed internet news portal that ran on a commercial basis, published news articles of its own and invited its readers to comment on them; the Grand Chamber expressly stated that it did not concern other internet fora, such as social media platforms.⁶⁵

MTE soon became the general approach that was endorsed by numerous subsequent cases, including those filed on the basis of Article 8 ECHR, such as *Pihl v Sweden* (2017),⁶⁶ *Tamiz v United Kingdom* (2017),⁶⁷ and *Høiness v Norway* (2019).⁶⁸ In all these cases the applicants tried to argue that a state was in breach of its positive obligation under Article 8 as it failed to protect their right to reputation by *not* holding intermediaries liable for third-party comments. All three cases, although section judgments only, support the reading that *Delfi*’s broadened margin of appreciation applies *only* when speech includes hate or incitement to violence. The commercial character of the platforms constantly seems to be de-emphasised, and *Delfi*’s role of eliciting comments in the context of its professional editorial activities is emphasised instead.

This continuous qualification of the *Delfi* judgment is also confirmed by Judge Spano in his 2017 article.⁶⁹ He reconciled *MTE* and *Delfi* by confirming that the Court only acted carefully to allow national experimentation and that the Grand Chamber endorsed the notice and takedown system as a primary vehicle for resolution of the digital content disputes. He said:

⁶³ *ibid* para 91 (presented as an application of the Grand Chamber decision in *Delfi*).

⁶⁴ *ibid* paras 5, 8–10, and 14. *MTE* and *Index* were joint applicants.

⁶⁵ *Delfi* (n 15) para 116; *Tamiz* (n 11) para 85.

⁶⁶ *Pihl* (n 11), regarding user-generated comments on a blog, the case was held inadmissible by the Third Section.

⁶⁷ *Tamiz* (n 11), regarding user-generated comments on a blog post hosted on a blogging platform, the case was held inadmissible by the First Section.

⁶⁸ *Høiness* (n 11), regarding user-generated comments, the Second Section found no violation.

⁶⁹ Spano (n 60).

[I]t may be argued that in *Delfi AS*, by in some sense encouraging Contracting States to consider the beneficial value of the notice-and-take-down system as a suitable mechanism for balancing the relevant conflicting interests, the Court adopted a middle ground between two diametrically opposing viewpoints on the regulation of the Internet, one advocating for an environment relatively free from regulation of on-line conduct and the other campaigning for a regulated Internet where the same legal principles apply both online and offline.⁷⁰

While one can disagree with his characterisation of the actual problem, as the *MTE* line of cases hardly can be portrayed as ‘relatively free from regulation’, his point about national experimentation is crucial. The judges, faced with their first case on this novel matter, were simply unsure about how to approach it and did not want to put a strait-jacket on their future judgments. Hence, they decided to make room for Member State legislatures. Unfortunately, the collateral consequence of this hesitancy is the widely assumed message among the public that the platform *ought* to be liable for comments posted by users—which evidently grossly mischaracterises the supposed motivations behind the judgment.

The test established in *Delfi* to determine the lawfulness of facilitator liability under Article 10 ECHR was subsequently reformulated in *MTE* as the following set of criteria: (i) the context of the comments, (ii) the measures applied by the applicant to prevent or remove the comments, (iii) the liability of the actual authors of the comments as an alternative to the facilitator’s liability, (iv) the consequences of the domestic proceedings for the applicant, and (v) the consequences of the comments for the injured party.⁷¹

In 2023, the Grand Chamber dealt with liability for the comments of others again in *Sanchez v France*.⁷² It reviewed a Fifth Section decision which found that the French decision imposing criminal monetary liability on a politician for unlawful third-party comments published on the Facebook profile he operated was sound. *Sanchez* offered an opportunity for the Court to refine the *Delfi* test and to confine the original exception within a very narrow context.⁷³ Unfortunately, the Court arguably only muddled the waters further. In *Sanchez*, the politician operating the Facebook profile was only specifically notified about one of two unlawful comments, which he did not incite in any way. French courts held the politician liable for the notified comment its author took down within 24 hours and for failing to remove the related un-notified comment in the same discussion thread.

In the reasoning of the Court, it is clear that the majority considered the provider to be put on notice with respect to both comments. However, as pointed out by the dissent, they ignored the extremely short time window for the first comment and the lack

⁷⁰ *ibid* 679.

⁷¹ *MTE* (n 15) paras 69 and 84.

⁷² *Sanchez* (n 14).

⁷³ European Information Society Institute, ‘Third-Party Intervention in re *Sanchez v. France*’ (*EISI*, 22 March 2022) <<https://husovec.eu/wp-content/uploads/2022/03/Final-web.pdf>> accessed 10 August 2023.

of specific notification of the second comment. The judges implied in *Sanchez* that at least after acquiring some knowledge of the situation, the provider of the forum, in this case, an owner of a profile on social media, should have investigated related potential unlawful acts. This outcome is not in line with the liability exemptions of the DSA,⁷⁴ which require much more specific knowledge before they strip liability exemptions. However, the *Sanchez* ruling cannot be cited as supporting the imposition of general monitoring obligations either.

Sanchez is probably best summarised by the following passage from the ruling:

As the Internet has become one of the principal means by which individuals exercise their right to freedom of expression ... the Court is of the view that interferences with the exercise of that right should be examined particularly carefully, since they are likely to have a chilling effect, which carries a risk of self-censorship. Nevertheless, the identification of such a risk must not obscure the existence of other dangers for the exercise and enjoyment of fundamental rights and freedoms, in particular those emanating from unlawful, defamatory, hateful or violence-inciting remarks, which can be disseminated as never before ... For this reason the possibility for individuals complaining of defamatory or other types of unlawful speech to bring an action to establish liability must, in principle, be maintained, to constitute an effective remedy for the alleged violations ... The Court observes that, at the relevant time, the holder of a Facebook account used for non-commercial purposes was not fully able to control the administration of comments. In addition to the fact that there was no automatic filtering process available—although it had been possible to remove public access ...—the effective monitoring of all comments, especially in the case of a very popular account, would have required availability or recourse to significant, if not considerable, resources. Nevertheless, to exempt producers from all liability might facilitate or encourage abuse and misuse, including hate speech and calls to violence, but also manipulation, lies and misinformation. In the Court's view, while professional entities which create social networks and make them available to other users necessarily have certain obligations ..., there should be a sharing of liability between all the actors involved, allowing if necessary for the degree of liability and the manner of its attribution to be graduated according to the objective situation of each one.⁷⁵

The ECtHR's case law is motivated by two diametrically opposed but similarly undesirable effects: the chilling effects caused by liability and the lack of right to effective remedy of victims. The Court's starting point is that those who facilitate other people's expressions, such as platforms or owners of profiles on social media, must bear their part of the shared responsibility for the resulting harm done to others. The more professional or better equipped they are, the more responsibility they have. Given that the

⁷⁴ Chs 6–7.

⁷⁵ *Sanchez* (n 14) paras 184–85 (emphasis mine).

46 Member States of the Council of Europe might each have different pieces of legislation to deal with such issues, the approach is usually very cautious in such sensitive areas.

In my view, the existing Strasbourg case law can be summarised as follows.⁷⁶

The ECtHR generally views the notice and takedown choreography as an appropriate balancing tool for the rights of victims, speakers, and platforms. This is why all attempts so far by victims to invoke their rival Article 8 rights against the Article 10 rights of speakers and platforms have failed when they tried to argue that the state shall hold platforms liable *prior to* obtaining knowledge about unlawful content by notification.⁷⁷ The ECtHR thus distributes the onus between victims (who must tell platforms about their grievances), platforms and their active account holders (who must investigate them swiftly), and perpetrators of harm (who are ultimately responsible). If the countries impose liability on facilitators prior to knowledge, platforms themselves can claim a violation of their Article 10.

However, in cases where the speech at stake is hate speech or incitement to violence and the platform had invited comments (but had not instigated them) in the context of its professional editorial activity (eg as a newspaper or politician), the states are permitted, as far as Article 10 is concerned, to impose duties and liability prior to such notification as well, under some circumstances. But this does not mean that in such cases, the states are *required* to do so in order to uphold Article 8 rights. *Delfi* thus only remains an option for the Member States. The case law also does not say that such permitted liability automatically means joint liability for damages caused by comments. The ECtHR reserves the ability to study the proportionality of legal consequences in each specific case. After all, even accountability obligations imposed by the DSA are a form of liability and thus must pass such a test.

Finally, the *Sanchez* ruling shows that the knowledge-acquisition process for the purposes of Article 10 should not be automatically equated with high standards under the DSA. Where the EU's DSA requires specific knowledge about illegality,⁷⁸ the Strasbourg jurisprudence seems much more flexible, but its exact legal standard remains unclear. Nevertheless, the ECtHR clearly continues to draw the distinction between aware and unaware facilitators of unlawful speech by others, the latter of which can be proportionally sanctioned, albeit only exceptionally. Figure 3.1 describes the Convention and its constraints.

The Member States of the Council of Europe, which are also members of the European Union, are additionally constrained by the EU Charter and, legislatively, by the DSA. The ECtHR case law is useful for the DSA discussions in two main ways. First, it provides a backdrop for the CJEU when developing the constitutional ceiling

⁷⁶ See more Martin Husovec and others, 'Grand Confusion After Sanchez v. France: Seven Reasons for Concern about Strasbourg Jurisprudence on Intermediaries', *Maastricht Journal of European and Comparative law* (2024, forthcoming).

⁷⁷ This does not rule out that cases of incitement could impose liability in such cases. Knowledge is part of the very act of incitement which goes hand in hand with intent.

⁷⁸ Ch 7.

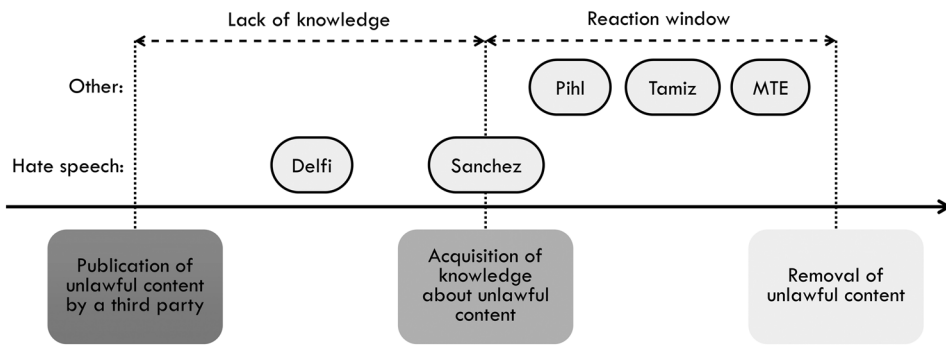


Figure 3.1 ECtHR intermediary liability constraints

under the EU Charter, which might go beyond the CJEU due to common tradition and existing secondary law. Secondly, ECtHR considerations arguably remain valid under the DSA's due diligence obligations, such as risk mitigation by VLOPs and VLOSEs. I will argue throughout the book that the principle of shared burden for social harms⁷⁹ should, in fact, be one of the defining principles that helps us with our understanding of not only the DSA's liability rules but also its accountability rules.

3.3 Luxembourg Jurisprudence

As noted earlier, unlike the Convention, the EU Charter applies only when EU law applies (Article 52(1) CFR). This means that secondary legislation usually serves a dual purpose. First, it positively harmonises a particular area of law by stipulating common solutions. Second, it opens the doors to assessing the problems within such areas by the EU Charter. The latter effect has proven much more important than simply serving as a check on the EU legislature's law-making powers. The CJEU has repeatedly reframed and reinterpreted problems and solutions to them from *within* the EU legal framework. Fundamental rights thus act as more than mere moderators of excess, serving as true guiding principles and lenses through which the CJEU develops the law.

It is expected that the DSA will be strongly shaped by the EU Charter for two main reasons. Firstly, its wide scope opens the door to EU law for many types of content disputes, ranging from the removal of unlawful content and content moderation practices of platforms to due diligence obligations of VLOPs. Since they regulate all types of digital content, the scope is essentially only limited by the concept of the services where such phenomena take place. Secondly, and also relatedly, such norms are often worded very broadly or use open-ended terms, such as an obligation to put in 'place reasonable, proportionate and effective mitigation measures, tailored to the specific systemic

⁷⁹ Ch 21.

risks'⁸⁰ and to act in 'diligent, objective and proportionate manner'⁸¹ and in 'due regard to fundamental rights'.⁸²

Another important consequence will be that the DSA will open the door for the horizontal effect of EU fundamental rights.⁸³ Under a directly applicable regulation, obligations to act in due regard to fundamental rights could be interpreted as a general clause for such indirect effect. This will increase the importance of the fundamental rights framework for fleshing out the most essential obligations that some services are asked to observe in their daily operations.

While the DSA is a very broad horizontal instrument, it does not capture the entire ecosystem of digital services as its name might suggest. The DSA mostly captures the obligations for content-layer services closer to the recipients of the service. At the moment, this is where most content disputes take place. The fundamental rights that are most likely to shape the DSA framework are the freedom to conduct the business of platforms (Article 16 CFR), the right to freedom of expression of readers and/or speakers (Article 11 CFR), and many conflicting rights of victims, such as the right to private life, data protection, consumer protection, protection of children, and so on.

An exhaustive debate on the human rights dimension of the rights of victims is beyond the scope of this book. The broad range of the rights at stake makes generalisations very difficult and can probably only be properly analysed separately. The conflicting rights often offer different justifications to limit the rights and freedoms of platforms, content creators (speakers), and their readers.⁸⁴

3.3.1 Freedom of expression of speakers

When content creators upload content on platforms, they exercise their freedom of expression. As I have highlighted in the context of the Convention, such expressions can receive different protections depending on the type of speech and how much they contribute to the public debate. Commercial speech, by definition, receives less protection than political speech. While the CJEU has accepted equivalence of Article 11 CFR with

⁸⁰ DSA, art 35.

⁸¹ DSA, art 14.

⁸² DSA, Rec 51.

⁸³ On the horizontal effect of fundamental rights, see Amélie Heldt, *Intensivere Drittwirkung: die mittelbare Drittwirkung der Meinungsfreiheit in Öffentlichkeiten der digitalen Gesellschaft: eine verfassungsrechtliche, rechtsvergleichende und interdisziplinäre Analyse* (Mohr Siebeck 2023).

⁸⁴ In some cases, even the same rights might clash, such as when entrepreneurial content creators clash with platforms (both invoking art 16 CFR) or when victims and readers clash about the tools that might be used to protect them against the abuses of speakers (both invoke art 7 CFR). Another example is when the speech interests of platforms, or even their advertising clients, and their content creators clash when defining what is the legal content that should be de-ranked (both invoking art 11 CFR).

Article 10 ECHR,⁸⁵ the CJEU's case law particularly 'falls behind the standards of protection afforded by the ECtHR to commercial speech'.⁸⁶ It has been criticised for lacking 'a systematic or consistent scrutiny of interferences' with commercial speech and for generally assuming that 'commercial speech makes no (significant) contribution to public discourse and constitutes a threat to pluralism'.⁸⁷ Unlike the Convention, the EU Charter also highlights the prominence of the freedom of arts and sciences (Article 13 CFR), and the obviously related rights of assembly (Article 12 CFR), thought, conscience, and religion (Article 10 CFR). Moreover, in the EU context, the freedom to conduct business has a special place and may apply to situations when content creators act as businesses.

In *Poland v Council/EP*, the CJEU broadly incorporated the ECtHR's internet case law by holding that:

Article 10 ECHR guarantees freedom of expression and information for everyone and applies not only to the content of information, but also to the means of its dissemination, for any restriction imposed on the latter necessarily interferes with the freedom to receive and impart information. As that court has pointed out, the internet has now become one of the principal means by which individuals exercise their right to freedom of expression and information. In the light of their accessibility and their capacity to store and communicate vast amounts of information, internet sites, and in particular online content-sharing platforms, play an important role in enhancing the public's access to news and facilitating the dissemination of information in general, with user-generated expressive activity on the internet providing an unprecedented platform for the exercise of freedom of expression.⁸⁸

The CJEU also incorporated the ECtHR's concept of prior restraints, which describes a scenario in which speech is limited before it can be disseminated. It notes that while such prior restraints are not absolutely prohibited, they must be carefully assessed because they 'pose such a risk to compliance with that fundamental right that a particularly tight legal framework is required'.⁸⁹ For instance, the CJEU has classified filters that block content automatically upon upload as such prior restraints. However, its review of the strength of the legal safeguards that the EU legislature must provide can still be seen as relatively weak.⁹⁰

⁸⁵ Case C-163/10 *Criminal Proceedings against Patriciello* ECLI:EU:C:2011:543, para 31; Case C-157/14 *Neptune Distribution SNC v Ministre de l'Économie et des Finances* [2016] 2 Common Market Law Review, 24, paras 63–65; Case C-547/14 R (*on the application of Philip Morris Brands SARL*) v *Secretary of State for Health* ECLI:EU:C:2016:325, paras 147–48.

⁸⁶ Doukas (n 37).

⁸⁷ *ibid.*

⁸⁸ *Poland* (n 31) para 46.

⁸⁹ *Poland* (n 31) para 68.

⁹⁰ Martin Husovec, 'Mandatory Filtering Does Not Always Violate Freedom of Expression: Important Lessons from *Poland v Council and European Parliament*' (2023) 60(1) Common Market Law Review 173.

3.3.2 Freedoms of providers

Luxembourg judges tend to conceptualise the rights of providers very differently from the Strasbourg judges. To date, the CJEU has not considered the *speech* interests of providers in a single case. Since *Google Spain* and its subsequent case law,⁹¹ platforms and infrastructure providers can only invoke economic interests. While restricting content on their services can trigger interference with freedom of expression, those rights are only thematised with respect to content creators and never to providers themselves. In *Poland*, the CJEU confirmed this again.⁹² This is in stark contrast to ECtHR case law, which analyses the same interferences as limits on the provider's freedom of expression.⁹³

While this might appear as a minor doctrinal difference, since the freedom of expression of users (ie both speakers and readers) potentially remains present in the balancing exercise, the consequences can be dramatic if users, as parties absent in the litigation, are not able to present their case. The CJEU famously held in *Google Spain* that '[data protection] rights *override*, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in finding that information upon a search relating to the data subject's name'.⁹⁴ This framing, which arguably overemphasises the economic interests of platforms and downplays their structural importance as continuous speech infrastructure, then discounts the weight of the societal contribution of search engines to the freedom to receive information, form opinions and express them.⁹⁵ Although subsequent case law has shown that the CJEU is not insensitive to speech concerns in the context of the right to be delisted,⁹⁶ any framing by the CJEU in past cases already sends a signal to the Member State courts or authorities.⁹⁷

Freedom to conduct business, the right that is mostly associated with providers, is an unusual right in the international fundamental rights toolbox.⁹⁸ Its origins in European case law can be traced to preliminary rulings of the German courts reviewing the validity of EU actions. The CJEU responded to them often by including economic considerations under the so-called general principles of the EU, which were meant to supplement the non-existent EU fundamental rights framework prior to the EU Charter.⁹⁹ The inclusion of Article 16 in the EU Charter signalled a possible transition

⁹¹ Case C-131/12 *Google Spain SL and Google Inc v AEPP and Mario Costeja González* ECLI:EU:C:2014:317 (*Google Spain*).

⁹² *Poland* (n 31) para 90.

⁹³ *Delfi* (n 15); *The Pirate Bay* (ECtHR) (n 17); *Telegram Messenger LLP* (n 16).

⁹⁴ *Google Spain* (n 91) para 97 (emphasis mine).

⁹⁵ Joris van Hoboken, *Search Engine Freedom: On the Implications of the Right to Freedom of Expression for the Legal Governance of Web Search Engines* (Kluwer Law International 2012).

⁹⁶ Case C-460/20 *TU and RE v Google LLC* ECLI:EU:C:2022:962, para 60ff.

⁹⁷ See for instance, the decisions by the German Federal Constitutional Court: BVerfG v 6 November 2019—1 BvR 276/17; BVerfG v 6 November 2019—1 BvR 16/13.

⁹⁸ Steve Peers and others, *The EU Charter of Fundamental Rights: A Commentary* (Hart Publishing 2014) 438, 463.

⁹⁹ See for instance, where the German court examined an EU regulation in light of the freedom of disposition in trade, economic liberty, and freedom of action: Case C-11-70 *Internationale Handelsgesellschaft*

of these principles¹⁰⁰ to a full-fledged right, although the EU Charter still refers to it only as ‘freedom’ both in the provision and its section name.¹⁰¹

Historically, unlike classic civil and political rights, socio-economic rights were meant to be construed as mere ‘principles’ in the EU Charter.¹⁰² Their primary goal was to inform policy-making by the *legislature*. As noted by Lord Lester of Herne Hill, it is to be doubted that judges have any mandate or special expertise to determine how national resources should be allocated between different priorities.¹⁰³ However, after a little over ten years, it became clear that Article 16 CFR now forms an important part of the fundamental rights catalogue that actually tempers the judicial balancing of rights. Most problematically, however, such judicial balancing often comes at the expense of classical civil and political rights, such as freedom of expression. Typically, in the DSA context, this occurs when a platform’s right to conduct business is given priority over the negative impact on the speech interests of citizens.¹⁰⁴

The CJEU gradually conceptualised Article 16 as a freedom to engage in economic self-expression without being subject to unjustifiable restrictions. It ‘includes, inter alia, the right for any business to be able to freely use, within the limits of its liability for its own acts, the economic, technical and financial resources available to it.’¹⁰⁵ The cases to date disproportionality involved claims about the regulation of advertising of alcohol,¹⁰⁶ mandatory licensing of short news reports by broadcasters,¹⁰⁷ or costs of digital providers in implementing copyright enforcement measures.¹⁰⁸ The CJEU outlined that Article 16 ‘covers the freedom to exercise an economic or commercial activity, the freedom of contract and free competition.’¹⁰⁹ The freedom of contract includes the freedom to choose with whom to do business and to determine the price of a service.¹¹⁰

In cases involving the blocking of websites or content, the CJEU usually emphasised that even courts, when fashioning the relief granted to victims, must consider freedom to conduct business.¹¹¹ In other words, such considerations are not limited to the

ECLI:EU:C:1970:114; where in response to a German reference, CJEU examined a Commission decision under the right to freely choose and practice the trade and profession: Case C-4-73 *Nold* ECLI:EU:C:1974:51; and where in response to a German reference, CJEU examined an EU regulation under the freedom to pursue economic activity: Joint Cases C-143/88 and 92/89 *Zuckerfabrik Süderdithmarschen and Zuckerfabrik Soest* ECLI:EU:C:1991:65, paras 76–77.

¹⁰⁰ These were the Weimar origins of the right (arts 151–56 of the Weimer Constitution 1919); see Peers and others (n 98) 438.

¹⁰¹ However, it is questionable if this has any bearing given that other subjective rights, such as freedom of arts and sciences, are worded equally as freedoms.

¹⁰² Lord Peter Goldsmith, ‘A Charter of Rights, Freedoms and Principles’ (2001) 38(5) *Common Market Law Review* 1201, 1212

¹⁰³ *ibid.*

¹⁰⁴ Case C-314/12 *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH* ECLI:EU:C:2014:192.

¹⁰⁵ *ibid* para 49.

¹⁰⁶ Case C-544/10 *Deutsches Weintor eG v Land Rheinland-Pfalz* ECLI:EU:C:2012:526.

¹⁰⁷ Case C-283/11 *Sky Österreich GmbH v Österreichischer Rundfunk* ECLI:EU:C:2013:28.

¹⁰⁸ *UPC Telekabel* (n 104); Case C-360/10 *SABAM v Netlog NV* ECLI:EU:C:2012:85; Case C-70/10 *Scarlet Extended SA v SABAM* ECLI:EU:C:2011:771.

¹⁰⁹ *Sky Österreich* (n 107) para 42.

¹¹⁰ *ibid* para 43.

¹¹¹ *SABAM* (n 108); *Scarlet Extended* (n 108) paras 48–49.

legislature. The fact that access providers might be able to choose a method of implementation of costly and complex measures was viewed favourably as it does not fully ‘restrict the free use of the resources at his disposal’ because it provides some choice.¹¹² Moreover, this case law shows that the freedom to conduct business can equally apply in horizontal settings.¹¹³

In the context of the DSA, the freedom to conduct business might serve several functions. First, providers might rely upon it to defend against the DSA provisions. Second, the freedom to conduct business can be invoked by victims and content creators against the providers themselves. In cases where livelihoods and the functioning of business are increasingly embedded into the digital ecosystem, arbitrary and excessive actions of providers can equally be scrutinised. While for some disputes, there might be other legislative instruments, such as the Platform to Business Regulation, the Digital Markets Act or national unfair competition laws, the DSA obligations might run in parallel with them. For instance, over-restrictive efforts to mitigate risks through de-amplification can excessively interfere with the legitimate business operations of content creators on such platforms. Whenever platforms are expected to act by the DSA, they must properly account for these interests as well.

3.3.3 Freedom of readers to receive information

Article 11(1) CFR guarantees everyone a right to freedom of expression, including the freedom to hold opinions and to receive and impart information and ideas regardless of frontiers. Article 11(2) then guarantees specifically freedom and pluralism of media. The DSA potentially touches upon all of these different components. It protects speakers and readers by giving them tools against a set of private actors who organise highly visible places to exchange information and ideas.

The DSA is the single most significant piece of EU law that tries to legislatively guarantee freedom of expression in some concrete setting. While freedom of expression is often characterised by cases that protect against interferences, the digital ecosystem (as some other types of media before) has shown that such freedoms need to be equally protected from private power, whether acting as a self-interested market player or an agent of the state. In secondary EU law, the only comparable piece of legislation is the Open Internet Regulation that guarantees freedom of expression of end-users—ie readers and speakers (such as website owners and application providers) using the internet to exchange with each other.¹¹⁴ The EU is currently also preparing its European Freedom Media Act, which should target more traditional freedom of editorial media and their pluralism. The legislative efforts are best described as positive legislative

¹¹² *UPC Telekabel* (n 104) paras 50–54.

¹¹³ See also, *Peers and others* (n 98) 449, although these cases involve the state getting involved in enforcing remedies.

¹¹⁴ European Parliament and Council Regulation (EU) 2015/2120 laying down measures concerning open internet access [2015] OJ L 310/1, art 3 (Open Internet Regulation).

measures to protect freedom of expression from the encroachment of private and state powers.

With the growing secondary legislation guaranteeing freedom of expression interests, of which the DSA is the perfect poster child, its operationalisation raises a challenge for the CJEU. As pointed out by many, including Lorna Woods, '[t]he EU remains on the whole in an economic mind-set'.¹¹⁵ It, therefore, remains to be seen how the CJEU grapples with speech and due process regulation when confronting the trade-offs with the single market harmonisation and restrictions on economic freedoms.

3.4 Institutional Blind Spots

Multi-party balancing demands intensive fact-finding and understanding of one's institutional blindness. Some stakeholders very rarely or never appear before the institutions that interpret the law.

Daphne Keller refers to this as a 'Three-Body Problem'.¹¹⁶ She points out that absent parties often might have the most important interests in the disputes between two litigating parties. This problem is hard to overcome. Careful calibration of the balancing exercise is, therefore, required to consider the situations holistically. As argued by Keller, this sometimes means that the legislature, rather than the judiciary, is the only viable forum. Institutional blindness affects all institutions, but it affects courts more than the legislature. In a way, it explains why the Strasbourg court is hesitant to be too prescriptive in its case law.

The DSA is a genuine effort to deal with the problems prescriptively and horizontally by considering all interests. It opens the disputes up into more avenues and thus allows more parties to articulate their concerns.

Firstly, the Digital Services Coordinators and the EU Commission have it directly included in their mandate to consider the manifold interests of all the groups as their enforcement responsibilities. They also oversee *all* types of content and are therefore less likely to be captured by the narrative of one set of victims with distinct needs. In the context of VLOPs, the DSA focuses on due process and speech risks alongside risks to children, public security, and health risks, meaning that the risk of under-enforcement should be continuously considered against the risks of over-blocking (eg aggressive reduction of disinformation regarding health claims is also viewed in considering the impact on legitimate content).

Second, the DSA articulates several tools, such as collective redress, that should help proactively bring the interests of affected parties before the CJEU. Through the likely privatisation of enforcement of DSA obligations on the national level, such parties do not have to rely on the middleman of the state authorities to defend them. They can proactively defend their interests which were difficult to defend until now.

¹¹⁵ Steve Peers and others, *The EU Charter of Fundamental Rights: A Commentary* (Hart Publishing 2014) 337.

¹¹⁶ Keller (n 5).

However, some institutional limits of CJEU will remain a problem. Unlike in Strasbourg,¹¹⁷ the preliminary reference procedure under Article 267 TFEU does not allow for third-party interventions.¹¹⁸ This often means that the CJEU is not fully aware of the impact on non-parties, as the states rarely articulate how certain enforcement measures might influence the public's right to access information. Since the parties are just as generally not well-placed or even motivated to advance these arguments, the CJEU is missing relevant pieces of information. As a result, some cases which require multi-party balancing then deliver sub-optimal outcomes for freedom and rights that were not part of the conversation. Consequently, this places pressure on the Advocate Generals to be able to represent those forsaken views.

For instance, in the *UPC Telekabel* case, the CJEU adopts the view that the open-ended forms of website blocking better respect the rights of obliged access providers, as they can choose their method of implementation.¹¹⁹ Little does the Court realise that such injunctions increase the risk of over-blocking legitimate content, as they allow the same providers to adopt measures that are overly broad but cheap to implement. Similarly, in *Google Spain* and *Glawischnig-Piesczek*,¹²⁰ the CJEU adopted particular content blocking or de-amplification standards without properly considering their impact on speakers or readers and paid most of the attention to consequences for platforms and their economic interests. Yet, the latest case of *Poland* shows that when the CJEU is asked to address freedom of expression directly, it can do so very sensibly.¹²¹

To address this institutional blind spot, the decision-makers must address the remaining shortcomings of the regulatory setup.

One possibility is to permit third-party interventions in cases brought to the CJEU, as is successfully practised in Strasbourg.¹²² This would allow civil society to articulate arguments that were unaccounted for and supplement the lack of representation of some parties. While prior to the DSA, there was no agency to properly represent the interests of speakers and readers, this will change, at least in theory. In practice, it is still questionable to what extent the EU Commission, as the enforcer of the DSA, can properly and credibly reconcile all viewpoints, given that some of them might sometimes be in opposition to the goals that the Commission tries to achieve. But given that under the DSA, at least some administrative decisions will be made by the EU Commission, their judicial review might allow third parties to intervene before the CJEU.¹²³ However, in all other cases before the CJEU that interpret the DSA, including those originating from actions against national regulators, in the years to come some voices will not be heard in Kirchberg. That is unless procedural rules in Luxembourg change.

¹¹⁷ Registry of the Court, Rules of the Court (ECHR), r 44; delineating the procedure for third-party interventions.

¹¹⁸ Protocol on the Statute of the CJEU [2012] OJ C203/72, arts 23 and 23(a).

¹¹⁹ *UPC Telekabel* (n 104).

¹²⁰ *Google Spain* (n 91); Case C-18/18 *Eva Glawischnig-Piesczek v Facebook Ireland Limited* ECLI:EU:C:2019:821.

¹²¹ *Poland* (n 31).

¹²² Matthias Jacobs, Matthias Münder, and Barbara Richter, 'Subject Matter Specialization of European Union Jurisdiction in the Preliminary Rulings Procedure' (2019) 20(8) German Law Journal 1214, 1230–31.

¹²³ Protocol on the Statute of the Court of Justice of the European Union [2012] OJ C203/72, art 40; Rules of Procedure of the General Court OJ L 105, 23 April 2015, pp 1–66, art 143.

PART II

LIABILITY

Introduction to Liability Framework

4.1 Introduction	57	4.3 Two Generations of Rules	63
4.2 History of the ECD	61	4.3.1 The ECD as the first generation	63
		4.3.2 The DSA as the second generation	65

4.1 Introduction

On 22 November 1995, three buses full of policemen stormed the Munich offices of CompuServe, a prominent American company that operated online discussion newsgroups, in a surprise raid.¹ The unsuspecting employees were soon informed that the raid had to do with CompuServe's online groups that were involved in exchanging child abuse material and games harmful to children.² The police officers left empty-handed,³ but the raid worked wonders. Fearing the looming legal consequences, CompuServe felt compelled to take immediate action and demonstrate their willingness to cooperate. The German prosecutor wasted no time in delivering a stern message. CompuServe must take the necessary steps to avoid liability. He sent a list of 200 groups to block.⁴ CompuServe hurried to comply. But the hastily compiled list included a multitude of groups that bore only a vague connection to illegal content. Among the innocent casualties was a group dedicated to discussing breast cancer.⁵ Three months later, CompuServe introduced a primitive filtering software known as CyberPatrol. This software relied on a human-maintained blacklist of URLs specifically designed to block access to any content associated with child abuse material. It soon became apparent that CompuServe's actions were in vain. The German prosecutor remained unsatisfied.

This was the time when the legal troubles of internet companies started mounting. Only a few weeks before the Munich raid, a bailiff, accompanied by two United States (US) members of the Church of Scientology, raided the Amsterdam offices of a Dutch

¹ Nico Ernst, 'Ex-CompuServe-Chef Felix Somm im Interview' *Computerwoche Tec Workshop* (17 May 2000) <<https://www.tecchannel.de/a/ex-compuserve-chef-felix-somm-im-interview,401170>> accessed 3 August 2023.

² *ibid.* (The index of media deemed unsuitable for young persons by the Federal Department for Media Harmful to Young Persons (BPjM) included some computer games, such as Wolfenstein).

³ Michael Kunze, 'The Compuserve Switch-Off of USENET NewsGroups' (6 January 1996) <<http://www.rogeclarke.com/II/Compuserve.html>> accessed 3 August 2023.

⁴ *ibid.*

⁵ Ernst (n 1); Kunze (n 3).

provider, XS4ALL.⁶ As a prelude to a copyright lawsuit for hosting third-party websites, the entourage came to take steps to preserve evidence. Meanwhile, in the US, a District Court held in *Netcom* that a telecommunication company and a bulletin board provider could be liable for users' copyright infringements in yet another case initiated by the Church of Scientology.⁷ In another case, CompuServe's competitor Prodigy was held to be liable for content posted by its users under defamation law because it engaged in content moderation.⁸ The world was already becoming a global village. The cover of *Time* magazine was warning people about 'cyberporn',⁹ and the US Congress was intensely debating the US Communications Decency Act (CDA). This influenced popular opinion in other countries, including Germany.¹⁰

In Munich, despite CompuServe's efforts, the Munich police and prosecutors were not backing down. According to Kunze, a journalist for *Der Spiegel* Magazine, the entire group of German legal professionals had a bigger plan. In his view, the group set out to establish the principle that the providers are responsible for the content of others.¹¹ He later wrote that '[a]ll activities of the Task Force could not have happened if they were not supported by a whole bunch of local prosecutors and judges. Sticking together, chatting, doing favours forms a part of the social life in Munich'.¹²

The results came quickly.

On 26 February 1997, the prosecutor filed a criminal indictment of Mr Felix Somm, the managing director of CompuServe's German branch. To the astonishment of many, in May 1998, a judge of the Munich County Court sentenced Mr Somm to two years of imprisonment on probation and a fine of 100,000 marks,¹³ a sum that, in today's currency, equated to approximately €84,500.¹⁴ Mr Somm was found guilty of complicity in disseminating illegal material and of negligent dissemination of content harmful to minors in the form of then-popular computer games, such as Doom, Heretic, and Wolfenstein 3D. The judge's justification for the harsh judgment was clear—the internet cannot become a lawless space. He wrote:

there is a vital interest of society that technical progress in the teleservices sector *does not lead to the creation of lawless areas* in which such high legal interests as the

⁶ XS4ALL Internet, 'Press Release: Police and Members of Scientology Church Enter Offices of XS4ALL' (5 September 1995) <<https://felipe.home.xs4all.nl/cos/pers.eng.html>> accessed 3 August 2023.

⁷ *Religious Technology Center v Netcom On-Line Communication Services Inc* 907 F Supp 1361 (ND Cal 1995) (*Netcom*).

⁸ *Stratton Oakmont Inc v Prodigy Services Co* 23 Media L Rep 1794 (NY Sup Ct 1995) (*Prodigy*). CompuServe, in contrast, won a similar case in *Cubby Inc v CompuServe Inc* 776 F Supp 135 (SDNY 1991) exactly because it lacked elaborate content moderation policies.

⁹ TIME, 'TIME Magazine Cover: Cyber Porn' (*TIME.com*, 3 July 1995) <<https://content.time.com/time/covers/0,16641,19950703,00.html>> accessed 3 August 2023.

¹⁰ Kunze (n 3).

¹¹ *ibid.*

¹² *ibid.*

¹³ AG München NJW 1998, 2836. See also Brandon Mitchener and Nick Wingfield, 'A Former CompuServe Official Is Convicted in Pornography Case' *Wall Street Journal* (29 May 1998) <<https://www.wsj.com/articles/SB896371751696756000>> accessed 3 August 2023.

¹⁴ Inflation adjusted, using 'German Inflation Calculator to Factor Inflation into Any Calculation' <<https://www.lawyerdb.de/Inflationrate.aspx>> accessed 4 August 2023.

protection of minors and protection against sexually motivated violence are subordinated to purely commercial interests and thus sacrificed ... As managing director, the defendant was responsible for the business division in Germany. It was his responsibility to ensure that German laws were observed. *It was therefore part of his duty of care to ensure that no indexed games were offered to customers in Germany in the proprietary service.* The fulfilment of these duties of care is to be demanded of anyone working in this position in this area ... In view of these at least discernible circumstances, *the defendant should have expected* that indexed games would also be offered in the proprietary game forums as proprietary games of the parent company.¹⁵

Mr Somm's case caused international outrage. The Munich County Court ruling was even more surprising given that in June 1997, after Mr Somm's criminal indictment but before his sentence by the judge, the German legislature adopted a pioneering new law which included two separate liability exemptions—the first of its kind in Europe.¹⁶ Section 5(2) of the 1997 German law (IuKDG) provided that 'service providers are only responsible for third-party content that they make available for use if they are aware of this content and it is technically possible and reasonable for them to prevent its use'.¹⁷ Section 5(3) provided that '[s]ervice providers are not responsible for third-party content to which they merely provide access for use'.¹⁸ The two German liability exemptions entered into effect almost immediately on 1 August 1997.¹⁹ The German government even held a joint European Ministerial Conference with the European Commission in July 1997 in Bonn stressing that 'rules on responsibility should give effect to the principle of freedom of speech, respect public and private interests and not impose disproportionate burdens on actors'.²⁰ The Bavarian judge of the County Court, however, found the federal German legislation to be inapplicable.

While the Munich Regional Court eventually reversed the decision on appeal, it took Mr Somm over two years to clear his name.

Mr Somm's over-reaction to the letter of the prosecutor became one of the first well-known documented cases of what came to be known as 'over-blocking'—the damaging removal of legitimate content caused by providers' cautious response to legal risks. This episode and early US cases provided a strong warning that some explicit legal positioning of digital services might be necessary. XS4ALL, the Dutch provider, noted in its press release following the raid that: 'This whole affair demonstrates the need for clarity concerning the legal position [*sic*] of Internet Providers. ... If we as Internet

¹⁵ AG München NJW 1998, 2836 (emphasis mine).

¹⁶ The US passed its CDA in 1996.

¹⁷ Information and Communication Services Act (Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste) v. 22 July 1997 (BGBl. I, 1870) (IuKDG), art 1, § 5(2).

¹⁸ *ibid* art 1, § 5(3).

¹⁹ It took years for the courts to take German liability exemptions seriously. While police and prosecutors backed off from prosecuting access and hosting service providers for offering their services, civil courts, according to one study, either applied the new rules very reluctantly or overlooked them altogether. See Lothar Determann, 'Case Update: German CompuServe Director Acquitted on Appeal' (1999) 23 UC Law SF International Law Review 109, 119.

²⁰ European Ministerial Conference, 'Global Information Networks: Realising the Potential' (6 July 1997) <http://web.mclink.it/MC8216/netmark/attach/bonn_en.htm> accessed 5 August 2023.

providers are held responsible for what our users say, that will undoubtedly [*sic*] kill freedom of speech on the net.²¹

In the US, Congress had adopted the CDA which, among other things, tried to incentivise content moderation by giving providers near-blanket legal immunity from many types of liability for others.²² Section 230 CDA was proposed by two senators to specifically undo the court ruling in *Prodigy*.²³ The Congress would soon also adopt section 512 of the Digital Millennium Copyright Act (DMCA) in reaction to *Netcom* and other copyright cases.²⁴

In Europe, the European Commission published its communication to the European Parliament and Council in October 1996, explaining that providers will need legal assurances to operate in the internal market properly. The communication stated that:

Internet access providers and host service providers play a key role in giving users access to Internet content. It should not however be forgotten that the prime responsibility for content lies with authors and content providers. It is therefore essential to identify accurately the chain of responsibilities in order to place the liability for illegal content on those who create it ... The law may need to be changed or clarified to assist access providers and host service providers, whose primary business is to provide a service to customers, to steer a path between accusations of censorship and exposure to liability.²⁵

Shortly after the US adopted the DMCA, on 18 November 1998, the European Commission tabled a proposal for a Directive on certain legal aspects of electronic commerce in the internal market—commonly known as the E-Commerce Directive (ECD). This Directive included three liability exemptions modelled after the DMCA but also took inspiration from the German horizontal approach to immunities.

When, in November 1999, the appellate court found that the Munich court's interpretation of criminal negligence was overstretched and that Mr Somm lacked any intent, the world looked very different.²⁶ Laws establishing a new global norm were already being written in Europe and the US. By agreeing to the liability exemptions, all parties exercise self-constraint and do their part to facilitate the emergence of an environment from which the society at large can benefit. This is the essence of the digital social contract. According to it, any criminal, administrative or civil wrongdoing is primarily the wrongdoer's responsibility, and only secondarily, a shared responsibility

²¹ XS4ALL internet (n 6).

²² Only days after the German legislature adopted its new act, the US Supreme Court in June 1997 invalidated much of the Communications Decency Act but left the liability exception in s 230 intact. See *Reno v ACLU* 521 US 844 (1997).

²³ See the historical discussion in Jeff Kosseff, *The Twenty-Six Words That Created the Internet* (Cornell UP 2019) 57ff.

²⁴ *Playboy Enterprises Inc v Frena* 839 F Supp 1552 (MD Fla 1993); *Netcom* (n 7). See also Martin Husovec, 'Rising Above Liability: The Digital Services Act As a Blueprint for the Second Generation of Global Internet Rules' [2023] *Berkeley Technology Law Journal* (forthcoming).

²⁵ Commission, 'Illegal and Harmful Content on the Internet' (Communication) COM(96) 487 final, 12–13.

²⁶ LG München NJW 2000, 1051.

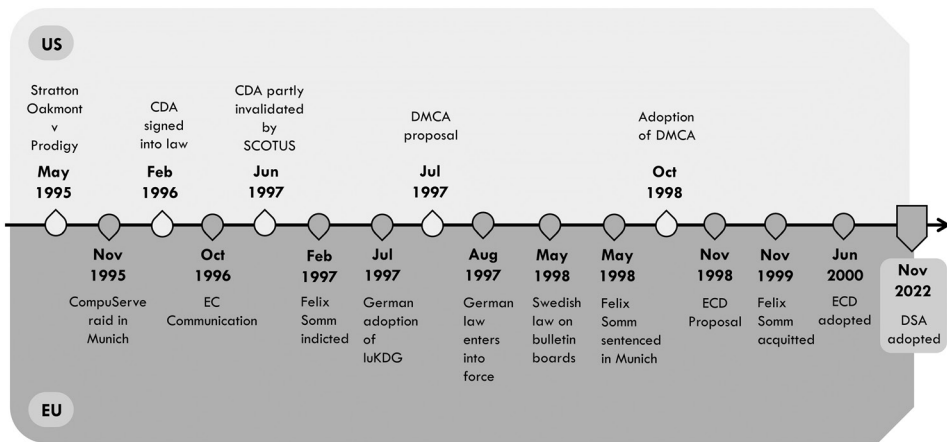


Figure 4.1 Timeline of intermediary liability rules

of other actors, such as providers, civil society, and victims. The shared responsibility means that each one has a role in enforcing the rights.

Even after many years, Mr Somm's story demonstrates the struggles that providers faced during the formative period of 1995–99 and acts as a reminder of the benefits of the existing system. Figure 4.1 shows the historical progression of legal acts.

4.2 History of the ECD

In November 1998, the European Commission tabled a proposal for the ECD. The proposal followed the course outlined in the Commission's 1996 Communication on 'Illegal and Harmful Content on the Internet'.²⁷ While the Jacques Santer Commission prepared the proposal, it was the next Romano Prodi Commission that successfully stewarded it through the legislative process towards its adoption in June 2000. The Member States did not make significant changes to the initial proposal, but they influenced the meaning of the text through additions of various Recitals.

Throughout the legislative process, much effort was expended on resolving the debate on the scope of the country-of-origin principle. In the European Council, several Member States demanded various limitations and clarifications. For the liability exemptions in particular, Sweden wanted a bulletin board exception from the prohibition of general monitoring obligations to be able to keep its newly adopted law on bulletin boards.²⁸ Moreover, several Member States, including Austria, Sweden, and Denmark,

²⁷ Commission, 'Illegal and Harmful Content on the Internet' (Communication) COM (96) 487 final, 12–13.

²⁸ Working Party on Economic Questions (Information Society services), 'Report on Draft European Parliament and Council Directive on Certain Legal Aspects of Electronic Commerce in the Internal Market Dated 11/12 November 1999' (1999) Doc 12667/99 ECO 364 CONSOM 68 CODEC 655, 6 <https://resources.law.cam.ac.uk/cipil/travaux/e-commerce/e-commerce_travaux_complete.pdf#page=316> accessed 5 August 2023; Law on Responsibility for Electronic Bulletin Boards (Lag (1998:112) om ansvar för elektroniska anslagstavlor) (Swedish Bulletin Board Act).

wanted the knowledge test, which only applied to the liability exemption for hosting, to apply to all liability exemptions.²⁹ Denmark also had some competence concerns about the applicability of liability exemptions in the area of criminal liability.³⁰ France argued for mandatory client data retention to accompany the hosting liability exemption.³¹ Ireland proposed to include search engines in the liability exemptions.³²

None of these requests concerning liability exemptions were strong enough to significantly change the European Commission's proposal. However, they led to the introduction of Recitals 42 (passivity), 47 (specific measures), and 48 (duties of care)—all of which greatly influenced the Court of Justice of the European Union's (CJEU) case law on these issues years later.

Article 15(2) and Recitals 42³³ and 48³⁴ were introduced to appease the countries that wanted a knowledge test to underpin all of the liability exemptions. Recital 47 introduced the clarification that 'monitoring obligations in a specific case' are not in any case prohibited.³⁵

An interesting historical aside is that these countries had initially sought to have the knowledge test applied across the board, in part due to 'the potential of future technological developments to permit [non-hosting] intermediaries to monitor the data they transmit' and the resulting effect that 'an exemption from liability might no longer be appropriate'.³⁶ To address these reservations, the revision clause in Article 21(2), which provides for the ability to amend conditions for liability exemptions in light of technical developments, was added.³⁷ The Swedish demand that the bulletin boards should be excluded from the prohibition of general monitoring was mollified by the Commission's argument that the Swedish law does not have to change.³⁸ This is interesting because section 4 of the Bulletin Board Act basically required random checks, although the exact scope was far from clear and the Swedish government itself insisted that it: 'is not intended that the activity of the supplier should be seriously hampered

²⁹ Working Party on Economic Questions (Information Society services) (n 28).

³⁰ *ibid* 8.

³¹ Permanent Representatives Committee, 'Extract of the Summary Record of the 1853rd Meeting of the Permanent Representatives Committee on 17 and 19 November 1999' (1999) Doc 12957/99 Ext 1 CRS/CRP 44 ECO 387 CONSOM 73 CODEC 714, 4 <https://resources.law.cam.ac.uk/cipil/travaux/e-commerce_directive/e-commerce_travaux_complete.pdf#page=325> accessed 5 August 2023.

³² *ibid*.

³³ This was introduced very late in the legislative process in December 1999. Council of the European Union, 'Draft Minutes of the 2233rd Council Meeting (Internal Market) on 7 December 1999' (2000) Doc 13858/99 PV/Cons 83 MI 126, 7 <https://resources.law.cam.ac.uk/cipil/travaux/e-commerce_directive/e-commerce_travaux_complete.pdf#page=370> accessed 5 August 2023.

³⁴ Probably to appease the Swedish delegation, the political agreement was reached in December 1999 to include what has become Rec 48 as a clarification accompanying art 15 ECD, which allows applicability of 'duties of care'. See *ibid* 8.

³⁵ COREPER, 'Outcome of Proceedings Dated 1 December 1999' (1999) Doc 13655/99 ECO 402 CONSOM 76 CODEC 749, 21 <https://resources.law.cam.ac.uk/cipil/travaux/e-commerce_directive/e-commerce_travaux_complete.pdf#page=333> accessed 6 August 2023.

³⁶ COREPER, 'Report on the Draft European Parliament and Council Directive on Certain Legal Aspects of Electronic Commerce in the Internal Market' (1999) Doc 13657/99 ECO 403 CONSOM 77 CODEC 750, 6 <https://resources.law.cam.ac.uk/cipil/travaux/e-commerce_directive/e-commerce_travaux_complete.pdf#page=361> accessed 6 August 2023.

³⁷ *ibid*.

³⁸ *ibid*.

by the act. If the number of messages is so large, that it is too cumbersome to check them all, it can be acceptable to provide an abuse board, to which users can complain of the existence of illegal messages.³⁹ The Swedish request thus probably lead to Recital 48 which vaguely speaks of ‘duties of care’. Denmark’s reservations regarding the legal basis of criminal liability were dismissed by the European Commission’s Legal Service and were not pressed by the other Member States.

The political agreement was reached in February 2000, and the Directive was approved by the European Parliament in June 2000 with a transposition deadline of January 2002. A series of landmark cases on this new system of liability exemptions soon followed—*Promusicae* in 2008,⁴⁰ *Google France* in 2010,⁴¹ *eBay* in 2011⁴² and *YouTube* in 2021⁴³—all decided by the Grand Chamber of the CJEU.

4.3 Two Generations of Rules

The CDA (section 230) and the Digital Millenium Copyright Act (DCMA) (section 512) in the US, the Informations- und Kommunikationsdienste-Gesetz (IuKDG) (section 5) in Germany and the ECD (section 4) in the EU all represent the first generation of digital services regulation. They tackled the crucial question of the time: when is a provider liable for its users’ content? While they offered various responses, ranging from almost ‘never’ to ‘if they acquire knowledge’, they united in the effort to provide assurances to firms about liability risks.

4.3.1 The ECD as the first generation

The first generation of rules regulates the behaviour of platforms by a legal threat of liability for the actions of others; if you do not remove content or behave in such and such way, you might be liable alongside your users. The conditional immunity model⁴⁴ defined roughly two decades of platform regulation in Europe between the

³⁹ The Swedish government provided the quoted text in the proposal to the parliament. Government Bill (1997/98:15) Responsibility for electronic bulletin boards (Ansvar för elektroniska anslagstavlor) <<https://www.regerin.gen.se/contentassets/25d815028bfc4ba4bcef3234291d6ddb/ansvar-for-elektroniska-anslagstavlor/>> accessed 6 August 2023. S 4 of the Swedish Bulletin Board Act says: ‘The supplier of electronic bulletin board shall, in order to be able to fulfill the obligations according to article 5, supervise the service to an extent which is reasonable considering the extent and objective of the service’. According to Rosen, five years after the law was adopted, it was not once applied by the courts. See Jan Rosén, ‘Server Copyright Liability - Notes on the Swedish Act on Liability for Intermediaries and two Recent Decisions of the Swedish Supreme Court’ [2002] 42 Scandinavian Studies in Law 147, 150.

⁴⁰ Case C-275/06 *Productores de Música de España (Promusicae) v Telefónica de España SAU* ECLI:EU:C:2008:54 (*Promusicae*).

⁴¹ Joined Cases C-236/08–C-238/08 *Google France SARL and Google Inc v Louis Vuitton Malletier SA* ECLI:EU:C:2010:159 (*Google France*).

⁴² Case C-324/09 *L’Oréal SA and others v eBay International AG and others* ECLI:EU:C:2011:474 (*eBay*).

⁴³ Joined Cases C-682/18 and C-683/18 *Frank Peterson v Google LLC and others and Elsevier Inc v Cyando AG* ECLI:EU:C:2021:503 (*YouTube and Cyando*).

⁴⁴ The model requiring at least knowledge to trigger liability, Husovec (n 24).

ECD (2000) and the DSA (2022). The legal rules were mostly reduced to coordinating liability for third-party content. During this period, the provider's only legal responsibility was to do everything necessary to avoid liability. Any extra efforts were voluntary and depended mainly on the business environment, public opinion, and political pressures, but very little on additional legal risks.⁴⁵ Thus, the liability system only punished failures of reactive behaviour, and any proactive behaviour was entirely voluntary.

The ultimate value that liability exemptions protect is decentralised speech. The internet's genius is in allowing anyone to speak their minds without seeking approval. The digital ecosystem weakened the power of traditional gatekeepers, such as TV and radio stations, newspapers, and book publishers, over our public sphere. Obviously, this creates challenges because editors were previously deputised to act as filters for the lawfulness, trustworthiness, and quality of information. Now that information is not always edited upfront, providers of digital services are deputised to act as *ex post* quasi-editors by engaging in content moderation. Without editors, the ecosystem shifts from filtering the content's quality upfront to managing its distribution. Even though such expectations towards digital providers reappoint them as gatekeepers, decentralised content is still allowed to flourish unless controls are too tight. And that is exactly why the control cannot be too tight. Imposing incentives that reinstate upfront editorial control automatically takes away the newly gained ability of individuals to speak and read what is not edited.

Without sympathy of the law, there would be no internet as we know it. In a world where technology facilitates decentralisation while the law disincentivises it, no rational actors would have created spaces or tools without editorial control. A liability regime for the actions of others is a key—albeit not the only—incentive to keep the decentralised architecture of the global network afloat.⁴⁶ Unless legislatures want to reinstate editors, some form of conditional immunity (or liability) is necessary. Figure 4.2 depicts the richness of the digital ecosystem and its players.

The ECD provided for three liability exemptions: conduit, caching, and hosting. Each represents a separate type of conditional immunity, that is, legal immunity that requires at least knowledge of providers to allow for liability for others. The conduit immunity is the most generous and applies to infrastructure services like internet access providers. It protects conduits from pressures to block websites or users without court orders. The caching immunity applies to services that facilitate communication flows by temporarily storing the websites of others. It protects caching services from having to act upon illegal content before it is removed from its source. And finally, the most

⁴⁵ Martin Husovec, 'Accountable, Not Liable: Injunctions Against Intermediaries' [2016] TILEC Discussion Paper No 2016-012 <<http://www.ssrn.com/abstract=2773768>> accessed 7 August 2023.

⁴⁶ In the literature, van Schewick argued most convincingly that technical architecture influences innovation and a decentralised environment for speech—Barbara van Schewick, *Internet Architecture and Innovation* (MIT Press 2010). Her work directly relates to the net neutrality debate, which posits that Internet access providers should not engage in discriminatory practices when routing traffic through their networks.

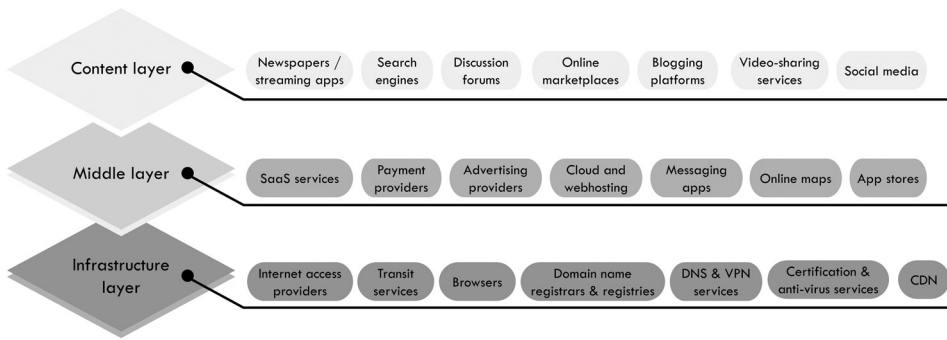


Figure 4.2 The internet tech stack

prevalent is the hosting immunity that protects the application layer of the internet, which stores the content of others. Hosts are protected from liability before they are notified or otherwise learn about illegal content. Given the prevalence of these services, hosting immunity creates the baseline choreography of digital enforcement—that of ‘notice and action’, although more commonly known as ‘notice and takedown’.

4.3.2 The DSA as the second generation

Regulation through liability exemptions has its limits. The horizontal liability exemptions are about creating breathing space for speech and markets while allowing enforceability of the rights of victims, but they do not address specific challenges. The rules of the first generation—sections 230 CDA, 512 DMCA, 4 ECD—all suffer the same insufficiency. They excel at coordinating expectations to encourage investment but fail at offering tools to solve a wide range of societal problems that emerge along with the use of these services. The past years have drawn contours of many societal challenges that require solutions, ranging from the protection of children to problems with hate speech or terrorism and subversive activities that try to attack the basis of our democratic systems.

All these problems are exacerbated by the ‘special features’ of the internet as a medium: its lack of editorial approval, low barriers to entry, including the zero cost of services across the board, the incredible speed and scale of distribution, its broad social and geographical inclusiveness, and resilience of communications. The regulators are thus rightly considering how to address these challenges. As the introduction shows, it is understood at the time of writing that strict liability for someone else’s content is a death sentence for decentralised speech. It means rewinding the clock to the pre-internet area, where editors are responsible for what they make available to readers. Any regulation needed to be more tailored.

To avoid this, the second generation of rules, such as the DSA, does not intend to change the underlying liability for someone else’s content. Instead, they try to create a set of independently enforceable due diligence obligations (Chapter 9.4). Those obligations are of a systemic nature, which means that the prescribed outcomes are owed

to the public.⁴⁷ A violation does not lead to responsibility for the communication of the content of others. It has separate legal consequences. Instead of endlessly trying to redraw the line between editors and mere intermediaries, the DSA spells out the legislature's specific expectations.

The DSA regulates the choreography of digital enforcement, which is guaranteed by liability exceptions. It regulates the process through which content moderation decisions are taken. Actors who have previously earned trust with the quality of their work are asked to be given better treatment. The decision to restrict the content taken by platforms must be explained. Content creators who are affected must be notified and offered reasons for content moderation decisions, which they can appeal to internally and, if necessary, externally. Some providers are asked to think about the risks posed by the design of their services.

This shift in focus from *liability* to *accountability* means the discussion primarily moves to a debate about the right systems and procedures to achieve appropriate aggregate outcomes. The DSA's due diligence obligations treat providers as accountable for operating systems but not liable for the individual harms caused by their users. The liability exemptions make sure that individual harms are not attributed to providers so the debate can move on to how to manage risks. Even the DSA's tool for the largest players, risk mitigation, implies that some failures are inevitable and acceptable. This is in stark contrast with how rules that set the basic legal expectations for liability operate. When liability rules are violated, platforms are exposed to liability, regardless of whether something is an occasional slip-off or a systemic problem.

The DSA's liability exemptions and accountability obligations are mutually compatible as long as they are based on the same principles. One can easily imagine accountability obligations that undermine liability exemptions. For instance, a rule that providers must verify the authenticity of all goods that other people trade on the provider's platform also clashes with the liability arrangements. Firstly, any fine enforcing it is a form of liability imposed for storing third-party information—that is, a liability for failing to verify. Secondly, it imposes a general obligation to monitor the authenticity of the content. Thirdly, it creates an obligation to acquire knowledge, which removes the applicability of the liability exemption for hosts.⁴⁸

Thus, while accountability is inherently proactive because it asks providers to think about potential risks in advance, it must remain targeted. Otherwise, accountability risks turning into strict liability. The DSA's approach is to keep relying on reactive liability exemptions while increasing accountability in ways that avoid general monitoring. This means that accountability is always targeted to duties in specific cases. In the legal design, to assure this is the task of the prohibition of general monitoring, which I discuss next.

⁴⁷ But it can still be privately enforced (ch 19).

⁴⁸ In the European system, the European legislature is the only one that can undermine liability exemptions. The DSA pre-empts any national attempts to impose such due diligence obligations.

Prohibition of General Monitoring Obligations

5.1 Introduction	67	5.3 Origins of the GMOP: From the ECD to the DSA	81
5.2 Scope of the GMOP	69	5.4 The GMOP as a Balancing Tool	83
5.2.1 What is an 'obligation'?	70	5.5 The GMOP as a Harmonisation Tool	87
5.2.2 What is 'monitoring'?	71	5.6 The GMOP vs the Member States	90
5.2.3 When is it 'general'?	72		

5.1 Introduction

The general monitoring obligations prohibition (GMOP) is an important principle of European Union (EU) digital services regulation. It protects *content creators* and *gatekeepers* of user-generated content, similar to how media privileges¹ protect *journalists* and *news organisations* when they publish editorial content. It limits what can be expected from regulatory enforcement by stipulating that relevant providers should not be required to take excessive and indiscriminate actions that could legitimately affect all content creators. The GMOP acts as an ordering principle for national and EU legislation on digital services by distributing responsibility in the digital ecosystem. Over the years, the GMOP has obtained 'quasi-constitutional' status because it started serving as a legislative and human-rights ceiling on digital regulation.

Originally, the GMOP was mainly intended to double down on the policy rationale behind the liability exemptions.² The knowledge-based exemptions cannot logically function if there is a concurrent obligation to obtain knowledge.³ Liability exemptions incorporate the idea that the responsibility for correcting wrongdoing in the digital ecosystem ought to be *shared* between different participants. It should primarily fall on content creators themselves and only secondarily on victims and providers or state authorities and civil society.

¹ See Damian Tambini, 'What is Journalism? The Paradox of Media Privilege' (2021) 5 European Human Rights Law Review 523, 537: 'Journalism is made possible by a variety of privileges and protections for both the activities of public interest newsgathering and the status of journalism.'

² The European law owes its existence to s 512(m) United States (US) Digital Millennium Copyright Act (DMCA). See s 512(m) DMCA: 'Nothing in this section shall be construed to condition the applicability of subsections (a) through (d) on—(1) a service provider monitoring its service or affirmatively seeking facts indicating infringing activity, except to the extent consistent with a standard technical measure complying with the provisions of subsection (i); or (2) a service provider gaining access to, removing, or disabling access to material in cases in which such conduct is prohibited by law.'

³ Case C-18/18 *Eva Glawischnig-Piesczek v Facebook Ireland Limited* ECLI:EU:C:2019:458, Opinion of AG Szpunar, paras 36, 41.

The GMOP forms the central part of the *digital social contract*. Under this digital social contract, victims of illegal content (or someone acting on their behalf) assist in finding and notifying illegal content, and the providers are usually expected to act upon the received notifications or court orders if they wish to be exempted from liability. The underlying logic is the following: imposing an obligation on providers to constantly vet user content would push them to become editorial media, thus reducing the instances where all content is user-generated. Crucially, the GMOP prohibits the Member States from legislating obligations that would significantly reverse the baseline distribution of tasks as outlined in the liability exemptions. For instance, legislation requiring providers to review 10% of the uploaded content manually would violate the GMOP because it reverses the baseline distribution of liability.

Only the EU itself can modify this digital social contract for European citizens. That said, even the EU legislature must consider the fundamental rights constraints discussed in Chapter 3. These constraints do not allow legislatures to make far-reaching changes from the red lines drawn by the Court of Justice of the European Union (CJEU).

Prior to Article 8 Digital Services Act (DSA), its predecessor, Article 15(1) E-Commerce Directive (ECD), provided that:

Member States shall not impose a general obligation on providers, when providing the services covered by [one of the liability exemptions], to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.

Article 15(2) ECD reassured that the previous prohibition did not limit the possibility of Member States imposing notification, communication, or disclosure duties where they might be required from such providers. Recital 47 ECD clarified that Article 15 ECD does not stand in the way of ‘specific’ monitoring.

Back in 2000, when ECD was adopted, the GMOP followed a double objective: on the one hand, it intended to harmonise diverging national rules, and on the other hand, it aimed to protect an incipient industry from burdensome or impossible obligations which would stifle market entry. The ECD explained that: ‘both existing and emerging disparities in Member States’ legislation and case law concerning the liability of service providers acting as intermediaries prevent the smooth functioning of the internal market, in particular by impairing the development of cross-border services and producing distortions of competition ...’⁴ The prohibition of general monitoring obligations was understood as the other side of the coin of liability exemptions. The drafters argued that the liability exemption would have been deprived of any effect if providers could be obliged by the Member States to identify illegal items at the source anyway.⁵ Without the GMOP, for instance, the limitation that liability can be imposed only upon

⁴ European Parliament and Council Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2000] OJ L178/1 (ECD), Rec 40.

⁵ Emmanuel Crabit, ‘La Directive Sur Le Commerce Électronique. Le Projet “Méditerranée” (2000) 4 Revue du Droit de l’Union Européenne 749, 815.

actual knowledge could have been circumvented by imposing non-monetary obligations to review everything uploaded to the services indiscriminately and manually. Furthermore, it would have been impossible for providers to avail themselves of the liability exemption dependent on a lack of knowledge if they had a concurrent obligation to know. Without the GMOP, the liability limitations would have a huge blind spot.

While ECD had a strong economic angle, it did not entirely ignore the liability exemptions' role in the context of fundamental rights.⁶ The CJEU quickly linked the GMOP in Article 15 ECD to the fundamental rights protection of users by highlighting the need to protect them from interference by private and public actors. This close link was identified early on,⁷ and it was strengthened in the recent case law of the CJEU, giving this provision a quasi-constitutional position; that is, a position that allows the legislature to slightly move behind its statutory red lines, but also not too far.

While the GMOP remains central to digital regulation, precisely what it entails is disputed. Article 8 DSA is the only provision in the Commission's proposal for the DSA that was not subject to any *substantive* change by the co-legislators—even though the issue was extensively debated. Some stakeholders tried to water down the language used in the ECD; others attempted to strengthen it. The tussle resulted in no material change for the provision. This demonstrates that everyone eventually felt that if they could not bend the provision their way, sticking with the Court's interpretation was the preferable way forward.

5.2 Scope of the GMOP

The last two decades since the adoption of the ECD led to seven CJEU cases dealing with the GMOP provision.⁸ The GMOP in Article 15 ECD often played a very important role in defining the outcomes, sometimes in unexpected ways. Given this central role, it is perhaps a little surprising that the actual contours of the provision remain largely disputed to this day. While the consensus around the wording of the DSA renewed the democratic mandate of the GMOP, the divergence of views on interpreting this provision will continue to exist. Stakeholders mostly agree on it 'in principle', but their exact views differ.

To identify what the GMOP means, it is necessary to clarify what an 'obligation' means, which qualifies as 'monitoring' (or 'fact-finding') and when it is 'general'.

⁶ ECD, Rec 46.

⁷ Case C-324/09 *L'Oréal SA and Others v eBay International AG and Others* ECLI:EU:C:2011:474 (*eBay*), para 139 ('... a general monitoring obligation would be incompatible with Article 3 of Directive 2004/48, which states that the measures referred to by the directive must be fair and proportionate and must not be excessively costly'). It was addressed more explicitly in *SABAM* and *Scarlet Extended*, see Case C-360/10 *SABAM v Netlog NV* ECLI:EU:C:2012:85 (*SABAM*) and Case C-70/10 *Scarlet Extended SA v SABAM* ECLI:EU:C:2011:771 (*Scarlet Extended*). In *Glawischnig*, the AG explicitly highlighted the link, although the court does not mention this, see Case C-18/18 *Eva Glawischnig-Piesczek v Facebook Ireland Limited* ECLI:EU:C:2019:821.

⁸ *eBay* (n 7); *Scarlet Extended* (n 7); *SABAM* (n 7); Case C-314/12 *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH* ECLI:EU:C:2014:192; Case C-484/14 *Tobias McFadden v Sony Music Entertainment Germany GmbH* ECLI:EU:C:2016:689; *Glawischnig* (n 7); Case C-401/19 *Republic of Poland v European Parliament and Council of the European Union* ECLI:EU:C:2022:297.

5.2.1 What is an ‘obligation’?

The GMOP covers every type of obligation. Thus, it covers any measure of the state, be it of the judiciary, legislature, or executive. The obligation can be a decision in an individual case, such as an order or generally worded legislation. The crucial element is that the Member States and the respective EU bodies give those obligations some authority. In contrast, political demands communicated in the media without a proper legal basis are unlikely to qualify as obligations. Understandably, there is a large grey zone of political coercion when enforcement authorities might ask providers to ‘do more’ by means of ‘voluntary measures’. The GMOP, in my view, limits any threats by authorities that have some legal credibility, ie those that are at least arguably enforceable. Thus, an authority of a Member State regulating digital content and demanding what amounts to general monitoring would violate Article 8 DSA, but a Member of the European or national parliament demanding the same would not.

Typical obligations imposed by *authorities* are legal orders issued by administrative authorities, criminal courts, or civil courts. The types of measures can range from website blocking, blocking of accounts, payments, freezing user privileges, removing or disabling content, delisting search results, preventing the reappearance of some content or recurrence of some conduct, limiting access to some services, or storing some data about third parties. Typical obligations imposed by *legislatures* are legal mandates to block accounts, remove or disable content, prevent the reappearance of content or recurrence of conduct, store data about third parties, or best efforts types of obligations to perform various checks. Compared to the situation before the DSA, many potential obligations of this kind are now harmonised by the DSA’s due diligence obligations. Pre-emption can also come from other parts of the DSA (Chapter 17).

Given that the change of wording introduces a passive form (‘no general obligation to monitor ... shall be imposed’), one open question is to what extent the principle binds non-state actors or limits public-private arrangements. The CJEU will undoubtedly have to clarify this. Two basic constellations are possible: first, an obligation is *imposed unilaterally* (eg an app store imposes it on its clients, the apps), or second, an obligation is *individually negotiated* (eg providers and interested non-governmental organisations (NGOs) agree on it in their fully negotiated contracts). In my view, given that only *voluntary* general monitoring is permitted, using contractual freedom to negotiate and solidify the same measures individually should be equally possible. Those measures are not subject to Article 8 DSA. On the other hand, Article 8 DSA should prevent any ‘obligations’ that are ‘non-voluntary’. Recital 26 reminds us that ‘[v]oluntary actions should not be used to circumvent the obligations of providers of intermediary services under this Regulation’. Thus, for instance, if an app store implements general monitoring in its capacity as a very large online platform (VLOP) trying to satisfy the DSA’s risk management obligations, the resulting obligations imposed on app developers are not voluntary. They originate from the legal mandate the app store internalises in response to Article 34 DSA.

5.2.2 What is ‘monitoring’?

From the reported history behind the ECD, it is evident that Article 15 ECD was intended to cover measures ranging from broad filtering of hosted information to area obligations, such as those adopted to protect minors.⁹ The term covers all kinds of general measures, including those that did not request monitoring by name but have the same effect.¹⁰ For instance, an abstract obligation ‘to protect minors’ can mean the creation of tools for parents but also an obligation to observe and evaluate users to assess their age. Only the latter obligation would qualify as monitoring. In the context of the DSA, this ‘by object or effect’ distinction is now also reflected in the words of ‘de jure or de facto’ in Recital 30 DSA. The European Parliament demanded clarification during the negotiations.

The GMOP has two prongs: a) monitoring the information stored or transmitted, and b) actively seeking facts or circumstances indicating illegal activity. The CJEU case law to date is silent on the difference. Fact-finding seems to imply obligations involving human judgement while monitoring mostly implies using machines.¹¹ Fact-finding implies discovering, acquiring, and establishing facts by someone. Monitoring, in contrast, customarily means an act of observing or recording. It thus implies surveillance over someone or something by either people or machines. Taken together, monitoring practically means surveillance of users and their content on the digital service.

When a measure targets past actions or static targets, such as removing specific illegal content on a URL, there is usually very little concern that this would amount to ‘monitoring’. In such cases, the content can be identified with precision using a URL or an Internet Protocol (IP) address and domain name. To comply, the provider does not usually have to monitor anything. It simply removes specific content, blocks accounts, or deregisters a domain name. In contrast, the greatest difficulty comes with measures that attempt to police *future lawless acts or moving targets* on a particular service.¹² In order to fulfil such orders, providers must usually ‘monitor the information which [they] transmit or store’ or ‘actively to seek [new] facts or circumstances indicating illegal activity’. This typically applies to orders asking for the ‘stay-down’ of information, ‘prevention of re-appearance’, or those requiring ‘dynamic updating’.¹³

The liability chapter of the DSA is based on the idea that facts are gathered and evaluated usually by victims, and hosting providers only check their requests for manifest illegality.¹⁴ When orders or statutory obligations ask providers to continue to acquire

⁹ Crabit (n 5) 815.

¹⁰ Arguably, this also means that imposing direct liability for illegal content hosted on its service usually represents a breach of the liability exemption and the general obligation to monitor.

¹¹ This seems to be suggested by the AG in Case C-314/12 *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH* ECLI:EU:C:2013:781, Opinion of AG Cruz Villalón, para 78.

¹² Martin Husovec, ‘Holey Cap! CJEU Drills (yet) Another Hole in the e-Commerce Directive’s Safe Harbours’ (2017) 12(2) *Journal of Intellectual Property Law & Practice* 115, 119.

¹³ For the practice in the Member States, see EUIPO and CEIPI, *Study on Dynamic Blocking Injunctions in the European Union* (EUIPO 2021) <<https://op.europa.eu/s/yX4r>> accessed 21 August 2023.

¹⁴ See ch 7.

new information, they modify liability exemptions because first, they oblige providers to know, and then punish them for knowing. The problem does not arise, however, if the measure is prospective, but the new information continues to be supplied by victims. This is the case for dynamically updated website blocking injunctions that change their target after they are granted by judges.¹⁵ The key consideration in such cases is the question of oversight.

The DSA does not make all monitoring or fact-finding obligations illegal. However, it allows them only if they are specific, ie if they are properly targeted. One can clearly draw an analogy with data retention. Article 8 DSA prevents indiscriminate surveillance of digital content and people using the internet but permits the legitimate targeted actions of authorities.¹⁶ Surveillance measures imposed on providers to fight illegal content or behaviour online are not entirely prohibited, but they must be administered by authorities, be proportionate and strictly targeted—at least unless the EU legislature says otherwise. Thus, a court order asking providers to preserve or release evidence, or observe a specific user, easily satisfy the requirements of Article 8 DSA. However, once the orders extend to the broader digital public, the difficulties start.

5.2.3 When is it ‘general’?

Based on Recital 47 ECD, pre-DSA case law quickly distinguished specific and general monitoring. While specific monitoring is permitted, general monitoring is prohibited by Article 15 ECD. Where the boundary lies exactly, however, has become a longstanding contention between the CJEU and Member States, and even within the CJEU. Over the years, the EU legislature adopted legislation that reiterates the GMOP in very different sectorial legal instruments to complicate things further. It is, therefore, possible that the GMOP carries different meanings in different contexts.

Early case law interpreted general monitoring as measures that concern large parts of the user base of a particular service. Thus, searching content posted by everyone would be seen as general, even if it was performed to find something particular (eg an image depicting the abuse of a particular child). Thus, knowing what needle you are looking for does not justify searching the entire haystack. The interpretation was devised first by the Grand Chamber of the CJEU in *L’Oréal v eBay* in 2011,¹⁷ and it was then applied by a five-judge chamber in the *SABAM* and *Scarlet Extended* cases in 2012.¹⁸

¹⁵ See, for instance, the decision of the District Court of Hague, Rb Den Haag 22 September 2017, Case C/09/535341, ECLI:NL:RBDHA:2017:10789 (*Stichting Brein/Ziggo & XS4ALL*), para 5.3 (‘orders [an ISP] in the event that TPB starts operating via other/additional IP addresses and/or (sub)domain names ... to block and keep blocked the access of their customers to these ... within three working days after delivery by Brein’).

¹⁶ A similar opinion is presented by Folkert Wilman, ‘Two Emerging Principles of EU Internet Law: A Comparative Analysis of the Prohibitions of General Data Retention and General Monitoring Obligations’ (2022) 46 CLS Review 105728.

¹⁷ *eBay* (n 7) para 139.

¹⁸ *SABAM* (n 7); *Scarlet Extended* (n 7).

In *eBay*, the CJEU ruled that an injunction imposed on an online marketplace, as a type of measure, ‘cannot have as its object or effect a general and permanent prohibition on the selling, on that marketplace, of goods bearing those trademarks.’¹⁹ The Court applied the standard proposed by AG Jääskinen,²⁰ and it accepted that measures consisting of a suspension of accounts or measures enabling identification of its sellers would be sufficiently specific.²¹ The Court noted that the two mentioned measures are not the only ones possible.²² The German courts took this to mean that the applied standard is not exhaustive,²³ which was arguably wrong because the CJEU clearly referenced²⁴ the following standard properly articulated by AG Jääskinen:

An appropriate limit for the scope of injunctions may be that of a double requirement of identity. This means that the infringing third party should be the same and that the trade mark infringed should be the same in the cases concerned. Hence, an injunction could be given against an intermediary to prevent the continuation or repetition of an infringement of a certain trade mark by a certain user. Such an injunction could be followed by an information society service provider by simply closing the client account of the user in question.²⁵

In *Sabam* and *Scarlet Extended*, a national court considered whether an internet access provider and a social networking platform could be asked to install filtering systems. The CJEU concluded that this would involve the ‘systematic analysis of all content and the collection and identification of users’ IP addresses from which unlawful content on the network is sent.’²⁶ This was viewed as too general. On the other hand, in *UPC Telekabel*, the CJEU accepted website blocking measures as a legitimate and specific type of monitoring when it followed the advice given by the AG:

It would constitute such an inadmissible measure if the court had ordered the ISP actively to seek copies of the infringing page among other domain names or to filter all the data carried in its network in order to ascertain whether they constitute transfers of specific protected film works and to block such transfers. However, such a measure is not in issue in the present case. Rather, the referring court is required to decide on the blocking of a specific website. The measure therefore does not infringe Article 15(1) of Directive 2000/31.²⁷

¹⁹ *eBay* (n 7) para 140.

²⁰ Case C-324/09 *L’Oréal SA and Others v eBay International AG and Others* ECLI:EU:C:2010:757, Opinion of AG Jääskinen, para 182.

²¹ *eBay* (n 7) paras 141–42.

²² *ibid* paras 141–43.

²³ See German Federal Supreme Court cases, BGH v 22 July 2010 – I ZR 139/08 (*Kinderhochstühle im Internet I*); BGH v 12.07.2012 – I ZR 18/11 (*Alone in the dark*); BGH v 15 August 2013 – I ZR 80/12 (*File-Hosting-Dienst*); BGH v 16 May 2013 – I ZR 216/11 (*Kinderhochstühle im Internet II*).

²⁴ *eBay* (n 7) para 141, pointing to the part with standard.

²⁵ *eBay* (Opinion of AG Jääskinen) (n 20) para 182.

²⁶ *Scarlet Extended* (n 7) para 40; *SABAM* (n 7) para 38.

²⁷ *UPC Telekabel* (Opinion of AG Cruz Villalón) (n 11) para 78, suggests this.

This reasoning was not without problems, in particular, because website blocking is an enforcement goal that can be implemented in a number of ways. Some blocking can take the form of specific monitoring (as defined by *eBay*), such as when a Domain Name System (DNS) entry is blocked. However, Deep Packet Inspection (DPI) based blocking, which scans all data carried in the network as it passes an inspection point, constitutes indiscriminate monitoring. The CJEU did not consider this point and simply approved website blocking as an enforcement goal.

In the *McFadden* case, concerning a wi-fi hotspot, AG Szpunar argued that ‘a measure requiring the owner of an internet connection to examine all communications transmitted through that connection’ would ‘clearly conflict with the prohibition on imposing a general monitoring obligation.’²⁸ In his view, ‘in order to constitute a monitoring obligation “in a specific case”, such as is permitted under Article 15(1), the measure in question must be limited in terms of the *subject* and *duration* of the monitoring, and that would not be the case with a measure that entailed the examination of all communications passing through a network.’²⁹ Thus, Szpunar proposed to use the subject and duration as the limiting principles. The Court accepted the conclusion of the AG’s analysis and ruled that ‘examining all communications passing through an internet connection’ is a violation of the GMOP without explicitly referring to the two conditions.³⁰ It should be recalled that the Court already spoke of ‘general and *permanent*’ obligations as being incompatible in *eBay*. Therefore, AG Szpunar’s view had a firm footing in the case law.

In *Tommy Hilfiger*, a case dealing with the obligation in the offline context (preventive obligations imposed on a flea market operator), the Court restated its case law, weaving in also requirements of the IP Enforcement Directive, as follows:

Lastly, the Court held that injunctions must be equitable and proportionate. They must not therefore be excessively expensive and must not create barriers to legitimate trade. Nor can the intermediary be required to exercise general and permanent oversight over its customers. By contrast, the intermediary may be forced to take measures which contribute to avoiding new infringements of the same nature by the same market-trader from taking place.³¹

The ‘general and *permanent* oversight of customers’ is equivalent to ‘general and permanent monitoring’ known from *eBay*. Similarly, in line with that ruling, the decision seemed to again suggest that the only specific oversight that would be acceptable is one limited to ‘avoiding new infringements of the same nature by the same market trader from taking place’.

²⁸ Case C-484/14 *Tobias McFadden v Sony Music Entertainment Germany GmbH* ECLI:EU:C:2016:170, Opinion of AG Szpunar, para 132.

²⁹ *ibid.*

³⁰ *McFadden* (n 8) para 87.

³¹ Case C-494/15 *Tommy Hilfiger Licensing LLC and Others v Delta Center* ECLI:EU:C:2016:528, para 34.

This case law was largely consistent, although not universally followed, until 2019, when the CJEU decided the *Glawischnig* case.³² Before I explain that ruling, it is crucial to understand the precedential weight of all these decisions. The only Grand Chamber ruling from the cases above is *eBay*. All other rulings, including *Glawischnig*, are ‘only’ five-judge rulings. In *SABAM* and *Scarlet Extended*, the judge rapporteur was one of the leading copyright judges, Malenovský.³³ In the only Grand Chamber judgment, *eBay*, the rapporteur was another leading IP judge, Ilešič. The *Glawischnig* ruling was authored by Malenovský just before he retired from the bench.³⁴

In *Glawischnig*, the CJEU accepted that specific monitoring could also entail automated tools applied to the entire user base to locate and block a specific infringement. If the needle sought was specifically identified (eg a website or a specific piece of content), the haystack could span the entire service. The Court argued that if the *instructions* for the continuous search were specific enough, the analysis of all content on the service would not be against the GMOP. The important caveat was that the case, unlike all earlier IP cases, concerned defamation, and the national measure subject to scrutiny was a judgment spelling out such instructions and identifying which exact expressions were illegal. Thus, the obligations resulted from a judge applying the law to specific facts and instructing the platform on what exact content must be removed and prevented. This was a clear shift from the Court’s previous position. AG Szpunar’s opinion was willing to impose future filtering of content only upon the same user—thus searching only in a related haystack.³⁵

The five-judge chamber explained its new position as follows:

(41) It follows therefore that, in order for an injunction which is intended to bring an end to an illegal act and to prevent it being repeated, in addition to any further impairment of the interests involved, to be capable of achieving those objectives effectively, that injunction must be able to extend to information, the content of which, whilst essentially conveying the same message, is worded slightly differently, because of the words used or their combination, compared with the information whose content was declared to be illegal. Otherwise, as the referring court made clear, the effects of such an injunction could easily be circumvented by the storing of messages which are scarcely different from those which were previously declared to be illegal, which could result in the person concerned having to initiate multiple proceedings in order to bring an end to the conduct of which he is a victim ...

³² *Glawischnig* (n 7).

³³ For the analysis of how the judges start de facto specialising, see Eleonora Rosati, *Copyright and the Court of Justice of the European Union* (2nd edn, OUP 2023).

³⁴ The Court held that a website blocking measure does not have to specify the means as long it targets a specific website. However, this could also mean that the measure is only specific under the old understanding (eg domain name blacklisting) but also includes measures that scan the entire contents of transmitted communications (eg DPI technology to spot the targeted website). This aspect was later criticised by other members of the Court, such as the AG, see *McFadden* (Opinion of AG Szpunar) (n 28).

³⁵ *Glawischnig* (Opinion of AG Szpunar) (n 3) para 75.

(45) In light of the foregoing, it is important that the equivalent information referred to in paragraph 41 above contains specific elements which are properly identified in the injunction, such as the name of the person concerned by the infringement determined previously, the circumstances in which that infringement was determined and equivalent content to that which was declared to be illegal. Differences in the wording of that equivalent content, compared with the content which was declared to be illegal, must not, in any event, be such as to require the host provider concerned to carry out an independent assessment of that content.

(46) In those circumstances, an obligation such as the one described in paragraphs 41 and 45 above, on the one hand—in so far as it also extends to information with equivalent content—appears to be sufficiently effective for ensuring that the person targeted by the defamatory statements is protected. On the other hand, that protection is not provided by means of an excessive obligation being imposed on the host provider, in so far as the monitoring of and search for information which it requires are limited to information containing the elements specified in the injunction, and its defamatory content of an equivalent nature does not require the host provider to carry out an independent assessment, since the latter has recourse to automated search tools and technologies.³⁶

The decision was immediately understood as a departure by other AGs³⁷ and academic commentators.³⁸ According to Angelopoulos and Senftleben,³⁹ however, its reach should remain confined to defamation and be understood as chipping away from the baseline *eBay* standard only when judges issue specific instructions. Thus, even the new lowered standard, in their view,⁴⁰ does not permit national legislatures to use measures that would operate without judicial authorisation in each case.

The major difficulty with *Glawischnig* is that it does not consider the limits of the potentially continuous order. In the analogous online world, few judges would issue permanent search warrants without oversight. A warrant targeting a company that orchestrates public and private communications would be unthinkable without due consideration given to time and tailoring of the order's scope to avoid overreaching. The Court in *Glawischnig* refused to engage on all these points because it remains silent on what additional safeguards, if any, are required to grant the order.

A few months after *Glawischnig*, the CJEU issued a Grand Chamber decision on a related issue. In *Poland v Council/EP*, the Court reinforced the logic behind the *Glawischnig* ruling.⁴¹ Here, the Court scrutinised an EU legislation that 'required to

³⁶ *Glawischnig* (n 7) paras 41, 45, and 46 (emphasis mine).

³⁷ Case C-401/19 *Republic of Poland v European Parliament and Council of the European Union* ECLI:EU:C:2021:613, Opinion of AG Øe, paras 112–13; Daphne Keller, 'Facebook Filters, Fundamental Rights, and the CJEU's *Glawischnig-Piesczek* Ruling' (2020) 69(6) *Journal of European and International IP Law* 616.

³⁸ Christina Angelopoulos and Martin Senftleben, 'An Endless Odyssey? Content Moderation Without General Content Monitoring Obligations' (2021) <<https://ssrn.com/abstract=3871916>> accessed 1 August 2023.

³⁹ *ibid* 18, 22.

⁴⁰ *ibid* 4.

⁴¹ *Poland* (n 8).

use automatic recognition and filtering tools⁴² at the mere request of right holders. According to the Court, although the GMOP was mentioned in the legislation, it was not violated but rather acted as a safeguard. The Court explained it as follows:

Fourthly, by stating, in terms similar to those employed in Article 15(1) of Directive 2000/31 in respect of that directive, that the application of Article 17 of Directive 2019/790 must not lead to any general monitoring obligation, Article 17(8) of that directive provides an *additional safeguard for ensuring that the right to freedom of expression and information of users of online content-sharing services is observed*...⁴³

Thus, the Court accepted that the entire user base of a video-sharing service can be subject to monitoring and that the specific instructions do not have to be issued by a court. On the one hand, the Court confirms that the GMOP is not violated if the specific instructions come from individuals without pre-existing judicial determination. On the other, unlike judicial injunctions, the legal basis was an act of Union law that also included additional safeguards, where a restatement of the GMOP only served as one of such safeguards. In other words, while the principle of general monitoring was invoked by the state, the legislation was not that of the Member State but the Union, and it was accompanied by additional safeguards. In my view, for the Court, this spoke in favour of loosening up the GMOP standard since there was no concern that the Member States would fragment the single market or that the national authorities do not provide some level of supervision.

The main focus of CJEU's judgment in *Poland* is on strict targeting of measures and the level of errors. The Court notes that filtering and blocking upon upload constitutes a prior restraint and thus cannot lead to the blocking of legal content. The technology can be used but must 'distinguish adequately between unlawful content and lawful content'.⁴⁴ This seems non-negotiable for the Court. The Court in *Poland* notes that the technology put in place must also comply with 'an additional safeguard'.⁴⁵ It must achieve such adequacy without 'an independent assessment of the content' of facts or law. In my view, this means that machines must be capable of satisfying the standard without human involvement. Here is how the Court expresses it:

90 ... That clarification means that the providers of those services *cannot be required to prevent the uploading and making available to the public of content which*, in order to be found unlawful, *would require an independent assessment of the content* by them in the light of the information provided by the rightholders and of any exceptions and limitations to copyright (see, by analogy, judgment of 3 October 2019, *Glawischnig-Piesczek*, C-18/18, EU:C:2019:821, paragraphs 41 to 46).⁴⁶

⁴² *ibid* para 54.

⁴³ *ibid* para 90 (emphasis mine).

⁴⁴ *ibid* 86; *Scarlet Extended* (n 7) para 52; *SABAM* (n 7) para 50.

⁴⁵ *Poland* (n 8) para 90.

⁴⁶ *ibid* (emphasis mine).

And this is the referenced text from *Glawischnig*:

46 In those circumstances, an obligation ... appears to be sufficiently effective for ensuring that the person targeted by the defamatory statements is protected. On the other hand, that protection is not provided by means of an excessive obligation being imposed on the host provider, in so far as the monitoring of and search for information which it requires are limited to information containing the elements specified in the injunction, and its defamatory content of an equivalent nature *does not require the host provider to carry out an independent assessment, since the latter has recourse to automated search tools and technologies*.⁴⁷

In my view, this means that the limit of the GMOP is what the technology in question can do *autonomously*.⁴⁸ The Court understands independent assessment as an assessment of facts or law which requires recourse to non-automated tools, which can only mean human judgement. The reason is linguistic but also teleological. If the same need for assessment is triggered by a notification, it would clearly be labelled as an independent assessment. Moreover, *if* an upfront obligation to review uploaded content by humans is illegal, it should not make any difference *how* the sample for manual review is generated. Thus, if it is illegal to mandate humans to do sample checks a priori, the same should be true if such sample checks are mandated to sort out errors generated by machines.

Only the machine-only configuration does not increase the stock of knowledge. Whatever a machine sees does not lead to actual knowledge of the provider and thus cannot lead to liability. The opposite reading, ie that faulty technology can generate many false positives that humans must review even only for obvious errors, would mean that those generated false positives might lead to actual knowledge and thereby strip providers of liability exemptions exactly because they are reviewed by humans—the very point that the GMOP tries to prevent.

Even in the context of Article 17 of the Copyright in the Digital Single Market (CDSM) Directive, the technology used must be precise enough. While the Court does not go into the details, this also has consequences for what can be subject to such user-base-wide orders. If infringements cannot be identified and evaluated with a negligible margin of error, there can be no expectation that machines can meaningfully help in uncovering them. This is why I think that the Court is permitting user-base-wide measures only for ‘automatable infringements’.⁴⁹

⁴⁷ *Glawischnig* (n 7) paras 45–46 (emphasis mine).

⁴⁸ Martin Husovec, ‘Mandatory Filtering Does Not Always Violate Freedom of Expression: Important Lessons from *Poland v Council and European Parliament*’ (2023) 60(1) Common Market Law Review 173.

⁴⁹ I have previously developed this concept to explain when infringements can be spotted by technology with a negligible margin of error: Martin Husovec, ‘The Promises of Algorithmic Copyright Enforcement’ (2018) 42(1) Columbia Journal of Law & the Arts 53.

Thus, if humans must get involved to complement automation to assure the adequacy of error rates, their involvement rightly triggers the GMOP. While this reading is intuitive, it is not followed by some Member State courts.⁵⁰

So—where does this leave us?

It is indisputable that the CJEU gradually broadened its standard for what constitutes permissible monitoring under Article 15 ECD. In my view, the Court is currently moving away from user-specific tailoring to a more flexible test. Arguably, three main factors determine whether monitoring is general and prohibited, or specific and allowed: (a) specificity of instructions, (b) adequate automatability of implementation, and (c) existence of safeguards. The maximisation of these factors leads to strict targeting for speech, privacy and data protection concerns, and proportionality for the right to conduct business.

Specificity of instructions requires that a legal mandate (an order or law) must specify whose rights are protected, which exact rights, and which infringements must be prevented. The type of violation subject to the request must be sufficiently narrow. For instance, the request cannot concern just any violation of personality rights but must be limited to the same or almost identical expressions of already identified offensive comments. While the Court does not require one specific technological implementation, it seems to insist that at least the enforcement goals, such as blocking of a website, removal, and reappearance, are formulated with sufficient precision. This means a request asking ‘any infringement’ to ‘disappear’ from the service would fail.

Whenever specific instructions try to prevent some acts of users, their implementation must be susceptible to adequate automation. It cannot go beyond what machines can implement with adequate precision.⁵¹ In my view, if there is no way for a provider to automate compliance, no proactive action is required to satisfy preventive duties. Providers might bear the burden of proof to justify this, but if proven, the inability to adequately automate should exonerate them from the obligation. If this were not the case, the providers would be forced to employ humans to seek and assess facts, which would violate the GMOP.⁵² Thus, for instance, demanding that platforms use filters that are so imprecise that they must be complemented by humans should violate the GMOP, as would requiring them to check individual pieces of content before such filters are put into place.

The specificity of instructions and their scalability through automation achieves a fair balance because it reduces the effort and resources the providers must put in place. In the spirit of Article 7 DSA, it insulates desirable behaviour—compliance with injunctions—from being a potential source of new liability risks for the provider—knowledge of new violations—to avoid disincentivising it. Because the burden for

⁵⁰ See the German Federal Supreme Court case before the *Glawischnig* ruling, *Alone in the Dark* (n 23), and the Austrian Supreme Court case after the *Glawischnig* ruling, also allowing expansion to laypersons, OGH 30 March 2020, 4 Ob 36/20b SZ 2020/25, para 6.1.

⁵¹ While this is not entirely clear from *Poland* (n 8) para 90, it is clear from *Glawischnig* (n 7) para 46.

⁵² This does not preclude providers from relying on humans in the process, but their involvement cannot be used as an excuse for lowering the standard.

social harms online is shared (see Chapter 21), each party is required to do their part, and providers cannot be asked to conduct ‘a detailed legal examination’⁵³ or seek out new facts as it would represent ‘a burden in excess of what can reasonably be expected.’⁵⁴

The existence of the appropriate legal mandate supervised by authorities is also crucial for the observance of safeguards—an implicit third requirement in case law. In fact, the presence of authorities that oversee the grant is already one such safeguard. The other can take different forms, such as advanced notice to affected parties, their ability to challenge orders or their implementation, time limits for orders, or disclosures and transparency. The CJEU has so far addressed these points in its discussion of proportionality;⁵⁵ however, they are clearly inextricably connected with the legal basis.

Once the instructions are specific, they must still pass the requirement of being prescribed by the law and proportionate, including being subject to sufficient safeguards. In the absence of Union legislation to the contrary, the instructions to trigger monitoring must always be issued by the authorities. This is not because of Article 8 DSA but due to the interpretation of liability exemptions (see Chapter 6). Obligations to perform specific monitoring, subject to penalties of any kind, are a form of liability for information. They are thus caught by liability exemptions but are, in turn, released by injunction clauses to preserve ‘the possibility for a court or administrative authority’ to issue orders. In other words, even specific monitoring obligations compatible with the GMOP can still only be issued by authorities. As a result, specific monitoring cannot be triggered by a request of a private party merely enabled by legislation. Only if an authority is involved in conferring such obligation does the liability exemption not stand in the way. National law giving power to individuals to legally request specific monitoring without any involvement of authorities violates the DSA.⁵⁶

Thus, even under the most favourable interpretation of Article 8 DSA, national non-judicial or non-administrative stay-down obligations (obligations to prevent future recurrence of infringement) are not compatible with Articles 4–6 DSA unless the EU legislature introduced them. For all other cases, only national decisions issued by authorities, if they include specific instructions, can lead to such obligations. The non-judicial or non-administrative stay-down can only be introduced in some form by the EU legislature, as we have seen in the case of Article 17 CDSM Directive.

The CJEU still seems to be in the process of outlining what exactly constitutes an illegal general monitoring obligation.⁵⁷ A lot more case law can be expected on the matter in the coming years. However, given that the DSA is a measure of full harmonisation providing for a complex system of mechanisms to tackle illegal content online,

⁵³ Joined Cases C-682/18 and C-683/18 *Frank Peterson v Google LLC and Others and Elsevier Inc v Cyando AG* ECLI:EU:C:2021:503, para 116.

⁵⁴ Case C-460/20 *TU and RE v Google LLC* ECLI:EU:C:2022:962, para 71.

⁵⁵ *UPC Telekabel* (n 8) para 57.

⁵⁶ To be sure, laws allowing merely request-based specific monitoring can be legislated but are reserved for the EU legislature. The EU legislature can naturally amend the DSA itself. We have witnessed this in *Poland*—a case reviewing the constitutionality of art 17 CDSM Directive.

⁵⁷ Andreas Paulus, ‘Schutz des geistigen Eigentums’ in Josef Isensee and Paul Kirchhof (eds), *Handbuch des Staatsrechts der Bundesrepublik Deutschland* (Band XI, C. H. Beck 2013) § 247, paras 49–51.

it is difficult to find space for national laws imposing other proactive obligations in their legislation anyway (see Chapter 17).⁵⁸ The GMOP will thus serve as an important European backstop against indiscriminate surveillance of people and content.

5.3 Origins of the GMOP: From the ECD to the DSA

Having attempted to demarcate the scope of the GMOP, it is useful to examine its legislative history and developments up to this point. Article 8 DSA essentially serves as a ‘bridge of continuity’⁵⁹ for the GMOP between the ECD and the DSA. However, the provision is slightly reworded to better fit into a regulation. Table 5.1 illustrates the changes.

First, given the change from a directive to a regulation, the prohibition is no longer directed to the Member States (‘Member States shall not’). Instead, a passive form is used to express a general prohibition (‘no ... shall be imposed’). Article 8 DSA thus clearly formulates a substantive principle rather than merely a procedural rule limiting state action. This brings about no change for state actions on the national level, such as orders issued by authorities or legislative acts. It might, however, change or clarify how Article 8 DSA covers state action of EU bodies (eg by the European Commission) and whether it also covers non-state actors. Article 15 ECD did not explicitly cover EU bodies as it only spoke of the Member States. Article 8 DSA widens the scope by turning the language from specific to all-encompassing. Given the powers that the European Commission gains with the DSA, it is only natural that the GMOP also explicitly started applying to the EU bodies.

Second, while the ECD included a cross-reference to a provider ‘when providing the services covered by Articles 12, 13 and 14’ (ie those with the liability exemptions), the

Table 5.1 GMOP in the ECD and DSA

GMOP in Article 15 ECD	GMOP in Article 8 DSA
<i>‘Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.’</i>	<i>‘No general obligation to monitor the information which providers of intermediary services transmit or store, nor actively to seek facts or circumstances indicating illegal activity shall be imposed on those providers.’</i>

⁵⁸ If the measure at stake undermines the DSA mechanisms, it can be pre-empted by such DSA provisions without even invoking the GMOP. For instance, art 22 DSA would pre-empt national authorities from issuing injunctions obliging providers to prioritise assessment of notifications even from entities that do not qualify as trusted flaggers; art 23 would pre-empt injunctions requiring that no prior warning be served prior to account blocking.

⁵⁹ Interview with Irene Roche Laguna, Deputy Head of Unit for Coordination and Regulatory Compliance, European Commission (2021–23). The interview was carried out over a number of sessions across the three years.

Table 5.2 Recital 47 ECD vs. Recital 30 DSA

Recital 47 ECD	Recital 30 DSA
‘Member States are prevented from imposing a monitoring obligation on service providers only with respect to obligations of a general nature; this does not concern monitoring obligations in a specific case and, in particular, does not affect orders by national authorities in accordance with national legislation.’	‘Providers of intermediary services should not be, neither de jure, nor de facto, subject to a monitoring obligation with respect to obligations of a general nature. This does not concern monitoring obligations in a specific case and, in particular, does not affect orders by national authorities in accordance with national legislation, in compliance with Union law, as interpreted by the CJEU, and in accordance with the conditions established in this Regulation. Nothing in this Regulation should be construed as an imposition of a general monitoring obligation or a general, active fact-finding obligation, or as a general obligation for providers to take proactive measures to in relation to illegal content.’

DSA refers merely to ‘intermediary services’ along with the technical activities of transmitting or storing. This could be read as a mere simplification of the text, but it could also be read as stipulating that the prohibition of general monitoring *does* apply *when-ever* providers exercise those technical functions, *regardless* of whether they eventually lose a liability exemption because they stop being neutral (see Chapter 6).

Finally, the last cosmetic change is that the second paragraph of Article 15 ECD is dropped entirely. It made sense in a minimum harmonisation instrument like the ECD but not in a full harmonisation instrument. The DSA covers some ways under which the Member States’ actors can obtain information from digital intermediaries regarding the identity of their users. In fact, in the context of the discussions leading to the adoption of the ECD, it was thought that this paragraph was unnecessary from a legal perspective since no provision of the Directive had the potential effect of limiting the possibility of legislation by the Member States.⁶⁰ Article 15(2) ECD was only added to ensure that such national laws could not derogate from the liability exemptions.⁶¹ A similar cosmetic change is the title of the article which shifts from ‘[n]o general obligation to monitor’ to ‘[n]o general monitoring or active fact-finding obligations’.

There has also been a change in the accompanying Recitals. Under the ECD, the most important arguments were found in Recital 47. In DSA, it is Recital 30. The table below shows how they compare. The EU co-legislators wanted to add a ‘dynamic reference’ to the rich case law established by the CJEU. The text clearly states that the DSA must be subjected to the same case law of the CJEU as under the ECD. The co-legislators agreed upon this dynamic reference at the last minute after a long debate regarding a slightly erratic attempt at ‘codifying’ some elements of such case law, as proposed by the Council (see Table 5.2).

⁶⁰ *ibid.*

⁶¹ Crabit (n 5) 816.

Firstly, Recital 30 DSA stipulates that specific monitoring obligations, in particular those imposed by national orders, should be issued in compliance with Union law, including the EU Charter. Already under the ECD, these orders were within the remit of EU law because orders permitted by injunction clauses were technically derogations that had to comply with the GMOP.⁶² This clarification, along with provisions like Article 9 DSA on orders, renders the conclusion inescapable.

Secondly, Recital 30 DSA emphasises that provisions of the DSA itself are equally subject to the GMOP. This is a crucial reminder, given that the DSA has numerous tools that could be interpreted broadly. For instance, the risk-based measures applicable to VLOPs and very large online search engines (VLOSEs), or the ‘best efforts’ obligations imposed on online marketplaces, when interpreted in light of Article 8 DSA, may not de facto or de jure lead to an obligation to generally monitor or fact-find illegal content, including the ‘general obligation [to take] proactive measures’.⁶³ These obligations are legislated next to liability exemptions as special rules that indirectly amend liability exemptions, but under the condition that they remain targeted as required by the GMOP.⁶⁴

5.4 The GMOP as a Balancing Tool

The prohibition of general monitoring is a reflective surface for many freedom of expression, privacy and data protection concerns in the digital environment. It de facto constitutes a tool for constitutional balancing. Looking at its wording, one would easily think that the most important right that the GMOP protects is the right to conduct business (Article 16 EU Charter of the Fundamental Rights (CFR)).⁶⁵ However, as was mentioned in the introduction, the most frequently protected right that the GMOP guarantees is actually the right to freedom of expression and information (Article 11 CFR). So far, it is less understood that the GMOP equally protects personal data and privacy (Articles 7–8 CFR). Table 5.3 lists examples of typical measures and risks in the context of Article 8 DSA.

To date, the typically mentioned policy rationale of the GMOP has been that it protects against blocking lawful content due to limits of technology. Arguably, Recital 26 now reinforces this focus by stating that ‘providers ... should, for example, take reasonable measures to ensure that, where automated tools are used to conduct such activities, the relevant technology is sufficiently reliable to limit to the maximum extent possible the rate of errors.’ In this sense, Article 8 DSA acts as a brake on using technological

⁶² On the injunction clauses (arts 14(3), 13(2), and 12(3) ECD), ch 8.

⁶³ DSA, Rec 30.

⁶⁴ In the absence of European harmonisation, enforcing some of the due diligence rules, such as fines for failing to engage in risk mitigation, would fall under the remit of the liability exemptions and be barred by them in the national law. The EU thus opened the regulatory space; however, it only used the tools in the DSA.

⁶⁵ Charter of Fundamental Rights of the European Union [2012] OJ C326/391, art 16.

Table 5.3 Keys risks for general monitoring

	Freedom of expression	Privacy and data protection	Right to conduct business
High risks	Over-blocking of legal information caused by inadequate automation	Preventive indiscriminate surveillance of people's private communications	Preventive obligations that require independent fact-gathering or assessment
Low risks	Reactive measures to remove specific content or block specific users	User-targeted measures	Reactive measures to remove specific content or block specific users

solutions that might be inadequate from the perspective of freedom of expression. As explained by the CJEU:

... A filtering system which might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications, would be incompatible with the right to freedom of expression and information, guaranteed in Article 11 of the Charter, and would not respect the fair balance between that right and the right to intellectual property. ... The providers of those services cannot be required to prevent the uploading and making available to the public of content which, in order to be found unlawful, would require an independent assessment of the content by them in the light of the information provided ...⁶⁶

This reading was suggested by AG Øe, who felt that given the technological improvements, the CJEU had already approved more permissive standards of the GMOP in *Glaswischnig*.⁶⁷ The most compelling description of the GMOP's function can be found in the following passage, where he summarised it as follows:

I am inclined to regard the prohibition laid down in Article 15 of Directive 2000/31 as a general principle of law governing the Internet, in that it gives practical effect, in the digital environment, to the fundamental freedom of communication. I note, moreover, that the Court has already brought together compliance with that freedom and that prohibition in its case-law. One cannot exist without the other. It follows, in my view, that that prohibition goes beyond the scope of Article 15 of Directive 2000/31 and is binding not only on the Member States, but also on the EU legislature.⁶⁸

The AG rightly evoked the case law of the CJEU, which previously dressed up its rejection of the national measures in the EU Charter's cloth.⁶⁹ The CJEU eventually fully

⁶⁶ *Poland* (n 8) paras 86, 90.

⁶⁷ *Poland (Opinion of AG Øe)* (n 37) para 113.

⁶⁸ *ibid* para 106.

⁶⁹ *Scarlet Extended* (n 7) paras 40, 52; *SABAM* (n 7) paras 38, 50.

accepted this reading by AG Øe when it ruled that the GMOP constitutes ‘an additional safeguard for ensuring that the right to freedom of expression and information of users of online content-sharing services is observed.’⁷⁰ As discussed above, in having the speech concerns of content creators in mind, this had led to several important limiting principles: (a) strict targeting of measures, (b) adequacy of error rates, and (c) machine-only implementation of the tools. While these measures protect providers against excessive demands, the right to conduct business, in fact, shapes the measures less than the right to freedom of expression and information. For instance, the adequacy of error rates actually raises costs for providers who could employ cheaper solutions. The Court’s failure to constantly articulate this⁷¹ should not be immediately seen as a failure to recognise this trade-off.

Thus, the GMOP emphasises the precision of enforcement rather than its cost to providers. If delivering adequate quality is more expensive but still proportionate, the GMOP arguably demands that quality be given preference. This never-ending compromise between cost and precision is also evident in the requirement for preventive measures, whereby machines must, in themselves, be able to deliver such adequate quality. In the end, this protects providers from excessive demands to employ human moderators to complement faulty technologies, but it protects speakers exposed to faulty decision-making. Taken together, the GMOP acts as an incentive to improve technological means.

The above argument was brought to a close by the European Commission, who much earlier speculated that: ‘one can imagine that if filtering techniques had become flawless and costless, the need for a prohibition on imposing a general monitoring obligation would have become obsolete.’⁷² But is it true? If automated tools were to become flawless, would this render the GMOP superfluous?

First, it is fairly clear that such a flawless state can never be reached. No technology can avoid making mistakes, more so if applied to contextually sensitive legal assessments. No amount of machine learning and great data sets will change that. More realistically, automated tools may become sufficiently good in some areas so that they can outperform humans in the rate of their errors.⁷³ This would constitute a tremendous improvement. Of course, such tools could hardly ever become costless as they would require access to new data sets. Plus, the laws determining their assessments change as well. The most realistic expectation is that technological tools will become better than humans at some point and thus can be deployed in many more areas than today and at lower costs. This will obviously broaden their deployment.

⁷⁰ *Poland* (n 8) paras 86, 90.

⁷¹ Most obviously in *Glawischnig* (n 7). As argued in ch 3, the Court is often influenced by the framing in its responses, which does not immediately mean that what goes unmentioned is entirely left out of the picture.

⁷² Commission, ‘“Online Services, Including e-Commerce, in the Single Market” (Commission Staff Working Document) Accompanying the Document “A Coherent Framework to Boost Confidence in the Digital Single Market of e-Commerce and Other Online Services”’ (Communication) SEC(2011) 1641 final, 50.

⁷³ Husovec, ‘The Promises of Algorithmic Copyright Enforcement’ (n 49) 67–69.

However, even perfect tools can still implicate data protection rights and constitutional issues around mass surveillance. One might still worry about the impressive efficiencies of imaginary error-free systems. Such systems could be viewed as autonomously seeing and deciding too much. The automated tools can draw on years of data and assess many aspects of people's lives. They could provide efficiencies that inevitably come at the expense of the privacy and agency of individuals. Thus, it is hard to imagine that even error-free tools would ever make the GMOP entirely redundant. Better technology will only highlight the data protection dimension. At the moment, the freedom of expression dimension seems justifiably more central. As technologies progress, this may change.⁷⁴

It seems less known that the CJEU previously conceptualised the GMOP in light of both Articles 8 and 11 of the EU Charter, thus also covering the right to personal data among its functions.⁷⁵ Automated tools of enforcement, such as filters, sometimes need personal data (eg videos depicting persons). The long-term retention of such data, its processing in reference databases, often through profiling, and the ability to reach automated decisions are all obvious concerns of data protection law. Privacy concerns have been less important in much of today's case law dealing with IP rights because content recognition technologies sometimes avoid processing personal data. However, in other areas, such as face or voice recognition, personal data will have to be used. This is already the case with filtering technologies such as PhotoDNA, which processes highly sensitive photographs of child abuse material.

There is no doubt that many measures that could qualify as general monitoring, even in the absence of Article 8 DSA, would need to be scrutinised under other EU acts in the data protection law⁷⁶ and the CJEU case law on data retention and automated assessment.⁷⁷ During the legislative process, the European Parliament suggested including explicit safeguards against various cases of abuse of personal data in Article 8 DSA. However, that proposal was not adopted.

To conclude, the GMOP, at its core, protects individuals against indiscriminate surveillance of their behaviour and expressions.⁷⁸ It also protects providers from

⁷⁴ This was precisely the argument raised by the European Parliament when proposing modifications to art 8 that would prohibit the imposition of automated tools for content moderation, the provision of end-to-end encrypted services or the anonymous use of the services. European Parliament, 'Amendments adopted by the European Parliament on 20 January 2022 on the proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (DSA) and amending Directive 2000/31/EC ((COM(2020)0825 — C9-0418/2020 — 2020/0361(COD)))' [2022] OJ C336/48, 138.

⁷⁵ *Scarlet Extended* (n 7) para 50: '... as the contested filtering system may also infringe the fundamental rights of that ISP's customers, namely their right to protection of their personal data and their freedom to receive or impart information, which are rights safeguarded by Articles 8 and 11 of the Charter respectively'. However, the Court did not invoke art 15 ECD specifically in this context.

⁷⁶ Council Regulation (EC) 2016/679 of 27 April 2016 on the protection of natural persons concerning the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1 (GDPR); European Parliament and Council Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties [2016] OJ L119/89 (Law Enforcement Directive).

⁷⁷ Case C-817/19 *Ligue des droits humains ASBL v Conseil des ministres* [2022] ECLI:EU:C:2022:491.

⁷⁸ For a similar point, Wilman (n 16).

unreasonable costs. The principle can be articulated as follows: *the state is only allowed to pursue digital enforcement in a targeted fashion; individuals shall not be placed under general suspicion that their behaviour or expressions are unlawful.*

5.5 The GMOP as a Harmonisation Tool

As a full harmonisation instrument, the DSA already leaves a small margin for national rules to impose due diligence obligations onto intermediaries to tackle illegal content online (see Chapter 17). But, even within that narrow space, the GMOP acts as a co-ordination mechanism for the Member States. Article 8 DSA stops the Member States from introducing various national experiments. Thus, for the digital single market, the robustness of the rule is crucial. It offers a general framework that limits national efforts to increase the responsibility of certain providers in their national law at the expense of harmonisation. It pre-empts uncontrolled national experimentation with policies that could undermine harmonised norms.

The GMOP is sometimes criticised by content industries for its inconsistency since providers are allowed to voluntarily do what the authorities cannot tell them to do. However, this criticism misses the point about the GMOP's legislative purpose. The GMOP, similar to liability exemptions, is a coordination mechanism. It constrains the Member States' ability to regulate. The GMOP limits the national legislatures directly. It does not limit providers who have the freedom to contract. The GMOP is instead a tool that dictates what type of monitoring behaviour, if requested by the state, shall be illegal. This explains why some types of monitoring cannot be requested by the Member States but can be adopted voluntarily by the providers or why some types of specific monitoring can be deployed by the EU legislation but not by the Member States.

This coordination role might have been overshadowed by the fact that the GMOP began to embody much more than just a framework for coordinating who can legislate in the zone of shared competencies between the Member States and the EU. The CJEU's interpretation of the concept, in conjunction with the EU Charter, means that some parts of the GMOP have obtained quasi-constitutional status—they cannot be legislated away even by the EU legislature.⁷⁹ As a result, some of the measures that are not allowed for the Member States to legislate on, cannot be introduced by the EU legislature either. Doing so would violate the EU Charter that protects the GMOP's core as a tool for balancing.⁸⁰

⁷⁹ This is a part of the petrification effect that can also be observed in other parts of the EU law. Martin Husovec, 'Intellectual Property Rights and Integration by Conflict: The Past, Present and Future' (2016) 18 Cambridge Yearbook of European Legal Studies 239.

⁸⁰ *Poland* (n 8); *Scarlet Extended* (n 7).

From this perspective, there are two possible ways how to look at the GMOP:

- GMOP is a unitary *statutory provision* that always has the same meaning, regardless of whether it constrains the EU legislature and authorities or national legislatures and authorities.
- GMOP is a *principle* that has its core and *statutory versions*; while the EU legislature is bound only by the core guaranteed by the EU Charter, the Member States are bound by its statutory versions, which are left to the CJEU to interpret.

Under the second interpretation, only a core of the GMOP is guaranteed by the EU Charter and cannot be legislated away even by the EU legislature. The GMOP's statutory version in Article 8 DSA guarantees more protection than the core. It limits the Member States (and the EU) when introducing their measures in the area and the authorities interpreting them. The statutory scope is decisive when the CJEU reviews the actions of the Member States, particularly the orders of their courts or authorities (eg in cases of injunctions against intermediaries). The core, on the other hand, comes to its application when the EU legislature tries to undermine the GMOP itself. The EU legislature can fashion several versions of the GMOP as long as they comply with the core that is guaranteed by the EU Charter.

The gap between the core and statutory versions of the GMOP determines to what extent the EU can implement something that its Member States cannot.⁸¹ This sounds odd, but it would be consistent with the harmonisation logic behind the provision. It explains why the EU's legislative instruments, such as the CDSM Directive, can adopt different approaches regarding liability while still reiterating that they follow the principle.⁸² In such areas with specific laws, the EU legislature complies with the core of the principle, but not necessarily with a specific statutory version (eg Article 8 DSA) that is binding upon the Member States.

Under the first interpretation, on the other hand, the GMOP has a single meaning, which is the same for the Member States' legislatures and the EU legislature. Measures imposed by the Member States are constrained identically to those imposed by the EU

⁸¹ AG Øe argued the opposite that there is no gap. He states that 'the concept of 'general monitoring obligation' must be interpreted in the same way, irrespective of the origin of such an obligation'—ie whether it is a national or an EU measure: *Poland (Opinion of AG Øe)* (n 37) fn 124.

⁸² Some emphasise that even art 17 CDSM Directive remained under art 15 ECD, and thus, the meaning should remain the same. In my view, if the context changes, the meaning can too, and while technically correct, I do not necessarily think that the concepts used in two different contexts retain the same meaning.

legislature. It also means that even where Article 8 DSA does not apply, the GMOP still follows any EU legislation as a shadow.⁸³

Case law to date does not give a satisfactory answer to this very consequential question. The only case to date that could have clarified the issue, *Poland*, failed to do so. When discussing two different directives that mention the GMOP, the Court noted that they express the GMOP in 'similar terms', thus suggesting that they could express it in principle. When the Court applied the concept, it spoke about it as 'an additional safeguard', then interpreted as limiting the use of automation.⁸⁴ This latter remark would suggest that the GMOP can mean different things in different legal acts, and its content might be influenced by other safeguards in each specific legal act.

In my view, it is too early to tell. Given the legislative history and purpose, the second interpretation appears to me to be more plausible. The GMOP was initially only mentioned in Article 15 ECD. However, the references to it in the meantime have been added to many other acts, such as the General Data Protection Regulation (GDPR), Audiovisual Media Services Directive, CDSM Directive, and the Terrorist Content Regulation.⁸⁵ The GMOP has indeed become a key principle of internet regulation, whether directly or by cross-reference to Article 15 ECD. In the coming years, the GMOP as a constitutional and statutory concept (in Article 8 DSA or other acts of EU law) will likely gain even more importance.

In my view, given the rising number of EU legislative acts, the CJEU will have to clarify at some point that the use of the concept means different things in different contexts, for instance, in the constitutional context (as a brake on legislature) and the statutory context (as a feature of diverse legislative solutions). It is plausible that soon the Court might recognise several legislative designs of the GMOP, with Article 8 DSA offering the baseline meaning from which other acts can deviate if they offer more extensive complementary safeguards.

For instance, one could argue that when Article 17 CDSM Directive imposes a stay-down obligation that entails filtering, *its* GMOP is informed by the effectiveness of other legislated safeguards mitigating the same risks. This means asking: what did the EU legislature additionally do to contain these risks in this specific setting? If the legislature took the risks into account, then arguably, the specific version of the GMOP standard in a separate legal instrument could be more permissive, as in *Poland*. The reason is that the relevant concerns are now partly addressed by more specific safeguards in the statutory design (eg prior risk assessment).

⁸³ The best example to date is the CJEU's transplantation of the GMOP into the IP Enforcement Directive, including in the offline context: see *Tommy Hilfiger* (n 31) para 34. For more on the debate, Husovec, 'Holey Cap! CJEU Drills (yet) Another Hole in the e-Commerce Directive's Safe Harbours' (n 12) 118ff.

⁸⁴ *Poland* (n 8) para 90.

⁸⁵ Audiovisual Media Services Directive, Rec 48 and arts 28a(5), 29b(1), and 29b(6); CDSM Directive, Rec 66 and art 17(8); Terrorist Content Regulation, Rec 25 and art 5(8). For its precursors, see the General Data Protection Regulation, Consumer Protection Cooperation Regulation, European Electronic Communications Code Directive, Market Surveillance Regulation, General Product Safety Regulation and Payment Services (PSD2) Directive.

If the Court admits such split reading, the guiding principle should be the risk of abuse of such monitoring. When the European legislature departs from the DSA, it must still calibrate its interventions well to address the core concerns of indiscriminate monitoring. With this reading in mind, the Court's reference to the GMOP as an 'additional safeguard' in *Poland* paints it as a sort of a backstop safeguard—the internet's ultimate safety net.⁸⁶ Put differently, Article 8 DSA is a default rule of the legal system that only the EU legislature can redesign, but never suspend entirely. It is a pillar of the DSA as a digital rights charter (see Chapter 18).

5.6 The GMOP vs the Member States

Liability exemptions require that specific monitoring must be administered by authorities or courts on the national level (see Chapter 8). In the absence of EU legislation dispensing with this requirement, specific monitoring based on mere requests of individuals violates the DSA. But the problem is that assurance of the proper scope of such orders often requires more procedural safeguards, such as rights to affected parties to challenge implementations (*UPC Telekabel*),⁸⁷ or the need for oversight of the implementation (*Glawischnig*).⁸⁸ However, the doctrine of procedural autonomy of the Member States somewhat limits the ability of the CJEU to demand specific procedural safeguards. According to the settled case law:

in the absence of EU rules on the matter, it is for the national legal order of each Member State to establish procedural rules for actions intended to safeguard the rights of individuals, in accordance with the principle of procedural autonomy, on condition, however, that those rules are not less favourable than those governing similar domestic situations (principle of equivalence) and that they do not make it excessively difficult or impossible in practice to exercise the rights conferred by EU law (principle of effectiveness)⁸⁹

Given that most EU law does not introduce such safeguards, it is unsurprising that the national situation is far from ideal. For instance, Austrian and German courts narrowed down the procedural safeguards following *UPC Telekabel's* ruling to a theoretical ability to sue in a separate lawsuit.⁹⁰ German and Austrian courts

⁸⁶ Graham Smith makes a similar point, Graham Smith, 'Time to Speak up for Article 15' (*Cyberleagle*, 21 May 2017) <<https://www.cyberleagle.com/2017/05/time-to-speak-up-for-article-15.html>> accessed 1 August 2023.

⁸⁷ *UPC Telekabel* (n 8) para 57.

⁸⁸ *Glawischnig* (n 7).

⁸⁹ Case C-3/16 *Lucio Cesare Aquino v Belgische Staat* ECLI:EU:C:2017:209, para 48.

⁹⁰ Austrian Supreme Court case OGH 24.06.2014, 4 Ob71/14s, para 5.1; the Hamburg District Court case, LG Hamburg v 12 May 2021 – 310 O 99/21. <https://www.quad9.net/uploads/20210618_Sony_Quad9_Injunction_GERMAN_redact_ccaba9768b.pdf> accessed 1 August 2023.

have also interpreted the GMOP as permitting obligations to filter that involve humans.⁹¹

Without further specification of the safeguards, the effectiveness of Article 8 DSA is heavily limited by the consequences of the doctrine of procedural autonomy. This comes at the expense of the rights of some individuals. In this context, Kaleda, a judge of the General Court, argues⁹² that '[i]n the absence of harmonisation, the application of Article 47 of the Charter could therefore lead to the establishment of a minimum procedural standard, which can be invoked in order to achieve a certain degree of uniformity'. This is particularly important for some injunctions where the two litigating parties neglect the position of the affected third party—the so-called 'Three-Body Problem'.⁹³

Apart from Article 47 EU Charter, another solution is to strengthen the quality of the law analysis. The CJEU could require that safeguards be adopted explicitly *by legislation*. After all, the EU Charter and Court's case law dictate that the interference and safeguards must be 'prescribed by the law'.⁹⁴ Since Article 8 DSA already acts as a coordination tool by giving the Member States permission to intervene by imposing specific monitoring, it only makes sense to require that permitted measures are safeguarded against abuse *explicitly* within national legislation. Thus, any acceptance of website blocking, for instance, would only be possible if national law also spells out the safeguards that the Court prescribes.

The English courts have demonstrated the most elaborate thinking about safeguards in European case law. They require discharge clauses in cases of a material change, and for the benefit of targeted websites and affected providers, transparency notices to the public and explicit sunset clauses.⁹⁵ This is in stark contrast with some other jurisdictions that sometimes do not foresee any safeguards at all.⁹⁶

⁹¹ *Alone in the Dark* case (n 23), where this was first accepted by the German Federal Supreme Court; Austrian Supreme Court case, OGH 4 Ob 36/20b (n 49) para 6.1.

⁹² Saulius Lukas Kalėda, 'The Role of the Principle of Effective Judicial Protection in Relation to Website Blocking Injunctions' (2017) 8(3) *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 216; also discussion of the procedural side in Martin Husovec, 'Injunctions against Innocent Third Parties: The Case of Website Blocking' (2013) 4(2) *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 116.

⁹³ Daphne Keller, 'The Three-Body Problem: Platform Litigation and Absent Parties' (*Lawfare*, 4 May 2023) <<https://www.lawfaremedia.org/article/the-three-body-problem-platform-litigation-and-absent-parties>> accessed 10 August 2023.

⁹⁴ *Poland* (n 8) para 67; also Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* ECLI:EU:C:2020:559, para 176; *Opinion 1/15 of the Court (Grand Chamber)* ECLI:EU:C:2017:592, paras 140–41.

⁹⁵ *Cartier International AG & Ors v British Sky Broadcasting Ltd & Ors* [2014] EWHC 3354 (Ch) [262].

⁹⁶ To illustrate the state of fragmentation, the website blocking injunctions are subject to many different national practices regarding the following issues: (a) who is considered to be an infringing third party, (b) the form of the orders, (c) their specificity, (d) scope of preventive duties, (e) types of used technologies, (f) possibility of ex post submission upgrade, (g) use of a subsidiarity principle, (h) assessment of effectiveness, (i) cost allocation, (j) post grant supervision, (k) locus standi for users and website operators, and (l) the enforcement of court orders. See Martin Husovec and Lisa van Dongen, 'Website Blocking, Injunctions and Beyond: View on the Harmonization from the Netherlands' (2017) 12(8) *Journal of Intellectual Property Law & Practice* 695.

In my view, expecting civil judges to introduce such safeguards in their orders is unrealistic. Post-DSA, the advantage is that many horizontal safeguards will already be introduced; however, not all of them will apply to compliance with national orders. Ideally, the Member State (or the EU) should adopt more detailed national legislation about how injunctions against intermediaries are to be handled by courts, what safeguards can be imposed by courts or supervised by other authorities, and who should carry what costs. The Member States that rely on administrative enforcement of orders already do it to some extent. However, more horizontal laws of this type are generally missing.

Liability Exemptions: General Requirements

6.1 Introduction	93	6.2.6 Economic nature of services	113
6.2 General Requirements	95	6.3 Emerging Difficult General Issues	116
6.2.1 Relevant technical activities	96	6.3.1 Impact of liability-excluding norms	117
6.2.2 Information 'provided by recipients'	97	on liability-establishing norms	117
6.2.3 Scope of exempted 'liability'	99	6.3.2 Neutrality and reliance on factual	118
6.2.4 The neutrality condition	101	presumptions	118
6.2.5 Provider's own investigations	111	6.3.3 The place of the neutrality test	121

6.1 Introduction

In October 1996, the European Commission published its Communication to the Council and European Parliament under the title 'Illegal and Harmful Content on the Internet'.¹ This laid the basic principles for the E-Commerce Directive (ECD) proposal unveiled in 1998. The communication stated that:

Internet access providers and host service providers play a key role in giving users access to Internet content. It should not however be forgotten that the prime responsibility for content lies with authors and content providers. It is therefore essential to identify accurately the chain of responsibilities in order to place the liability for illegal content on those who create it ... The law may need to be changed or clarified to assist access providers and host service providers, whose primary business is to provide a service to customers, to steer a path between accusations of censorship and exposure to liability.²

The ECD was adopted in June 2000.³ The main purpose of its liability exemptions is to *structure* the regulation of digital services in the world's largest single market. By clarifying legal expectations, the exemptions incentivise investment in novel services. Businesses in the Member States suddenly did not have to worry about how various national laws would regulate their businesses. By aligning expectations, the ECD created

¹ Commission, 'Illegal and Harmful Content on the Internet' (Communication) COM (96) 487 final.

² *ibid* 12–13.

³ University of Cambridge maintains a fantastic resource concerning the legislative history of the e-Commerce Directive, see Centre for Intellectual Property and Information Law, 'E-Commerce Directive' (*University of Cambridge*) <<https://www.cipil.law.cam.ac.uk/resources/european-travaux/e-commerce-directive>> accessed 1 August 2023.

a baseline that allowed companies to expand and scale across the European Union (EU) borders.

Two decades later, the Commission concluded in its impact assessment for the Digital Services Act (DSA) that the ECD largely succeeded in achieving this goal.⁴ Similarly, the 2020 evaluation report prepared for the European Parliament's Committee on Internal Market and Consumer Protection (IMCO), which I had co-authored, concluded that:

The common liability exemption rules allow the firms to more easily scale up on the digital single market. Although far from constituting uniform rules, they give companies basic reassurances concerning the operation of their business in dealing with third-party content, and to stakeholders in enforcement of their rights. They also provide a common vocabulary for European judicial discourse. The benefits in terms of approximating the liability framework can be best seen when compared with largely the non-harmonised preventive measures.⁵

The original objective continues to remain valid today. This is now emphasised by Recital 16 of the DSA.⁶ Through the DSA, the liability exemptions received a 'renewed democratic mandate'⁷ from the legislatures in the EU. In 2010–20, the liability exemptions were often subject to criticism from some stakeholders that the rules were no longer 'up-to-date' or 'fit for purpose'. The oft-used argument was that most of our current digital services did not exist in 2000. While the argument was factually wrong because virtually most digital services predate the liability exemptions, it expressed a sentiment that 'many things have changed' since 2000. And obviously, many are different.

In two decades, the internet grew from a toy for experts to an essential tool used by everyone on a daily basis. Facebook (2003), YouTube (2005), and Twitter (2006) did not exist in 2000. Nor did Google's advertising system AdWords launched in the same year. With the arrival of mobile phones and IoT, digital services became much more embedded in people's lives. Thus, it is true what we understand as 'the Internet' started substantially changing *after* the ECD was enacted.

The fact that 22 years later, the co-legislators decided to only *build upon* the liability exemptions of the ECD is the greatest testimony to how future-proof the framework is. The framework arguably owes part of its success to its focus on omnipresent technical

⁴ Commission, "Impact Assessment" (Commission Staff Working Document) Accompanying the Document "Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (DSA) and Amending Directive 2000/31/EC" SWD(2020) 348 final, para 32.

⁵ Alexandre de Streel and Martin Husovec, 'The E-Commerce Directive as the Cornerstone of the Internal Market – Assessment and Options for Reform' (Study Requested by the IMCO committee, PE 648.797, EU Parliament 2020) 35 <[https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648797/IPOL_STU\(2020\)648797_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648797/IPOL_STU(2020)648797_EN.pdf)> accessed 1 August 2023.

⁶ DSA, Rec 16: 'The legal certainty provided by the horizontal framework of conditional exemptions from liability for providers of intermediary services... has allowed many novel services to emerge and scale up across the internal market. That framework should therefore be preserved.'

⁷ Interview with Irene Roche Laguna, Deputy Head of Unit for Coordination And Regulatory Compliance, European Commission (2021–23).

activities, such as storage or access, instead of chasing ever-evolving types of products and business models. However, given the ECD's early adoption, the law could say little about the regulation of various problems that might arise within digital services. The DSA tries to fill this regulatory gap.

Despite the topic's political sensitivity, the co-legislators—the European Parliament and the Council—changed the Commission's proposal only to a limited extent, having largely confirmed and even expanded it. The DSA repeals Articles 12–15 ECD and incorporates them as Articles 4–8 into the DSA. Articles 4–6 DSA—introducing liability exemptions—have largely been untouched. However, there are some minor wording changes in the context of all three exemptions. They usually extend their applicability to novel types of services.

Legally speaking, the result of Articles 4–6 DSA is that no national law can modify rules concerning hosting, caching, and mere conduit *activities*. Being a Directive, the ECD gave rise to many different transpositions and interpretations at the national level. Incorporating such rules in a directly applicable regulation is hoped to provide greater uniformity and certainty for cross-border services. The liability exemptions depict a measure of full harmonisation from which the Member States cannot deviate. Any conflicting national provisions modifying their content, even if indirectly, are automatically pre-empted by the DSA and must be set aside by a national court.⁸ The pre-emptive effect of the liability exemptions is much broader (Chapter 17).

6.2 General Requirements

In this subchapter, I explore various general conditions that apply to liability exemptions. Over the years of the existence of the ECD, these conditions have been subject to growing case law and numerous controversies. The DSA has made some changes to the pre-existing case law; however, the role of the Court of Justice of the European Union (CJEU) remains key.

The EU legislature intervenes to regulate various digital services to establish and advance the Digital Single Market (DSM). The internal market rationale is not just the legal basis of the law in this area⁹ but also its primary objective. The prominence of the internal market rationale is evident in the initial recitals of the instrument as well. Article 1 DSA demonstrates that the law pursues not only the goal of completing the DSM but also other goals, such as protecting the fundamental rights of victims, content creators, and other users. Because the Union legislation is based on the internal market clause, it can only regulate activities that are inherently economic.

⁸ Regulation is directly applicable and takes precedence; see Case 106/77 *Amministrazione delle Finanze dello Stato v Simmenthal SpA* ECLI:EU:C:1978:49. For other types of technical activities which fall outside the ambit of liability exemptions (or of the DSA), the Member States can continue to maintain or introduce their national rules, including national liability exemptions.

⁹ European Parliament and Council Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market [2000] OJ L178/1 (ECD), Rec 1; DSA, Recs 2 and 4. They share the same legal basis, art 114 TFEU (previously art 95 TEC).

6.2.1 Relevant technical activities

Liability exemptions apply to services based on the *technical activities* they perform. The qualification criteria do not consider business models or types of final products that incorporate them; they only consider the underlying technical functioning. Rules only look at whether the description of technical activities performed matches that of liability exemptions (see Figure 6.1).

This remains counter-intuitive for many. Often, it is believed that liability exemptions were designed for some types of services or even companies. This is not the case. Unlike due diligence obligations, liability exemptions are generally blind to business dimensions. Storage of third-party information can be embedded in infrastructure services (eg cloud computing) or application-layer services (eg video-sharing apps). Such services can be deployed by providers of mostly user-generated content (eg social media) or editorial content (eg newspapers, regarding readers’ comments). It can be provided for a fee, free of charge, or for a different consideration (eg for a subscription or tokens). Most of the questions about how and by whom are irrelevant for the purposes of delineating the scope of technical activities.

Hosting concerns every activity that can be described as ‘storage’; mere conduit any activity that can be defined as ‘transmission in a communication network’ or ‘provision of access’ to it; caching any activity described as ‘transmission in a communication network’ performed for the sole purpose of making its onward transmission more efficient or secure. All technical activities outside the three are outside the scope of the liability exemptions, and because of the definitional set-up of the regulation, they are also not within the ambit of the DSA (Chapter 9).

The DSA stresses that all possible future digital services should be considered under the regulatory umbrella. Recital 29 attempts to stretch the imagination of those

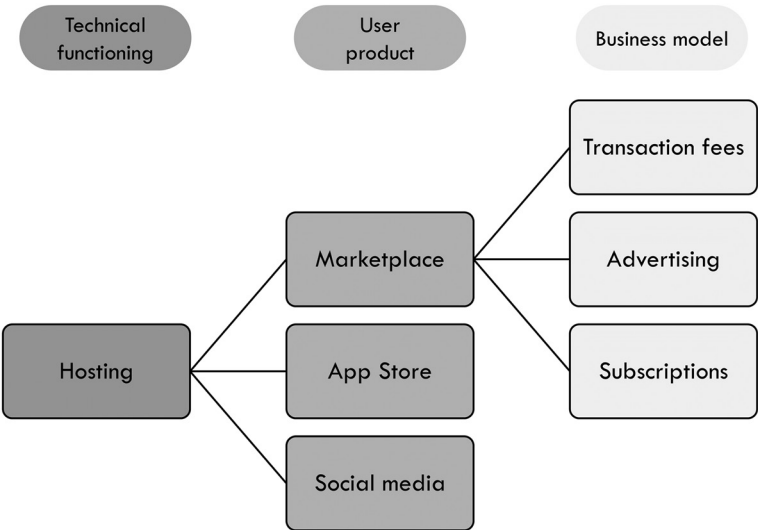


Figure 6.1 Functionality and its primacy

interpreting the law because digital services ‘develop continually’ and the law’s reading should keep in touch with times. Therefore, Recital 29 emphasises that:

Intermediary services may be provided in isolation, as a part of another type of intermediary service, or simultaneously with other intermediary services. Whether a specific service constitutes a ‘mere conduit’, ‘caching’ or ‘hosting’ service depends solely on its technical functionalities, which *might evolve in time, and should be assessed on a case-by-case basis*.¹⁰

Thus, although the DSA maintains the triad of existing regulated technical activities, it attempts to broaden some of them. Each regulated technical activity covers a wide range of digital services processing user-generated content that is subject to a plethora of business models. For instance, hosting, defined as the storage of third-party information, can form the core of discussion fora, video-sharing platforms, social networks, app stores, webhosting, and cloud computing services. The technical activity embedded in such services does not have to be the only activity of the service. For instance, providing access to a communication network under the mere conduit exemption can be part of hospitality services provided by hotels or be offered as a standalone service provided by telecommunication firms. In the case of composite services (Chapter 9.2), several entities might be able to invoke the liability exemption for the activity they perform together. For instance, owners of social media pages and companies might both qualify as hosting providers vis-à-vis third-party comments posted on such pages.¹¹

As long as exempted technical activities can be said to constitute ‘an information society service’—ie they are provided ‘at a distance, by electronic means and at the individual request of a recipient of services’—in the context of what can be regarded as an economic activity, they are covered by the DSA (section 6.2.6).¹² However, the *manner* in which the technical activities are embedded in the service can influence the interpretation of conditions under which liability exemptions continue to apply. For instance, when a provider tries to present someone else’s content as its own, it might disqualify itself from otherwise available liability exemptions (section 6.2.4).

6.2.2 Information ‘provided by recipients’

All relevant technical activities must process ‘information provided by a recipient of the service.’ Thus, storage of the *provider’s* information, such as when newspapers upload their own articles onto their own website, is by definition *not* covered.¹³ But comments

¹⁰ DSA, Rec 29 (emphasis mine).

¹¹ The Austrian Supreme Court held in 2016 that an owner of a page can qualify as a hosting provider (Case No 6Ob244/16z).

¹² See Rec 5 relying on the definition from a recast European Parliament and Council Directive (EU) 2015/1535 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services [2015] OJ L241/1.

¹³ Case C-291/13 *Sotiris Papasavvas v O Fileleftheros Dimosia Etaireia Ltd and others* EU:C:2014:2209.

that their users upload in response to their articles are covered. The legal framework is meant to cover responsibility for content generated by users.

But which information exactly is said to be users' and which is said to be providers'?

Our current interpretation emphasises user-generated content services that rely on the user's *push*—an act of uploading or accessing. When users push their information onto digital services, we consider it user-generated, even if such a push requires little effort from the user's side. In contrast, when providers *pull* information from the outside world to re-organise it, we consider such services to fall outside the remit of the liability exemptions. Search engines, for instance, struggle with the current framework because they process information that presumes the website owners' consent in the absence of opt-outs. Thus, unless they have a more curated relationship with website owners, they pull user-generated content (Chapter 8).

But even among 'pushed content', it is not easy to draw the line. Most lawyers would say that Spotify is streaming its own editorial collection of music, and YouTube is providing music uploaded by its users. However, this distinction seems to rest on very small differences. Streaming services usually make available music provided by distributors—musicians' agents—who upload music.¹⁴ The service's checks of uploaded music are not extensive. This type of content quality control is not too dissimilar from the practices of an app store which is considered a user-generated content service. Both services distribute other people's content—music or apps—for remuneration. If the streaming services cut out the distributors and allow music to be uploaded directly by authors, the difference will vanish entirely. The key to analysing these types of scenarios, therefore, seems rather how providers satisfy the condition of being provided with information discussed below.¹⁵

More frequently, the only kind of selection being carried out takes the form of automated sorting of information, which involves no choice. For instance, streaming services also carry podcasts. They have a much looser relationship with content creators of podcasts than those of music. As a result, for podcasts, streaming services might be regarded as hosting services of non-editorial 'provided' content while they remain distributors with regard to music. However, neutrality can be lost if the streaming service concludes an exclusive deal with one of the podcasters and their content becomes featured by the service.

As technology develops over time, it is inevitable that the struggle to define when information is still 'provided by' the recipient of the service not only remains but, in fact, gets worse. Going forward, the notion of pull and push might blur further. Which opt-outs from industry practices are a sign of push, and which are pull? Moreover, digital services will invent new ways of sorting through the available information.

¹⁴ For more about the streaming ecosystem, Competition and Markets Authority, 'Music and Streaming Final Report' (2022) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1120610/Music_and_streaming_final_report.pdf> accessed 1 August 2023.

¹⁵ As explained below, this has important consequences for whether such services can become VLOPs. In my view, even non-neutral services can become VLOPs.

The emergence of generative chatbots on social media shows that automated ‘user-generated’ content services can entirely obscure users’ genuine contributions. When users are nowhere to be seen, is the content still user-generated? In my view, the DSA has the tools to resolve these challenges. However, they need to be applied carefully. This debate is inextricably linked with the legal concept used by the CJEU to limit the applicability of liability exemptions—that of the *neutrality of a provider*. I discuss this in a separate section on the neutrality of providers below (see section 6.2.4).

Generally, any liability exemption only limits ‘liability for information.’ Furthermore, it limits only liability for information ‘provided by the recipient of the service.’ Although the DSA relies on the broad meaning of ‘recipient of the service’, in the liability exemptions context, the ‘recipients of the service’ still mostly refers to content creators who use the service to store or send information. This is logical since readers are rarely held liable for information they decide to access.¹⁶

Under the ECD, the recipient was usually interpreted to mean only an individual *requesting* the service, eg the end-user uploading the information or accessing a website. However, under the DSA, it is clear that anyone who ‘uses the service’ can fall under the term’s scope.¹⁷ This means that both those who impart information online and those who consult the information are considered recipients. Some liability exemptions, such as those applicable to mere conduit services, can thus gain broader scope because relevant recipients now do not have to send any information. It is enough that they receive it through the service. This opens the applicability of liability exemptions to situations when users of digital services consume third-party information rather than produce it.

6.2.3 Scope of exempted ‘liability’

The scope of exempted ‘liability’ is as broad as it gets. The broad scope is the design choice of the drafters of the ECD who wished to coordinate all possible forms of liability that could hinder the internal market. The notion thus covers all forms of criminal, administrative, and civil liability, regardless of whether imposed on providers as accessories or directly liable actors.¹⁸ The wide scope of the term is also needed due to the horizontal nature of the liability exemptions. The intention to preserve this approach is confirmed by the DSA’s broad definition of illegal content, which indicates that the liability exemptions must be ‘prepared’ for all kinds of illegality scenarios,

¹⁶ One example is laws banning the possession and reading of child abuse material. See, for instance, possession of images criminalised by s 1(1)(c) of the UK Protection of Children Act 1978.

¹⁷ Art 3(b) DSA defines ‘recipient of the service’ as ‘any natural or legal person who uses an intermediary service, in particular, to seek information or make it accessible.’

¹⁸ Joined Cases C-682/18 and C-683/18 *Frank Peterson v Google LLC and others and Elsevier Inc v Cyando AG* ECLI:EU:C:2020:586, Opinion of AG Øe, para 226. The same in the US context, see s 512(c) DMCA that ‘limits the liability of qualifying service providers for claims of direct, vicarious and contributory infringement for storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider’, cited from ‘HR Rep No 105-551 Part 2 (1998)’ at 53 (Committee on Commerce Report) <<https://www.congress.gov/congressional-report/105th-congress/house-report/551/2>> accessed 1 August 2023.

ranging from criminal sanctions for child abuse, orders imposed in civil litigation, to demands of administrative authorities in consumer or medical law.

As explained by AG Szpunar, according to the preparatory works relating to the ECD,¹⁹ ‘the limitation of liability in question extends, horizontally, to all forms of liability for unlawful acts of any kind, and thus to liability under criminal law, administrative law, and civil law, and also to direct liability and secondary liability for acts committed by third parties.’²⁰ Under the DSA, ‘illegality’ is defined with reference to the national and EU legal orders. In utilising the term ‘liability’, the DSA encompasses any legal consequences that national law imposes on providers if such consequences are in any way triggered by their users’ behaviour when using their services. While the users’ behaviour is abstracted into the notion of ‘information’, since every move in the digital world produces information, the scope effectively covers any traces left by interactions between users and relevant providers of digital services.

The only form of liability specifically singled out for a different treatment is targeted injunctions. As noted by AG Szpunar, the ECD ‘makes a distinction between actions for damages and injunctions which must be taken into account when it comes to identifying the delimitation of liability prescribed in that provision.’²¹ The CJEU confirms the special status of the injunctions.²² This means that the exempted liability in Articles 4–6 DSA covers injunctions; however, *some* of them are, in turn, permitted by so-called injunction clauses (Articles 4(3), 5(2), and 6(4) DSA). According to the CJEU:

[a liability exemption] of the directive does not preclude the person harmed by that infringement from *seeking before a national authority or court* to have the service provider prevented from allowing that infringement to continue.²³

As explained in Chapters 5 and 8, this means that only orders of *authorities* are permitted to impose specific obligations on the providers subject to liability exemptions. Thus, for instance, a national law allowing non-state actors to formulate a binding request would be trying to impose liability that is exempted; such national rules must be set aside as violating Articles 4–6 DSA.

A special case of liability is pre-trial compensation and trial costs. The CJEU clearly held in *McFadden* that such compensation, as an ancillary claim connected with enforcing the main pecuniary claims such as damages, is limited by liability exemptions. As explained by the CJEU,²⁴ ‘to be well founded, such an ancillary claim requires that the principal claim is also well founded.’

¹⁹ Commission, ‘Proposal for a European Parliament and Council Directive on Certain Legal Aspects of Electronic Commerce in the Internal Market’ COM(1998) 586 final 27.

²⁰ Case C-484/14 *Tobias McFadden v Sony Music Entertainment Germany GmbH* ECLI:EU:C:2016:170, Opinion of AG Szpunar, para 64; also Case C-401/19 *Republic of Poland v European Parliament and Council of the European Union* ECLI:EU:C:2021:613, Opinion of AG Øe.

²¹ *McFadden* (Opinion of AG Szpunar) (n 20) para 70.

²² Case C-484/14 *Tobias McFadden v Sony Music Entertainment Germany GmbH* ECLI:EU:C:2016:689, para 77.

²³ *McFadden* (Opinion of AG Szpunar) (n 20) paras 68–69.

²⁴ *McFadden* (n 22), para 75 (in the context of mere conduit exemption).

However, the CJEU held the opposite to be the case for injunctions. AG Szpunar argued that the liability exemptions should also cover ‘any other pecuniary claim that entails a finding of liability for copyright infringement with respect to the information transmitted, such as a claim for the reimbursement of pre-litigation costs or court costs.’²⁵ The Court, probably driven by deference to national procedural rules, ruled the opposite—namely that pre-trial compensation and trial costs associated with permitted injunctions are not precluded by the provision. It held that the mere conduit liability exemption ‘does not prevent that same person from claiming the reimbursement of the costs of giving formal notice and court costs incurred in a claim [before a national authority or court to have the service provider prevented from allowing that infringement to continue].’²⁶ It remains unclear how broadly this allowance for pre-trial and trial costs of seeking permitted injunctions is to be interpreted. Does it only apply to the situation when authorities get involved? Or does it apply to any substantive claim for injunctive relief regardless of whether authorities have reviewed the claim?²⁷ In my view, and in line with injunction clauses, such a reading should be limited to cases whereby injunctions were sought before the authorities. Otherwise, the argument about protecting procedural autonomy holds barely any water.

6.2.4 The neutrality condition

The goal of liability exemptions is to limit the liability for non-editorial content originating from users and not limit the liability for the platform’s own editorial content. Thus, as explained above, a newspaper’s liability might be limited for comments, but not for its journalism. While in theory, the line between the two seems clear, in practice, it is becoming a heavily contested one with the growing integration of user-generated content into services. In addition, if users are acting on the instruction of the providers themselves, such content is not non-editorial either. For instance, a comment posted by an employee or contractor in the discussion forum remains editorial. The liability exemption system, thus, must be able to define the criteria for when users’ content is not users anymore.

In its first Grand Chamber judgment, *Google France*, the CJEU developed a doctrine of neutrality limiting the applicability of all three liability exemptions in situations when the providers act beyond their role as ‘intermediaries.’²⁸ Invoking a recital, it held that the hosting safe harbour only applies to a provider whose position is ‘neutral’

²⁵ *McFadden (Opinion of AG Szpunar)* (n 20) para 74.

²⁶ *McFadden* (n 22) paras 77–78.

²⁷ On the risks of this interpretation Martin Husovec, ‘Holey Cap! CJEU Drills (yet) Another Hole in the e-Commerce Directive’s Safe Harbours’ (2017) 12(2) *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 115.

²⁸ Cases such as *Joined Cases C-236/08–C-238/08 Google France SARL and Google Inc v Louis Vuitton Malletier SA* ECLI:EU:C:2010:159 (*Google France*); *Case C-324/09 L’Oréal SA and others v eBay International AG and others* ECLI:EU:C:2011:474; *Case C-521/17 Coöperatieve Vereniging SNB-REACT UA v Deepak Mehta* ECLI:EU:C:2018:639; *Joined Cases C-682/18 and C-683/18 Frank Peterson v Google LLC and others and Elsevier Inc v Cyando AG* ECLI:EU:C:2021:503.

in relation to user-uploaded content.²⁹ The test is whether the provider's 'conduct is purely technical, automatic and passive, which implies that that provider does not know or control the data which it stores.'³⁰ Any disqualifying active intervention gives the provider 'knowledge of and control over the content.'³¹ However, the disqualification applies only to specific content with respect to which the provider did not behave neutrally, and not all the remaining content on the service.³²

Subsequent case law tried to determine what constitutes a disqualifying level of 'knowledge or control'—most of the time, without much success in clarifying the issue. In the two Grand Chamber cases, *L'Oréal v eBay* (2011) and *YouTube and Cyando* (2021), the Court hardly advanced a unified test of neutrality.

The test used by the Court is capable of solving easy cases, such as whether newspapers are exempt from their liability for their own articles.³³ In *Papasavvas*, the CJEU applied the test³⁴ and held that 'since a newspaper publishing company which posts an online version of a newspaper on its website has, in principle, knowledge about the information which it posts and exercises control over that information, it cannot be considered to be an "intermediary service provider" within the meaning of Articles 12 to 14 of Directive 2000/31.'³⁵ The Court, however, never explained why this is the case.

This distinction was primarily important for hosting services, even though it applies equally to mere conduits and caching services. The nebulous case law of the CJEU led to numerous disputes about the concept of passivity. It led to cases before the European Court of Human Rights, such as *Delfi v Estonia* and *Sanchez v France*, that arguably should never have ended up there on a proper reading of the EU law.³⁶ The *eBay* ruling was particularly unhelpful in bringing clarity to the issue.³⁷ It led to widespread speculation as to whether 'presentation optimisation' is sufficient to lead to a loss of neutrality.

The CJEU case law led some Member States courts to conclude that many providers lost their neutrality and gave ammunition to some industries that viewed the relevant case law as suggesting that mere *technical control* of information already disqualifies them from EU protections. This expansive interpretation of passivity greatly influenced

²⁹ See extensively on the history of this: Martin Husovec, *Injunctions against Intermediaries in the European Union: Accountable but Not Liable?* (Cambridge University Press 2017); Folkert Wilman, *The Responsibility of Online Intermediaries for Illegal User Content in the EU and the US* (Edward Elgar Publishing 2020).

³⁰ *Google France* (n 28) para 114; *eBay* (n 28).

³¹ *YouTube and Cyando* (n 28) para 109.

³² *Google France* (n 28) paras 109, 120 ('those data'); *eBay* (n 28) para 113 ('those data').

³³ *Papasavvas* (n 13) para 45.

³⁴ *ibid* 44.

³⁵ *ibid* 45. The Austrian Supreme Court held in 2016 that an owner of a page can qualify as a hosting provider (Case No 6Ob244/16z).

³⁶ In *Delfi AS v Estonia* App no 64569/09 (ECtHR, 16 June 2015), the Estonian courts erroneously ruled that a newspaper hosting comments of others is not a passive host. In *Sanchez v France* App no 45581/15 (ECtHR [GC], 15 May 2023), the French courts did not even consider that the administrator of a page on social media could be a hosting provider vis-à-vis comments posted by users and thus shielded from liability for them.

³⁷ *eBay* (n 28) para 116. What seemed to have been overlooked by some national courts was the fact that in the *eBay* case, *eBay* itself actively promoted some advertisements outside of its services on websites such as Google or MSN and assisted with optimisation within its website. *eBay* chose the relevant keywords to advertise and paid for the advertising. Thus, optimisation expressed active contribution by employees of *eBay*: see *eBay* (n 28) para 31; *L'Oréal SA v eBay International AG* [2009] EWHC 1094 (Ch) [26], [52] (High Court of England and Wales, Chancery Division).

the 2016–19 EU copyright debate. The European Commission's copyright unit even used the terms from the case law to justify its expansion of the 'communication to the public' right in 2016.³⁸ The neutrality test was thus bound to influence the DSA debate.

In December 2019, the newspapers reported that, according to the Commission, 'concepts such as 'active' or 'passive' hosts, linked by the Court to the notion of 'optimising content', appear outdated in light of today's services.'³⁹ Public consultation,⁴⁰ targeted interviews with judges,⁴¹ and studies outsourced by the Commission⁴² in preparation for the DSA concluded that the 'active/passive dichotomy' was unclear and needed further clarifications. In the Impact Assessment, the Commission stated that:

The fact that there is no such thing as an 'active host', but that a provider might play an active role regarding some listings, but not others (for instance because it presents it or recommends it in a special manner) does not lead to the necessary legal certainty to provide legal intermediation services without risking claims for damages or even criminal liability. Many automatic activities, such as tagging, indexing, providing search functionalities, or selecting content are today's necessary features to provide user-friendly services with the desired look-and-feel, and are absolutely necessary to navigate among an endless amount of content, and should not be considered as 'smoking gun' for such an 'active role'.⁴³

Eventually, however, in its 2020 proposal for the DSA, the Commission did not explicitly touch the concept. It only reworded the relevant ECD recitals that originally gave birth to the doctrine. The text of Recital 42 ECD was modified into Recital 18 DSA, which states the following:

The exemptions from liability established in this Regulation should not apply where, instead of confining itself to providing the services neutrally by a merely technical and automatic processing of the information provided by the recipient of the service, the provider of intermediary services plays an active role of such a kind as to give it knowledge of, or control over, that information. Those exemptions should accordingly not be available in respect of liability relating to information provided not by the recipient of the service but by the provider of the intermediary service itself, including where the information has been developed under the editorial responsibility of that provider.

³⁸ Commission, 'Proposal for a Directive of the European Parliament and of the Council on Copyright in the Digital Single Market (CDSM Directive)' COM/2016/0593 final, Rec 38 ('In respect of Article 14, it is necessary to verify whether the service provider plays an active role, including by optimising the presentation of the uploaded works or subject-matter or promoting them, irrespective of the nature of the means used therefor').

³⁹ Alexander Fanta and Rudl Tomas, 'Leaked Document: EU Commission Mulls New Law to Regulate Online Platforms' (*Netzpolitik*, 16 July 2019) <<https://netzpolitik.org/2019/leaked-document-eu-commission-mulls-new-law-to-regulate-online-platforms/>> accessed 1 August 2023.

⁴⁰ Commission, 'SWD(2020) 348 Final' (n 4) annex 2.

⁴¹ *ibid.*

⁴² Sebastian Schwemer, Tobias Mahler, and Håkon Styri, *Legal Analysis of the Intermediary Service Providers of Non-Hosting Nature: Final Report* (EU Publications Office 2020) 32.

⁴³ Commission, 'SWD(2020) 348 Final' (n 4) annex 9.

Recital 18 thus consolidated the test—though still not clarified it. It repeats the criteria from the case law of the CJEU, such as knowledge or control, but it also links them to ‘editorial responsibility’—a term that previously was not used by the ECD.⁴⁴ The European Commission was probably modest because AG Øe’s Opinion in *YouTube and Cyando* dispelled some of the biggest misunderstandings about the concept.⁴⁵ It was only during the legislative process that the Court arguably tried to address the confusion introduced in its previous Grand Chamber ruling in *eBay*. However, although it did solve some issues, the Court still hardly clarified the concept. The *YouTube and Cyando* decision de facto held that the most common activities of modern digital services—algorithmic categorisation, personalisation, ranking or provision of search—do not disqualify providers from neutrality and do not rob them of protections.

Indeed, the *YouTube and Cyando* decision of the Grand Chamber provides the most elaborate application of the neutrality condition in the pre-DSA context. However, the judgment itself is not among the clearest because it interchangeably shifts between three different issues: a) the neutrality of hosting providers, b) the criteria for communication to the public, and c) the standard of specific knowledge required to strip hosting providers of their exemption. The Court’s reasoning is construed by arguing first that no hosting provider that fulfils the criteria for communication to the public can be neutral.⁴⁶ Thus, whatever qualifies someone as communicating their users’ content to the public must also disqualify him from neutrality. Second, the Court explains what activities do not constitute ‘specific knowledge’, and thus knowledge that can strip hosting providers from the liability exemption. Since, as I have argued above, the standard for neutrality must be stricter, logically, whatever is not sufficient to confer specific knowledge can neither confer ‘specific knowledge of’ for neutrality purposes.

With this caveat, the ruling confirms several important issues. The Court held that algorithmic categorisation, personalisation, ranking or provision of search do not confer specific knowledge.⁴⁷ It is not sufficient that the provider has abstract knowledge (meaning general awareness) that his service carries some infringing content.⁴⁸ However, if it is true that neutrality’s ‘knowledge of’ must be more stringent, then this clearly also means that these same activities cannot disqualify from neutrality. It also clarified that the installation of content monitoring tools that help to uncover infringing content does not constitute an active intervention which disqualifies them from neutrality.⁴⁹ In the DSA, these findings are now incorporated into Recital 22

⁴⁴ In DMCA legislative history, the editorial decisions of providers were being discussed already: ‘HR Rep No 105–551 Part 2 (1998)’ (n 18) at 51 (‘The term “selection of the material” ... means the editorial function of determining what material to send, or the specific sources of material to place on-line [eg, a radio station], rather than “an automatic technical process” of responding to a command or request, such as one from a user, an Internet location tool, or another network’).

⁴⁵ *YouTube and Cyando* (Opinion of AG Øe) (n 18) paras 158, 161: ‘eBay sometimes promotes some offers on the Internet itself outside its business’.

⁴⁶ *YouTube and Cyando* (n 28) paras 107–08.

⁴⁷ *ibid* para 114.

⁴⁸ *ibid* para 111.

⁴⁹ *ibid* para 109.

as clarifications of when ‘specific knowledge’ required by the hosting exemption is missing and Article 7 DSA concerning voluntary own-initiative investigations and legal compliance.

The CJEU in its discussion builds on AG Øe’s Opinion which defined the neutrality test as follows:

I understand the Court’s case-law to mean that a provider plays an ‘active role’ of such a kind as to give it ‘knowledge of, or control over’, the data which it stores at the request of users of its service where it does not simply engage in the processing of that information, which is neutral vis-à-vis its content, but where, by the nature of its activity, it is deemed to acquire intellectual control of that content. That is the case if the provider selects the stored information, if it is actively involved in the content of that information in some other way or if it presents that information to the public in such a way that it appears to be its own. In those circumstances, the provider goes outside of the role of an intermediary for information provided by users of its service: it appropriates that information.⁵⁰

In AG Øe’s view, the ‘involvement’ must concern ‘intellectual control’, which results in the ‘appropriation’ of information. This, in my view, maps well to the language of the DSA and my conceptualisation below. In fact, the above paragraph is followed by AG’s citation to my prior work⁵¹ that discussed the German doctrines of adopted content and why the neutrality test partly serves to demarcate what is still third parties’ and already providers’ content.

In sum, the *YouTube and Cyando* judgment, informed by AG Øe’s Opinion, improves our understanding of neutrality. It makes it clear that neutrality cannot be lost by the omnipresent technical functionalities of the interactive web but only by interventions that get the providers ‘too involved’ in the content of their users. The judgment also clarifies the underlying policy rationale, which is to draw the line when providers either instruct the production of content or appropriate it so much that they must gain editorial responsibility. Despite all these new insights, the judicial test for neutrality remains underdeveloped.

Even the DSA’s new text introduces new hints but cannot deliver a test. According to Folkert Wilman of the Commission’s Legal Service:

... there seems to be a subtle development. In particular, there is no reference to a requirement of passivity on the part of the service provider – its role may therefore be active to a certain extent, as long as it does not lead to knowledge or control in the sense just mentioned. In this manner the DSA deviates somewhat from the E-Commerce Directive, which contained such a reference to passivity.⁵²

⁵⁰ *YouTube and Cyando* (Opinion of AG Øe) (n 18) para 152.

⁵¹ *ibid* fnn 52 and 142, citing Husovec (n 29) 55–57.

⁵² Folkert Wilman, ‘The Digital Services Act (DSA) – An Overview’ (2022) 6 <<https://www.ssrn.com/abstract=4304586>> accessed 1 August 2023.

Recital 22 concerning conduits and caching speaks of not ‘alter[ing] the integrity of the information’ as opposed to ‘manipulations of a technical nature.’ The conduit exemption in Article 4 speaks of *not* initiating the transmission, selecting its receivers, and selecting or modifying the information contained. Caching exemption in Article 5 speaks of *not* modifying information and complying with some industry standards. Hosting exemptions in Article 6 speaks of *not* acting under the authority or the control of the provider and *not* creating the impression that the online platform provides information.

Recital 18 consolidates the test to ‘play[ing] an active role of such a kind as to give it knowledge of, or control over, that information.’ Knowledge and control are thus two different mutually non-exclusive criteria. Newspapers publishing articles by freelance journalists have both ‘knowledge of’ their articles and ‘control over’ them. Since editors can influence the content of those articles, and they might have instructed their authors, the conclusion seems inescapable. However, how about an app store that publishes its guidance for app developers and screens apps before their distribution? Does quality control confer on the app store ‘knowledge of’ or ‘control over’ the apps?

In my view, different active interventions could be depicted on a spectrum like the one below. Sprinkled around the DSA are numerous references to neutrality. Looking at the universe of possibilities, two elements of the test can be translated as ‘control over meaning’ and ‘knowledge by participation.’ Logically, the standard for ‘knowledge of’, triggering loss of neutrality, must be more stringent than the standard of actual knowledge triggering loss of hosting exemption. Otherwise, the former would be superfluous, and there would be no difference between the various exemptions.⁵³ On the contrary, the opposite is visible in that each liability exemption has its own set of qualifiers that further flesh out what constitutes active interventions (eg mere conduit cannot modify transmitted information but hosting services can to some extent). I will argue that these specific active interventions reveal what type of control Recital 18 is about. In my view, the DSA and case law are converging on the notion that ‘control over’ means control over the *meaning* of information, ie control over *who* says *what* (see Figure 6.2).

6.2.4.1 Editorial control

Newspapers control the meaning of information. By editorial control, they influence what journalists write. Hence, they are not neutral with respect to journalistic articles. Blogs, in contrast, do not influence what bloggers publish. Even if they pre-approve content, they do not edit submitted blogs. However, if a newspaper running a blog section edits a blog article and republishes it with its other journalistic articles, its relationship to that specific article is no longer neutral. It does not matter that the article was

⁵³ The ruling in *McFadden* rejected the knowledge requirement for all liability exemptions.

	INTERVENTION		
	NON-NEUTRAL PROVIDER		NEUTRAL PROVIDER
	Control OF MEANING	Knowledge BY COLLABORATION	Knowledge BY LEARNING
MERE CONDUIT	Recital 21 Article 4(1)(c)	Recital 20	N/A
CACHING	Recital 21 Article 5(1)(a)	Recital 20	Article 5(1)(e)
HOSTING	Recital 24 Article 6(2); 6(3)	Recital 20, 23 & 24 Article 6(2)	Article 6(1)

Figure 6.2 Neutrality of services

not originally developed under editorial responsibility. The same conclusion should apply if the newspaper did not edit the article but would simply present it to readers as its own newspaper content. This hypothetical shows that control over the meaning of information covers situations when providers influence *what* is being published by users, as well as when they change *who* is publishing it.

Conduit and caching exemptions have specific language in the exemptions themselves supporting such reading of what constitutes neutrality of control over information (eg Articles 4(1)(c), 5(1)(a), etc). As noted by Recital 21, ‘[neutrality] should not be understood to cover manipulations of a technical nature which take place in the course of the transmission or access, as long as those manipulations do not alter the integrity of the information transmitted or to which access is provided’. Thus, ‘control over meaning’ does not extend to *mechanical manipulations* that do not influence the information’s integrity. However, who expresses the information plays a part in determining integrity if such information is published. The hosting exemption now clarifies this with a new paragraph specifically addressing the situation when users’ content is presented as providers’ own (Article 6(3)). In such cases, providers do not change what is said, they only change who says it. If reasonable readers read information as originating from the provider, one can question providers’ neutrality, too. If providers hide the origins of information to create the impression that it is of their own provenance, they accept editorial responsibility. Therefore, the bots that rely on user-generated content without properly attributing it cannot be treated as neutral providers even if they meet other criteria.

‘Knowledge of’, in contrast, covers situations where a user acts as a proxy. In these cases, the provider usually instructs a user to do something. A typical example of this

is the CJEU case of *'The Pirate Bay'*.⁵⁴ The provider here intentionally instructed by inducing its users to violate the law by uploading some material. As noted by Recital 23, such a user 'is acting under the authority or the control of the provider'. The provider instructing thus clearly cannot be neutral as he wishes the outcome to materialise. The hosting exemption specifically reflects this in its liability exemptions (Article 6(2)).

Both the ECD and the DSA anticipate this sort of accessorial liability: the ECD excluded from the liability exemption those cases where the provider exercises authority or control over the content provider (Article 14(2) ECD, for hosting services) or '*deliberately* collaborates with one of the recipients of his service to undertake illegal acts' (Recital 44 ECD, initially for mere conduits and caching services). The DSA's Recital 20 reiterates and reinforces the language previously used by ECD as follows:

Where a provider of intermediary services deliberately collaborates with a recipient of the services in order to undertake illegal activities, the services should not be deemed to have been provided neutrally and the provider should therefore not be able to benefit from the exemptions from liability provided for in this Regulation. This should be the case, for instance, where the provider offers its service with the main purpose of facilitating illegal activities, for example by making explicit that its purpose is to facilitate illegal activities or that its services are suited for that purpose. The fact alone that a service offers encrypted transmissions or any other system that makes the identification of the user impossible should not in itself qualify as facilitating illegal activities.

The difficult question is to decide what level of knowledge of the illegal acts of the user is necessary. As explained above, logically, the standard for 'knowledge of' triggering loss of neutrality must be more stringent than the standard of actual knowledge triggering loss of hosting exemption. Thus, the mental element of the provider must go beyond simply *knowing* that a user will commit specific illegal actions. The provider must be somehow implicated in the users' actions. One of the obvious ways would be to conceptualise 'knowledge of' as 'knowledge of participation', borrowed from criminal law. In most legal systems, providers could become accessors when they *intentionally* participate in the acts of others.⁵⁵ Arguably, this is what the word 'deliberately' suggests.

6.2.4.2 A possible test for neutrality

Thus, the neutrality test could be formulated as follows: *did the platform exercise control over the meaning of the user's content, or does it have knowledge of its own deliberate participation in the acts of users?*

Two parts of the test are not mutually exclusive (eg newspapers deliberately participate in publishing stories of their freelance journalists and have control over the

⁵⁴ Case C-610/15 *Stichting Brein v Ziggo BV and XS4All Internet BV* ECLI:EU:C:2017:456 (*The Pirate Bay* [CJEU]).

⁵⁵ For a comparative overview of secondary liability, Christina Angelopoulos, *European Intermediary Liability in Copyright: A Tort-Based Analysis* (Wolters Kluwer 2017). For an overview of the English situation, Pey Woan Lee, 'Accessory Liability in Tort and Equity' (2015) 27 *Singapore Academy of Law Journal* 851.

substance of published articles). However, many situations would fall under one of the two subparts of the test. Let me offer some examples:

- App stores controlling the quality of submitted apps that undoubtedly obtain knowledge of the apps they distribute (though not necessarily of illegality of those apps) would remain neutral unless they deliberately participate in the app owners' specific wrongs, such as consumer fraud.
- A newspaper routinely pre-approving comments by users caught by its hate speech detection tool would preserve neutrality even when they sometimes obtain knowledge of circumstances. They could fail to act upon such knowledge by failing to investigate them but that would strip them of the liability exemption for a different reason.
- A hotel that specifically advertises its wi-fi connectivity as a good means to 'not get caught by law enforcement' could be viewed as losing neutrality for deliberately participating in the wrongs of its clients found to use the connection to commit some crimes.
- A price-comparison site that compiled product descriptions from various submissions of sellers by algorithmically evaluating their quality and then collaging various high-quality pieces into one text would lose neutrality because it produces new content with new meaning.
- An online marketplace that hides the identity of its sellers so that users cannot distinguish if they are buying from the provider or someone else would disqualify from neutrality because it gains control over the substance of the content by substituting itself as the expected producer of information.
- A video-sharing platform that automatically blurs potential depictions of violence would not be disqualified from neutrality because its interventions are merely mechanical and do not alter the meaning.
- A social network that attaches warning to posts of their users would not lose neutrality because the additional information does not alter the meaning of the commented information.
- A video-sharing service that ranks and recommends the content of its users via an algorithm would not lose neutrality because such recommendation does not change the meaning of the information ranked or recommended.

The difference between the price-comparison website and the video-sharing platform is that while both are involved in the substance of content, the video-sharing platform does not alter what is said. In contrast, the price-comparison website only uses users' information to produce new content with new meanings. The online marketplace does not change what is being said, as it preserves the originally submitted content, but alters who is saying it in the readers' perception.

Intervening in the meaning of the users' content thus has two dimensions: *who* says *what*. If the platform influences *what* is said by meaningfully intervening in drafting the provided information, algorithmically or not, it exercises intellectual control. Similarly,

if the platform changes *who* says something by presenting the provided content as its own and concealing its true authorship, it alters the meaning of the underlying information. The content now reads like a statement from the platform, not that of a third party. This last situation of ‘adopted content’ is now explicitly recognised by Article 6(3) DSA.⁵⁶

In the assessment of ‘adopted content’, it is less important to consider what *tools* are used rather than what the *outcome* is for the reader. If a platform appropriates third-party content by presenting it as its own, it does not matter if this integration results from algorithms or human actions. In both cases, the meaning of the information changes.⁵⁷ Similarly, while a platform employee’s suggestion as to what to include would qualify as an active intervention, the same can be said of automated tools that force the choice of the original author of the content. For instance, if an app provides the choices of background music to users of video-sharing platforms, it is unlikely to be able to claim a liability exemption for the inclusion of such music. At the same time, if the elements that are not the result of pre-selection can be separated, the liability exemption could continue to apply. Thus, a defamatory video that carries a piece of pre-approved music does not disqualify the provider from protection vis-à-vis the defamatory message. The video could be said to contain two different pieces of information despite being presented together as sound and image.

The ‘control of the meaning’, or as put by AG Øe, ‘intellectual control’, must be distinguished from purely *mechanical contributions*. When a platform changes the content’s font or format, there is no intervention on who says what—only the presentation of the information changes. This also follows from the recitals, which stress that modification for mere conduits and caching ‘should not be understood to cover manipulations of a technical nature which take place in the course of the transmission, as such manipulations do not alter the integrity of the information transmitted.’⁵⁸ The same is true for hosting, for instance, when the platform provides an automated translation of the text. However, if such translation mistakenly alters the meaning, the platform itself arguably changes what is said and thus exposes itself to liability.⁵⁹ The extent of acceptable mechanical contribution may differ based on the proximity of providers to their content. This is already implied in the different requirements found across the liability exemptions.

The above distinctions explain why categorisation, personalisation or ranking in the search results do not constitute disqualifying active interventions. They do not alter who says what; they only influence the delivery of the information. They assist the reader when receiving the information provided by the original author, but they do

⁵⁶ See also *YouTube and Cyando (Opinion of AG Øe)* (n 18) para 152.

⁵⁷ Consider a situation of a news portal that integrates parts of user comments into the content of articles without the author being obvious to the reader. In that case, the content would change, as the originator of the information would change from the reader’s point of view. The reader would consider this information is voiced by a news portal.

⁵⁸ DSA, Rec 21; ECD, Rec 43.

⁵⁹ This must be distinguished from when users utilise plug-ins. In these cases, translation is done by readers or users and not by platforms.

Table 6.1 Situations leading to the loss of neutrality

‘Control over’ meaning	‘Knowledge of’ own deliberate participation
A provider co-determining user’s content	A provider instructs the user’s wrongs
A provider presenting user’s content as the provider’s own	A user acting under a provider’s control or jointly collaborating

not interfere with what the author communicates. This is also true when an algorithm selects and subsequently displays only some of the content initially provided, so long as the author of such content is clearly designated to the reader.

This reading of neutrality thus presents the providers with a clear choice. If providers wish to integrate content heavily in their offering by instructing their users, redesigning their content, or concealing its origin, they can do so, but at the expense of losing the liability exemptions. Policy-wise, the resulting content shall then be regarded as editorial regardless of the means used to produce it or the fact that the finished product’s ingredients come from user-generated content.

Table 6.1 summarises the typical examples of active interventions.

6.2.5 Provider’s own investigations

The DSA’s liability chapter has introduced a new provision meant to provide interpretive guidance. Article 7 does not introduce a new liability exemption; however, it informs how to interpret various components of liability exemptions, and the prohibition of general monitoring obligations.

According to Article 7 DSA, entitled ‘[v]oluntary own-initiative investigations and legal compliance’, the following conduct must be encouraged:

Providers of intermediary services shall not be deemed ineligible for the exemptions from liability referred to in Articles 4, 5 and 6 solely because they, in good faith and in a diligent manner, carry out voluntary own-initiative investigations into, or take other measures aimed at detecting, identifying and removing, or disabling access to, illegal content, or take the necessary measures to comply with the requirements of Union law and national law in compliance with Union law, including the requirements set out in this Regulation.

The provision addresses the common concern that the voluntary actions of providers can cost them liability exemptions either because they lose the status of neutrality or gain knowledge as hosting providers. The CJEU has in *YouTube and Cyando* before the DSA’s adoption that the same followed already from the previous framework: ‘the fact ... that the operator of a video-sharing platform, such as YouTube, implements technological measures aimed at detecting ... content which may infringe copyright,

does not mean that, by doing so, that operator plays an active role giving it knowledge of and control over the content of those videos.⁶⁰ Article 7 introduces some more explicit language.

At this point, the added value of the provision is uncertain. On the one hand, it clearly can inform other provisions and their interpretation by articulating that desirable enforcement efforts should not be punished, and thus disincentivised, by increased uncertainty about providers' liability. In this sense, the provision draws inspiration from section 230(c) Communications Decency Act⁶¹ that tried to give comfort to 'good Samaritans' who, following the *Prodigy* ruling,⁶² were suddenly exposed to a worse legal situation if they did more to moderate the content of their users. However, Article 7 is a very different animal in a very different zoo. The DSA does not grant any legal immunity from liability for good faith content moderation actions. It only makes sure that existing liability exemptions are preserved. Thus, potential disincentives in the form of any liability to affected users remain unaddressed.

Some scholars like Kuczerawy worry that Article 7 might incentivise only more enforcement and thus more content removals because it does not provide well-rounded immunity.⁶³ I am less sure. Because the crucial counter-incentive—potential legal consequences for over-removal vis-à-vis a user—is not included in the immunity, the situation would appear the same as pre-DSA. However, given that the DSA increases incentives against over-removal elsewhere (see Chapters 10–11), I do not see deterioration of the incentive situation. However, I am equally unsure whether Article 7 will substantially change the case law on any related points: neutrality or knowledge.

Firstly, after *YouTube and Cyando*, neutrality clearly cannot be lost by simply doing more than notice and takedown. Post-DSA, many online platforms will have to do substantially more; thus, using the DSA-imposed measures on them to strip them of liability exemptions would be internally inconsistent. For very large online platforms (VLOPs), due to their big risk mitigation obligation under Article 35, there is hardly any space to say that some measures are still truly 'voluntary'. Second, post *YouTube and Cyando*, the case law is now also clear that the diligence expected of providers is limited to assessment 'without a detailed legal examination, that that communication is illegal and that removing that content is compatible with freedom of expression.'⁶⁴ Thus, even where circumstances arise during the carrying out of voluntary measures that show some indications of illegal behaviour, the indications must be very strong—basically limited to obviousness—that some behaviour is illegal. In my view, the likelihood of randomly bumping into specific knowledge about illegality without realising it is, very low.

⁶⁰ *YouTube and Cyando* (n 28) para 109.

⁶¹ 47 US Code § 230(c).

⁶² *Stratton Oakmont Inc v Prodigy Services Co* 23 Media L Rep 1794 (NY Sup Ct 1995).

⁶³ Aleksandra Kuczerawy, 'The Good Samaritan That Wasn't: Voluntary Monitoring Under the (draft) Digital Services Act' (*Verfassungsblog*, 12 January 2021) <<https://verfassungsblog.de/good-samaritan-dsa/>> accessed 1 August 2023.

⁶⁴ *YouTube and Cyando* (n 28) para 116.

6.2.6 Economic nature of services

The ‘Digital Services Act’ does not refer to ‘digital services’ in its articles. Instead, the DSA speaks about ‘intermediary services’—services that store or give access to people’s communications. The DSA does not regulate editorial services, such as newspapers or streaming. Looking at the digital ecosystem, ‘intermediary services’ are the most important types of digital services. Among the top 50 visited websites on the internet globally, the majority rely on users—ie other people, like you and I—to generate the content.⁶⁵ Thus, while the DSA is mostly about user-generated content, or user-to-user communication tools, because of the nature of such content the DSA is crafted broadly enough to capture most of the digital ecosystem (see Chapter 1).

But one limitation of the DSA is perhaps more consequential—ie a limitation to services of an economic nature.

Article 2 limits its scope to ‘intermediary services offered to recipients of the service that have their place of establishment or are located in the Union, irrespective of where the providers of those intermediary services have their place of establishment’. Article 3(f) defines ‘intermediary service’ as one of the following information society services: (i) a ‘mere conduit’ service; (ii) a ‘caching’ service, or (iii) a ‘hosting’ service. Finally, Article 3(a) defines ‘information society services’ as a ‘service’ as defined in Article 1(1), point (b), EU Directive 2015/1535. According to Article 1(2) of EU Directive 2015/1535, an ‘information society service covers any service normally provided for remuneration, by electronic means and at the individual request of a recipient of services.’⁶⁶

So, in a nutshell, to be in the scope of the DSA, a firm needs to provide an intermediary service, which in turn needs to be an information society service, which in turn needs to be a service. And what is a service? Article 57 TFEU establishes a very open definition: ‘Services shall be considered to be “services” within the meaning of the Treaties where they are normally provided for remuneration, in so far as they are not governed by the provisions relating to freedom of movement for goods, capital and persons.’ Therefore, the main characteristic of a service is to be ‘normally provided for remuneration’—a tricky condition in the context of ubiquitous and freely available online tools that might not always be at first ‘normally provided for remuneration’.

In 2000, the ECD already had to confront this question. Recital 18 ECD clarifies that ‘information society services are not solely restricted to services giving rise to online contracting but also, in so far as they represent an economic activity, extend to services which are not remunerated by those who receive them, such as those offering online

⁶⁵ The list at ‘List of Most Visited Websites’, *Wikipedia* (2023) <https://en.wikipedia.org/w/index.php?title=List_of_most_visited_websites&oldid=1168840226> accessed 8 August 2023.

⁶⁶ European Parliament and Council Directive (EU) 2015/1535 of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and rules on Information Society services (2015) OJ L241/1, codifying: European Parliament and of the Council Directive 98/48/EC of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations (1998) OJ L217/18.

information or commercial communications, or those providing tools allowing for search, access and retrieval of data.’ The CJEU has clarified that the concept of ‘normally provided for remuneration’ does not have to entail reliance on fees in the provider’s business model. According to the CJEU, ‘[t]he remuneration of a service supplied by a service provider within the course of its economic activity does not require the service to be paid for by those for whom it is performed.’⁶⁷ Even free-of-charge services whose business models are based on advertising or other business models,⁶⁸ such as the resale of data or analytics, can qualify as ‘normally provided for remuneration’.

In the context of multi-sided platforms, for instance, the fact that the user receives the service for free does not exclude it from constituting an economic activity, as other recipients of the service (such as advertisers or traders) will remunerate the service. In any event, it requires exercising an economic activity or being provided in the context of economic activity. In *Papasavvas*, the Court linked the concept to primary law when it held that ‘interpretation corresponds to that of the concept of ‘services’ within the meaning of Article 57 TFEU, which also does not require the service to be paid for by those for whom it is performed.’⁶⁹ The Court then argued that advertising undoubtedly turns the activity into services.⁷⁰ In *McFadden*, the CJEU established that offering access to a WiFi hotspot for free constituted a service, ‘where the activity is performed by the service provider in question for the purposes of advertising the goods sold, or services supplied by that service provider.’⁷¹ In other words, if the provider has some business motive, there is no doubt that it will qualify under the condition.⁷²

However, if it does not, and thus an economic motive is missing in their case, it depends on what interpretation is given to the term. The case law to date did not fully clarify whether the test is ‘objective’—ie a service is capable of being provided for remuneration, or is usually provided in such way by others—or ‘subjective’—ie a service is being provided for remuneration in this specific case.

I think that the objective test is more appropriate. With the subjective test, two persons in the same position can be treated differently only because they rely on different motives when doing the same thing. It would mean that non-profit entities or public services do not enjoy protections afforded to large corporations and limit the availability of enforcement tools in the DSA against such entities. Adopting the subjective interpretation would mean that national law can decide whether it wishes to extend the application of liability exemptions per analogy to such ‘non-economic’ services. This, in my view, would seriously compromise the harmonising effect and the effectiveness of the DSA. Digital offerings could escape DSA obligations by framing their activities as merely charitable or non-profit projects.

⁶⁷ *McFadden* (n 22) para 41.

⁶⁸ *McFadden* (n 22) para 42 (‘where the performance of a service free of charge is provided by a service provider for the purposes of advertising the goods sold and services provided by that service provider, since the cost of that activity is incorporated into the price of those goods or services’).

⁶⁹ *Papasavvas* (n 13) para 29.

⁷⁰ *ibid* para 30.

⁷¹ *McFadden* (n 22) para 41.

⁷² For a CJEU case supporting this reading, see Case C-339/15 *Vanderborght* ECLI:EU:C:2017:335.

The danger is real. The Slovak Supreme Court, applying the *McFadden* ruling,⁷³ recently opined that when a non-profit organisation operating a local news website hosts comments, it does not engage in economic activity.⁷⁴ As a result, the organisation does not benefit from the liability exemptions, and going forward, equally would not be subject to the due diligence rules of the DSA. The Member States can decide to align such situations with the DSA as they see fit. However, for liability exemptions, the human rights law can de facto impose an obligation to extend comparable regimes to non-profit actors.⁷⁵

While so far, we only have very few cases where providers would try to escape the definition of services, this might change under the DSA. Providers themselves have favoured and profited from wide interpretation. Under the pre-DSA legal landscape, ‘being a service’ meant benefitting from the treaty-based free movement of services; being an information society service means benefitting from the country-of-origin principle under the ECD; being an intermediary service means benefitting from a liability exemption. There were many benefits and few obligations. These changes under the post-DSA landscape create incentives to treat economic character as a loophole.

To close such a loophole, if a service can be turned into a business, regardless of whether it has already been, it should be viewed as a ‘service’. Thus, a non-profit service like Wikipedia, supported by donations, can always decide to sell insights,⁷⁶ should equally profit from liability exemptions, and be bound by DSA obligations. Its legal regime should not be dependent on the funding model of the service. This is in line with the traditional interpretation of the concept of ‘service’, which has been very broad.⁷⁷ Only such an objective reading assures that some players do not try to game the system by carefully timing their for-profit operations to avoid due diligence obligations.

This reading finds support in *European Commission v Hungary*, where the CJEU held that:

The decisive factor which brings an activity within the ambit of the FEU Treaty provisions on the freedom to provide services and, accordingly, of those relating to the freedom of establishment, is its economic character, that is to say, *the activity must not be provided for nothing*. By contrast, contrary to what is maintained by the Hungarian Government, *there is no need in that regard for the person providing the service to be seeking to make a profit...*⁷⁸

⁷³ *McFadden* (n 22).

⁷⁴ The Slovak Supreme Court (2022) Case No 9Cdo/78/2021, paras 34–37.

⁷⁵ Ch 3.

⁷⁶ Sarah Perez, ‘Google and the Internet Archive Are the First Customers to Gain Commercial Access to Wikipedia Content’ (*TechCrunch*, 29 June 2022) <<https://techcrunch.com/2022/06/29/google-and-the-internet-archive-are-the-first-customers-to-pay-for-commercial-access-to-wikipedia-content/>> accessed 1 August 2023.

⁷⁷ Lilian Edwards (ed), *The New Legal Framework for E-Commerce in Europe* (Hart 2005) 95.

⁷⁸ Case C-179/14 *European Commission v Hungary* ECLI:EU:C:2016:108, para 154.

Thus, whether an entity is seeking immediate profit is irrelevant. If it builds a digital service which generates value for others, it is not provided for nothing, irrespective of whether that value is converted into money.

A separate question concerns state-run services, such as domain name authorities for top-level domain names ('.fi' for Finland), run by the state in some countries. One can borrow from the CJEU's competition case law to consider whether these services qualify as a service. Here, the CJEU held that 'an undertaking is any entity engaged in an economic activity, irrespective of its legal status and the way in which it is financed'.⁷⁹ Any activity 'consisting in offering goods and services on a given market is an economic activity'.⁸⁰ Thus, the state may act as an undertaking, unless its activities 'fall within the exercise of public powers are not of an economic nature'.⁸¹ As long as economic activity can be separated, even if only in part, from the exercise of public powers, it is caught by competition law.⁸²

According to the case law,⁸³ the situation might depend on the underlying legislation. If the authority directly operates the service and charges fees on a statutory basis, its activities, such as domain name registration, are unlikely to qualify as an economic activity and, thus, a service. It would fall outside of the DSA. On the other hand, if the state only maintains legal supervision of the domain name authority but the operations are entirely outsourced to a third party and fees charges at its discretion, they should qualify as an economic activity. Again, from my perspective, it is irrelevant whether such service is then run for-profit (eg Slovak SK-NIC) or as a non-profit activity (eg Czech CZ.NIC or EU's EURid).⁸⁴ Obviously, the inapplicability of the DSA's rules does not preclude the states from adopting their own liability exemptions, or due diligence obligations, to such activities. Due to the inapplicability of the DSA, such exemptions are not pre-empted either. Thus, if a Member State operates one or more of such digital services, it can simply extend or even modify due diligence obligations in its national legislation.

6.3 Emerging Difficult General Issues

Before turning attention to specific liability exemptions, I wish to further discuss some of the difficult points that I see on the horizon as potentially important for the effectiveness of the DSA.

⁷⁹ Case C-138/11 *Compass-Datenbank GmbH v Republik Österreich* ECLI:EU:C:2012:449, para 35.

⁸⁰ *ibid* para 35.

⁸¹ *ibid* para 36.

⁸² *ibid* paras 37–38.

⁸³ *ibid* paras 42–48.

⁸⁴ European Parliament and Council Regulation (EU) 2019/517 of 19 March 2019 on the implementation and functioning of the.eu top-level domain name and amending and repealing Reg (EC) No 733/2002 and repealing Commission Regulation (EC) No 874/2004, art 9(2) on fees.

6.3.1 Impact of liability-excluding norms on liability-establishing norms

Liability exemptions function as liability exclusion provisions. They prevent European and national law, or their interpretation, from holding providers of such services liable. In other words, they only curtail the imposition of liability. The concept of ‘liability for third party information’ has an autonomous meaning, and it covers numerous areas of law, including civil, administrative, and criminal law, as long as the ultimate aim is to regulate the behaviour of content creators and hosts of such third-party information.⁸⁵ Similarly to the ECD, when the liability exemptions are no longer applicable because conditions are not fulfilled, it is up to other laws to establish any liability.⁸⁶

The Directive’s (the ECD), and now Regulation’s (the DSA), rules merely harmonise the exemption of liability, not the liability itself—it does not provide a positive basis for establishing when a provider can be held liable, which will depend on other legal instruments at the European or national level. Thus, in theory, there can be a gap.⁸⁷ On the other hand, this also means that the unavailability of the exemption does not automatically lead to liability; such a provider can, from the European perspective, also be declared ‘not liable’.

However, the relationship between liability exemptions and liability-establishing norms is further complicated by several factors.

First, the CJEU and national courts occasionally tend to establish liability at exactly the point where the exemption conditions are no longer satisfied (eg after a notice is not properly acted upon). Thus, the CJEU in *YouTube and Cyando* suggests that copyright liability for communication to the public will often coincide with a failure to satisfy the hosting liability exemption.⁸⁸ The judges applying liability-establishing rules alongside liability exemptions tend to be exposed to the anchoring effect of the exemptions. The two sets of rules thus can converge, although there is no legal requirement they do, and convergence can sometimes be counterproductive. This anchoring effect is not specific to EU law. Seeing liability exemptions as liability switches can be problematic because the policy reasons behind exempting liability can differ from those behind imposing it. The temptation to see what is exempted as the *only* appropriate course of conduct for a provider should be resisted. While for many services, such synchronisation of

⁸⁵ This issue was crucial in the pending Czech preliminary reference on unfair competition which was ultimately settled. Case C-470/22: *Request for a preliminary ruling from the Vrchní soud v Praze (Czech Republic) lodged on 14 July 2022—Česká národní skupina Mezinárodní federace hudebního průmyslu v I&Q GROUP, spol s r.o., Hellsy SE* [2022] OJ C418/12.

⁸⁶ The DSA does not impose the order in which the Member States apply the liability exemptions. They can, in theory, first apply liability provisions and then apply liability exemptions. However, this might sometimes risk misapplying the exemptions or applying them under the influence of national provisions. It might be more economical first to apply the liability exemptions and then liability provisions in national law, as the latter might have been devised long before these exemptions existed; thus, those liability provisions were not designed to avoid conflict.

⁸⁷ A good example is offered by the UK’s Defamation Act 2013 in s 5. See also *McFadden* (n 22). However, the DSA offers a number of accountability obligations imposed on providers while they act within the liability exemptions.

⁸⁸ *YouTube and Cyando* (n 28) paras 79–84.

exemptions and liability norms might not create problems, for some types of services,⁸⁹ or some types of liability,⁹⁰ it could have draconian effects. Thus, the fact that establishing liability is still a job of another set of legal norms should be always remembered. Switching off the immunity shield does not automatically mean switching on liability for others.

Second, liability-establishing norms that have their basis in EU law can sometimes complement or modify the DSA safe harbours. Only very rarely, as with Article 17 of the Copyright in the Digital Single Market (CDSM) Directive,⁹¹ do other EU rules specifically modify a liability exemption itself. Article 17 of the CDSM Directive introduces a special treatment for a subset of providers who are thereby explicitly excluded from the hosting exemption.⁹² A different example is the General Data Protection Regulation (GDPR), which has a less explicit relationship with liability exemptions. For instance, the GDPR's understanding of some hosting services differs substantially from the logic underlying the liability exemption regimes. However, the conflict between these special rules and the liability exemptions is not always real because two areas of law often regulate related aspects of the same business (eg data protection law regulates data collection designed around the collection and distribution of users' content). In fact, the complementary relationship between liability exemptions and other EU instruments is a much more frequent occurrence (see Chapter 17). The EU acts, such as the Terrorist Content Regulation or Audiovisual Media Services Directive, are excellent examples. These rules are perfectly compatible with the liability exemptions and other rules of the DSA but might contain further specifications of what is expected in certain sectors.

6.3.2 Neutrality and reliance on factual presumptions

One of the interesting and unresolved problems related to liability exemptions is to what extent the exemptions limit the use of factual presumptions or other evidentiary heuristics by national courts.

In *Bastei Lübbe*,⁹³ the CJEU addressed the question of whether an owner of an internet connection can be 'presumed' to be the wrongdoer in some circumstances.⁹⁴ German courts have developed a doctrine according to which if the connection were *prima facie* solely used by its owner, he would be subject to a rebuttable presumption

⁸⁹ An example of this is applying the same standard to cloud computing providers involved in hosting on the infrastructure level.

⁹⁰ An example of this is applying the same standard to criminal liability for terrorist crimes or civil liability for defamation.

⁹¹ CDSM Directive, art 17.

⁹² CDSM Directive, art 17(3) ('the limitation of liability established in Article 14(1) of Directive 2000/31/EC shall not apply to the situations covered by this Article') and the DSA, art 89(2) ('References to Articles 12 to 15 of Directive 2000/31/EC shall be construed as references to Articles 4, 5, 6 and 8 of this Regulation, respectively'), and specifically also supported by the DSA, art 2(4)(b).

⁹³ Case C-149/17 *Bastei Lübbe GmbH & Co KG v Michael Strotzer* ECLI:EU:C:2018:841.

⁹⁴ *ibid* para 20 (summarising the case law). See also German Federal Supreme Court case, BGH v 27 July 2017 – Case I ZR 68/16.

that he acted illegally. This requires the owner to explain and provide evidence of the opposite; otherwise, he is liable for transmitted information.

While the owner could be said to have acted as a mere conduit if other parties were involved, such as his family members, the presumption forces him to substantiate that he is a mere conduit, eg by naming persons who could have used his service. The CJEU did not consider the liability exemption dimension of the dispute. It ruled that such rebuttable presumption is not only acceptable but arguably partly required for the effective enforcement of intellectual property rights.⁹⁵ This poses an important question for the mere conduit liability exemption, as well as other liability exemptions. Are such presumptions a form of ‘liability for information transmitted’? If they are not rebutted, then this clearly manifests a liability for mere conduit service providers who may arguably be neutral (eg unaware co-tenants).

The difficulty with this rule is that the situation is akin to a national law that would condition the mere conduit exemption on disclosing some information. This would be incompatible with the DSA. However, if the rule is interpreted as a probability-based assessment of whether the mere conduit provider remained neutral, it could be more easily reconciled with Article 4 DSA. After all, the national courts must always make decisions in the context of factual uncertainty while relying on various heuristics.

This poses the question of *how far* the Member States and their courts can presume certain facts when the available evidence is limited. Undoubtedly, this question will come up before the CJEU. In *YouTube and Cyando*, the CJEU itself might be outlining an evidentiary standard concerning some of the infringements in copyright law that involves reliance on rebuttable presumptions.⁹⁶ Such presumptions were previously explicitly used by CJEU,⁹⁷ and thus, it is expected that the question of the limits of these presumptions will be tested sooner or later.

In its *YouTube and Cyando* judgment, the CJEU says that the following situations would fall outside the liability exemption and equally qualify as copyright infringement by the platform itself:⁹⁸

- the provider ‘participates in selecting’ infringing content;
- the provider ‘provides tools on its platform specifically intended for the illegal sharing of such content or that it knowingly promotes such sharing, which may be attested by the fact that that operator has adopted a financial model that encourages users of its platform illegally to communicate protected content to the public via that platform’;
- the provider, ‘despite the fact that it knows or ought to know, in a general sense, that users of its platform are making protected content available to the public illegally via its platform, refrains from putting in place the appropriate technological

⁹⁵ *ibid* paras 52–54.

⁹⁶ *YouTube and Cyando* (n 28) para 84.

⁹⁷ Case C-160/15 *GS Media BV v Sanoma Media Netherlands BV and others* ECLI:EU:C:2016:644.

⁹⁸ *YouTube and Cyando* (n 28) para 84; The case of Poland reiterates it as well, see *Republic of Poland v European Parliament and Council of the European Union* ECLI:EU:C:2022:297, para 27.

measures that can be expected from a reasonably diligent operator in its situation in order to counter credibly and effectively copyright infringements on that platform.⁹⁹

The first two scenarios are easily understood as situations where the intention is present. To participate, one must possess a will to join the action deliberately. To *induce* by providing tools, one has to envisage their use for such a purpose. The CJEU cross-referred to its case law on *The Pirate Bay*,⁹⁹ a provider whose intentions were evident to anyone. When it comes to hosting, such users would be likely understood to act under the authority or control of the service provider.¹⁰⁰

The last scenario is the most interesting. It seems to present an instance where the Court would be willing to *infer* the deliberate intent to participate in someone's wrong in the absence of other evidence of an initial common plan. In other words, it seems to envisage a scenario where deliberate collusion emerges from the interactions and mutual convenience of outcomes. In such a case, the Court appears to require evidence that the provider, once realising this, tries to counter this situation credibly and effectively. This does not mean it must do everything possible, but it must do more than pay lip service so that the Court may be convinced that it is not acting implicitly in concert. The Court's description of such a scenario suggests its *evidentiary nature*: when evidence of large-scale infringement is known to the provider, it must credibly dispel the suspicion that it is not acting in concert.

Basically, the burden of proof showing neutrality and lack of participation is shifted, following the establishment of some circumstances, to the provider who must dispel doubts about his neutrality and deliberate participation in the wrongs of others.

With this conceptualisation in mind, the standard is about a provider being a rogue player rather than failing once or twice. As a result, the evidence should be systemic, and the countermeasures neglected should be the low-hanging fruit that every reasonable actor would adopt in such a situation rather than the highest state of the art. After all, the test is used to *infer deliberate participation* in someone else's wrong—usually a high threshold. The intuition is that even if basic reasonable measures were withheld, and not applied, then the intentions of the hosting provider were not all that innocent and could have been aligned with those lawless users. In such a case, users do not misuse the service but use it as generally intended by the platform itself.

The CJEU will have to navigate the question of these presumptions delicately to maintain the balance the legislature tried to create. While, as in *McFadden*, it is understandable that the Court does not want to squeeze the procedural autonomy of the Member States, the lack of a common approach risks undermining the framework. The Court's passage from *McFadden* acts as a useful reminder of the conundrum:

⁹⁹ *The Pirate Bay* (CJEU) (n 54).

¹⁰⁰ DSA, art 6(2).

It is not for the Court to take the place of the EU legislature by subjecting the application of that provision to conditions which the legislature has not laid down ... To subject the exemption laid down in Article 12(1) of Directive 2000/31 to compliance with conditions that the EU legislature has not expressly envisaged could call that balance into question.¹⁰¹

6.3.3 The place of the neutrality test

Under the ECD, it was of no consequence whether the requirement of neutrality was understood as a test for ‘provided information’ or as a self-standing test derived from the recitals. Under the DSA, however, this changes. If the ‘provided information’ is stored by a provider, the DSA’s due diligence obligations apply even if the provider is not neutral. In contrast, if the information is interpreted as not ‘provided by recipients’, even though a provider stores it, the DSA’s due diligence obligations do *not* apply.

Recital 29 stresses that:

Whether a specific service constitutes a ‘mere conduit’, ‘caching’ or ‘hosting’ service depends solely on its technical functionalities, which might evolve in time, and should be assessed on a case-by-case basis.

Thus, the Recital makes clear that no other criteria, including neutrality, should be applied to the question of whether a service is regulated by the DSA. A contrario, this is also confirmed by Recital 18, which only says that ‘[t]he *exemptions from liability* established in this Regulation should not apply where, instead of confining itself to providing the services neutrally by a merely technical and automatic processing of the information provided by the recipient of the service, the provider of intermediary services plays an active role of such a kind as to give it knowledge of, or control over, that information’. Thus, the rest of the Regulations can continue to apply to them. This reading is reinforced by Recital 41 stating that ‘[t]he due diligence obligations are independent from the question of liability of providers of intermediary services which need therefore to be assessed separately.’

Finally, a similar point can be derived from Article 7. While the ECD included a cross-reference to a provider ‘when providing the services covered by Articles 12, 13 and 14’, the DSA refers merely to ‘intermediary services’ and the technical activities of transmitting or storing. This could be read as a mere simplification of the text. However, considering the above discussion, it stipulates that the prohibition of general monitoring *does* apply *whenever* providers exercise those technical functions, *regardless* of whether they eventually lose a liability exemption because they stop being neutral (see Chapter 5).

¹⁰¹ *McFadden* (n 22), paras 69–70.

Table 6.2 Legal concepts and their consequences

Legal concept	Legal consequences
Service as an ‘economic activity’	» determines whether the DSA applies at all.
Activity as ‘hosting’, ‘mere conduit’, ‘caching’	» determines whether the DSA applies at all.
Information is ‘provided by’ recipients of the services at their ‘request’	» determines whether the DSA applies at all;
The ‘neutrality’ of the provider vis-à-vis provided information	» determines whether the liability exemptions apply but not whether the due diligence obligations still apply; thus, services that adopt or instruct users’ content do not benefit from exemptions but might become VLOPs.

In my view, the DSA tries to make it clear that apart from the neutral intermediaries who benefit from Article 8, the provision also applies *whenever* due diligence obligations are imposed, including on non-neutral intermediaries.¹⁰² This is because the DSA, per Recital 30, explicitly submits its entire Regulation, and thus also the due diligence framework, to Article 8 scrutiny.¹⁰³ Thus, for instance, a provider of generative artificial intelligence (AI) that draws from submitted user-generated content is likely to be non-neutral vis-à-vis its input is unlikely to be covered by liability exemptions. However, such a provider remains subject to the DSA due diligence obligations and the Prohibition on General Monitoring (GMOP) and can become a very large online platform (VLOP).

This is not to say that Court should not delimit the scope of the DSA by interpreting the notion of ‘provided information’. Such test remains crucial to distinguish between user-generated-content services, and those without such a component. The courts and authorities have all the incentives to frame the test for ‘provided information’ very broadly if they wish to keep the scope of the applicability of due diligence obligations broader than the concept of neutrality. As far as liability exemptions are concerned, any over-broadness can still be mitigated through an independent narrower test of the neutrality of services. To illustrate this, consider the difference between two types generative AI systems: a) services built on top of content of users submitted them, and b) services built by pulling the content from the web. The former, as mentioned above, can qualify as hosts, but can still sometimes lack neutrality vis-à-vis their outputs. However, the latter cannot qualify as hosts because they are not provided with such user-generated content at all. The outcome then appears as shown in Table 6.2.

¹⁰² This is not that unconventional. The CJEU already held that the GMOP can still apply, eg in areas not covered by liability exemption, even in the offline context. For more on the debate, Husovec (n 27) 118.

¹⁰³ DSA, Rec 30 states that ‘[n]othing in this Regulation should be construed as an imposition of a general monitoring obligation or a general active fact-finding obligation, or as a general obligation for providers to take proactive measures in relation to illegal content’ (emphasis added).

Liability Exemptions: Specific Services

7.1 Introduction	123	7.4.1 Specifics of online marketplaces as hosts	133
7.2 Mere Conduits	123	7.5 Search Engines	136
7.3 Caching	126	7.6 Liability Exemptions Overlaps and Voids	143
7.4 Hosting	128		

7.1 Introduction

The three Digital Services Act (DSA) liability exemptions discussed in the previous chapter are built around different expectations. First, conduit immunity mostly expects providers to cooperate with the state authorities by following their orders. Second, the caching immunity expects speedy catch-up with those whose infringements they mirror. And finally, the hosting immunity imposes choreography of non-judicial notice and takedown upon providers. Each liability exemption has its own rules and specifics, which I will try to explain in this chapter. Some composite services, such as messaging apps or search engines, can see their different components fall under more than one liability exemption depending on how they operate (Chapters 7.6 and 9.2).

7.2 Mere Conduits

Article 3(g)(i) DSA defines the mere conduit services as ‘consisting of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network.’ Article 4 DSA then details the liability exemption as follows:

Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, the service provider shall not be liable for the information transmitted or accessed, on condition that the provider: ...

The logic behind the legal intervention remains the same as in 2000. The lowest parts of the technical infrastructure ‘stack’ are not expected to control the content that flows

through the ‘pipelines’ (Chapter 1). As much as postal services are not liable for the content of the letters and packages exchanged, internet infrastructure needs to have the same legal certainty that by facilitating, transmitting, and giving access to content which might be illegal, they are not, nor do they want to be, assuming any legal risk. The mere conduit exemption does this important job.

The provision covers services that provide ‘transmission’ or ‘access to’ any communication network. Unlike Article 12 E-Commerce Directive (ECD), the DSA’s text now explicitly covers liability for ‘transmission’ *and* giving ‘access to’ such provided information. The new wording extends the functionality of the provision. For instance, a pub owner who electronically and at a distance only provides codes to an open wi-fi operated by another company previously could not claim the liability exemption for the misuse of connectivity. Although such a pub owner gave access to a network, since liability was only exempted as regards the ‘transmission’, which he never carried out, there was no protection. Now, a pub owner can equally invoke the mere conduit provision because it is not liable for giving ‘access’.

The new wording was a long overdue demand by technical intermediaries who felt that the original liability exemption was too narrowly worded to cover only typical internet access providers. For years, various online intermediaries, such as content delivery networks or domain name registrars and registries, were unsure of whether they could invoke any exemptions. While many courts in the Member States often gave them some liability assurances,¹ the status quo did not help the internal market and caused fragmentation.

Recital 29 of the DSA now provides a long list of examples that intend to extend the application of the exemption to ‘generic categories of services, such as internet exchange points, wireless access points, virtual private networks, DNS services and resolvers, top-level domain name registries, registrars, certificate authorities that issue digital certificates, voice over Internet Protocol (IP) and other interpersonal communication services.’² It suggests the interpretation that providers of domain name services, such as domain name authorities (eg EURid), or domain name resolvers, are covered as mere conduits.³ These services can be said to provide *access* to the communication network, the internet, by offering a particular type of access service, being a translation

¹ In the German case of *ambiente.de*, the German Federal Supreme Court rejected the imposition of obligations on a domain name authority, citing the public interest in the cheap DNS infrastructure (BGH v 17 May 2001—I ZR 251/99). The Slovak Supreme Court reached a similar outcome on 12 July 2007, 3 Obo 197/06, *rover.sk*. See also the US case of *Lockheed Martin Corp v Network Solutions Inc* 141 F Supp 2d 648 (ND Tex 2001).

² Description of technical functioning, examples of services covered by art 12 ECD as well as ‘grey areas’ are provided by Sebastian Schwemer, Tobias Mahler, and Håkon Styri, *Legal Analysis of the Intermediary Service Providers of Non-Hosting Nature: Final Report* (EU Publications Office 2020).

³ The only relevant case to date was Case C-521/17 *Coöperatieve Vereniging SNB-REACT UA v Deepak Mehta* ECLI:EU:C:2018:639. However, the case did not clarify the issue. In the literature, Schwemer and colleagues expressed some doubts, but they did not seem to consider access-only mere conduits (probably influenced by the ECD’s original language). Their argument about domain name authorities providing ‘pointers’ is very much in line with the argument that such services provide access to the network, see Sebastian Felix Schwemer, Tobias Mahler, and Håkon Styri, ‘Liability Exemptions of Non-Hosting Intermediaries: Sideshow in the Digital Services Act?’ (2021) 8(1) Oslo Law Review 4, 14.

of an IP address to a domain name.⁴ The same applies to other services not mentioned in Recital 29, such as browsers, operators of nodes that help to re-route the internet traffic (eg Tor), and providers of video-communication tools (eg Zoom) or potentially even some operating systems.

This new wording should thus encourage national courts to apply the provision to less traditional infrastructure services⁵ and keep an open mind to new technological developments. Recital 29 acts as a sort of non-exhaustive, open list, referring to ‘a wide range of economic activities which take place online and that develop continually to provide for transmission of information that is swift, safe and secure, and to ensure convenience of all participants of the online ecosystem’.

A typical example of a service introduced to consumers only in the early 2000s is wi-fi hotspots. Today, wi-fi hotspots are ubiquitous—every hotel, public space, and restaurant offers a connection. Individuals share their internet connection with visitors. Wi-fi connection is promoted by states, including the European Union (EU).⁶ Only in 2016, however, did the Court of Justice of the European Union (CJEU) clarify that the providers of wi-fi hotspots benefit from the mere conduit liability exemption.⁷

For Article 4 DSA to apply, the relevant network does *not* have to be *public*. This means that transmission or access can relate to closed or private networks. Thus, even providers of some messaging apps can also be seen as providing transmission within and access to a communication network—the infrastructure allowing the connection between different phones. They also transmit the information. However, the problem that these messaging apps face is the issue of the duration of storage. According to Article 4(2) DSA:

The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.

The word ‘transmission’ suggests that the storage of information must only be transient. Although Article 4(2) DSA specifies that this ‘includes’ some forms of transient

⁴ DNS resolvers offer a technical translation service between a numerical IP address and an alphabet-based domain name (eg 2001:4860:4860::8888 for Google.com). Since such a translation service does not transmit the data (website’s content), it only provides simplified access to the communication network. The question remains how the CJEU will apply art 4(2) DSA, ie whether the IP address in the registry is seen as a tool of access or rather information to be stored only temporarily to enable transmission by someone else.

⁵ See, for instance, the Hamburg Regional Court ruling regarding DNS providers such as Quad9, LG Hamburg v 12 May 2021—310 O 99/21.

⁶ European Parliament and Council Regulation (EU) 2017/1953 amending Regulations (EU) No 1316/2013 and (EU) No 283/2014 as regards the promotion of internet connectivity in local communities [2017] OJ L286/1. The Commission proposal mentioned the intermediary liability question related to the provision of wi-fi hotspots (Wifi4EU), see Commission, ‘Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) No 1316/2013 and (EU) No 283/2014 as regards the promotion of Internet connectivity in local communities’ COM(2016) 589 final.

⁷ Case C-484/14 *Tobias Mc Fadden v Sony Music Entertainment Germany GmbH* ECLI:EU:C:2016:689.

storage, the word ‘transmission’ would still limit the storage. Messaging apps can operate in different ways. They can involve ‘permanent’ or only transient storage. The former would seem to exclude the application of the mere conduit exemption. In such cases, messaging apps relying on cloud-based storage might qualify as hosting providers instead (see section 7.6). On the other hand, if messaging apps only allow users to store the messages locally and only transmit the information, they can continue to qualify as mere conduits because they provide ‘access’ to the communication network.⁸ The likely test for ‘transmission’ is whether the period of storage is ‘longer than is reasonably necessary for the transmission,’ according to Article 4(2) DSA.

Apart from the overarching neutrality requirement (Chapter 6.2.4), the conditions for mere conduit liability exemption are that the provider: (a) does not initiate the transmission; (b) does not select the receiver of the transmission; and (c) does not select or modify the information contained in the transmission. Once these conditions are fulfilled, Article 4 DSA confers near-absolute immunity that cannot be retracted even by obtaining knowledge. Thus, an access provider notified about the illegal activity of a website on the internet has no general legal obligation to step in and block it for its customers. While authorities might be able to require the blocking, such orders or legislation must target specific websites (Chapters 5 and 8).

These three conditions are meant to prevent rogue actors from misusing the exemption to shield their illegal operations from liability. For instance, if a hotel owner providing open wi-fi were to instruct her employees or clients to engage in some illegal actions, the exemption would not apply. She could be said to have initiated the transmission or influenced what was transmitted. In such a case, the service provider ‘deliberately collaborates with a recipient of the services in order to undertake illegal activities.’⁹ The DSA and the ECD conceptualised such situations as active interventions that disqualify the mere conduit from the passive provision of the service. The same logic underlies the explicit requirements in Article 4(1) DSA against the initiation of *who* receives *what* transmission from *whom* on the network. The provider selecting any of these components is no longer a mere conduit.

If all the conditions are met, mere conduits cannot be held liable for the third-party information they have transmitted or given access to. Once the mere conduit liability exemption is inapplicable, the national law is free to impose liability.

7.3 Caching

Article 3(g)(ii) defines the caching services as ‘consisting of the transmission in a communication network of information provided by a recipient of the service, involving the automatic, intermediate and temporary storage of that information, performed for

⁸ But not as online platforms, as those exclude pre-approval (see DSA, Rec 14).

⁹ ECD, Rec 44; DSA, Rec 20.

the sole purpose of making more efficient the information's onward transmission to other recipients upon their request'. According to Article 5 DSA, its regime is defined as follows:

Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, the service provider shall not be liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient or secure the information's onward transmission to other recipients of the service upon their request, on condition that the provider: ...

Again, this provision is based on Article 13 ECD, which is the least litigated liability exemption of the three. The only change in the wording brought about by the DSA is the addition of the words 'or secure' when discussing the purpose of transmission. This alteration was motivated by the desire to capture the changing face of content delivery networks that increasingly not only, or not primarily, facilitate better and faster access to the network by providing geographically closer servers with copies of websites but also help to resolve and protect from various cybersecurity incidents, such as Distributed Denial-of-Service (DDOS) attacks. This regulatory change was already identified by the Commission in its Impact Assessment.¹⁰

Apart from the neutrality requirements, the specific operational requirements include: a) not modifying the underlying information, b) complying with the conditions on access to it, c) the industry rules regarding the temporal aspects of caching, and d) not interfering with the lawful use of technology to obtain data on the use of the information.¹¹ Finally, it is expected that the:¹²

Provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.

The caching exemption thus presents an immunity model close to hosting but with some additional protections. Caching services are not required to act upon notification if the targeted content was not removed from the original servers. They are generally only asked to *assess* whether the notified content was removed or disabled on the source website. If it was, an expectation to remove it is triggered; or the provider might expose

¹⁰ Commission, "Impact Assessment" (Commission Staff Working Document) Accompanying the Document "Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and Amending Directive 2000/31/EC" SWD(2020) 348 final, annex 9. This change was also favoured by Schwemer and colleagues, see Schwemer, Mahler, and Styri (n 2) 36.

¹¹ DSA, arts 5(1)(a)–(e).

¹² DSA, art 5(1)(e).

itself to liability. However, as long as it is still on the source website, actual knowledge of the illegality of information does not create any expectation to act. The only exception is if there is an order from an authority demanding the removal of such information. That order can also target the source website, which only refuses to implement it. An order targeting the caching provider must also comply (Chapter 8). Although compliance with the latter order is not presented as one of the conditions in Article 5(1)(e), it should equally lead to the loss of an exemption (argument *a minore ad maius*).

Examples of caching include stand-alone caching services and, increasingly, Content Delivery Networks (CDN), which incorporate caching services. The CDNs can be seen to incorporate various types of technical activities. Some of them can qualify as caching (temporary mirroring of content to a geographically closer location), hosting (for longer web hosting) or even mere conduit (a proxy reverse function that acts as an access point).¹³ This variety has also been identified and discussed in increasingly rich case law, particularly in Italy and Germany, where courts have struggled to determine whether the CDN services belong to a particular liability exemption and, if so, to which one.¹⁴ It remains to be seen whether the wording change and the clarification in Recital 29 mentioning the CDNs, together with reverse proxies or content adaptation proxies, will be sufficient to provide greater legal certainty.

In European case law, two other types of services are sometimes discussed in connection to caching. The first type of service is search engines that index the internet and create a ‘cache’ memory of its content to offer search results. Their potential status as caching services was fiercely debated in the negotiations of the DSA, as explained below. The second service is live streaming services, which is not mentioned in the DSA despite its increasing popularity. Livestreaming is often provided by dedicated services (such as Periscope), social media (such as Facebook), and video-sharing platforms (such as YouTube). Given the immediacy of the provision of content, these services fall in between traditional broadcasting, on-demand audio-visual services and digital user-generated services. The Commission detailed the potential qualification of livestreaming services in its Impact Assessment.¹⁵ However, those considerations led to little changes in the DSA’s text. This silence, however, should not, in my view, be interpreted as an exclusion but rather as calling for a ‘case by case’ assessment of the service at hand.

7.4 Hosting

Unlike the mere conduit services, which mainly cover the modern infrastructure behind the communication networks, hosting services often apply to the application

¹³ For the description and debate under the ECD framework, Schwemer, Mahler, and Styri (n 3).

¹⁴ See the Rome Commercial Court case, *Mediaset (RTI) vs Cloudflare* (2019) Case No 1932/2019 which was subsequently confirmed in Rome Commercial Court, *Mediaset (RTI) v Cloudflare* (2019) Case No 26942/2019; Cologne District Court case, LG Köln v 05.12.2019—Case 14 O 171/19 (*Universal Music GmbH v Cloudflare*).

¹⁵ Commission, ‘SWD(2020) 348 final’ (n 10) annex 9.

layer of the internet's technology stack. They cover services ranging from social media, discussion fora, online marketplaces, review websites, video-sharing services, and more. At the same time, the same exemption also applies to some infrastructure services, such as web-hosting services. Recital 29 DSA includes, eg 'categories of services such as cloud computing, web hosting, paid referencing services or services enabling sharing information and content online, including file storage and sharing'.

Admittedly, the presence of infrastructure-like services among mostly application-layer services is exceptional and requires careful distinguishing. As noted below, the DSA creates a new category of hosting services—online platforms—that better describes the application layer because they store and distribute information to the public as one of its main goals. All other hosting services that are not only excluded from the term due to their small size usually cover 'mere hosting' services that tend to cover the infrastructure, such as web hosting.

Article 6 DSA provides that:

Where an information society service is provided that consists of the storage of information provided by a recipient of the service the service provider shall not be liable for the information stored at the request of a recipient of the service on condition that the provider: ...

This wording mirrors that of Article 14 ECD, hence validating the legal approach supported by the ECD for 20 years and interpreted extensively by the CJEU. The scope of services remained unchanged. The CJEU so far has accepted the following services as covered by the hosting safe harbour: social media,¹⁶ online marketplaces,¹⁷ video-sharing platforms,¹⁸ cyber-lockers,¹⁹ and keyword-based advertising on search engines.²⁰ Other services that consist of 'storage of information' provided by others include storage of comments on blogs,²¹ or on social media by page administrators,²² services of app stores, cloud services and web hosting, distribution of Really Simple Syndication (RSS) feeds,²³ storage of user reviews,²⁴ and user offers of accommodation on sharing economy platforms.

The hosting safe harbour is subject to two main conditions. They apply if the provider:

¹⁶ Case C-360/10 *SABAM v Netlog NV* ECLI:EU:C:2012:85; Case C-70/10 *Scarlet Extended SA v SABAM* ECLI:EU:C:2011:771; Case C-18/18 *Eva Glawischnig-Piesczek v Facebook Ireland Limited* ECLI:EU:C:2019:821.

¹⁷ Case C-324/09 *L'Oréal SA and others v eBay International AG and others* ECLI:EU:C:2011:474.

¹⁸ Joined Cases C-682/18 and C-683/18 *Frank Peterson v Google LLC and others and Elsevier Inc v Cyando AG* ECLI:EU:C:2021:503 (*YouTube and Cyando*); Case C-401/19 *Republic of Poland v European Parliament and Council of the European Union* ECLI:EU:C:2022:297.

¹⁹ *YouTube and Cyando* (n 18).

²⁰ Joined Cases C-236/08 to C-238/08 *Google France SARL and Google Inc v Louis Vuitton Malletier SA* ECLI:EU:C:2010:159.

²¹ See, for instance, German Federal Supreme Court, BGH v 25 October 2011—Case No VI ZR 93/10; *Payam Tamiz v Google Inc* [2013] EWCA Civ 68.

²² The administrators of pages are hosting providers along with social networks.

²³ German Federal Supreme Court, BGH v 27 March 2012—VI ZR 144/11.

²⁴ German Federal Supreme Court, BGH v 23 June 2009—VI ZR 196/08 (*Spichmich.de*).

(a) does not have actual knowledge of illegal activity or illegal content and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or illegal content is apparent; and (b) upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the illegal content.²⁵

This wording again mirrors Article 14 ECD. Thus, all the pre-existing case law of the CJEU can apply to these requirements without any changes. According to CJEU in *Poland*, ‘for such an operator to be excluded, under Article 14(1)(a) of that directive, from the exemption from liability provided for in Article 14(1), it must have knowledge of or awareness of specific illegal acts committed by its users relating to protected content that was uploaded to its platform.’

The Court thus confirmed its earlier Grand Chamber ruling in *L’Oreal v eBay*, which held that knowledge under (b) can be obtained only by sufficiently precise and adequately substantiated notice.²⁶ In *YouTube and Cyando* and *Poland*, the Court also confirms that awareness itself must concern specific illegal acts. Typically, one can imagine that headline news about a case in the mainstream media can lead to awareness. The DSA, however, reiterates the original language of Article 14 of the ECD, which limited this standard of knowledge to only liability for damages. This means that on the national level, in situations where ‘awareness’ exists but ‘actual knowledge’ is absent, liability can be imposed only in the form of damages.²⁷ This has important consequences for various forms of criminal liability, which would always need to clear the hurdle of actual knowledge. In most cases, awareness and actual knowledge coincide as types of knowledge, but only the former can be derived from a broader set of circumstances.

In contrast, mere general awareness (abstract knowledge) of illegal activity is in itself insufficient. The DSA now dispels some of the doubts previously left open by the ECD. First, Recital 22 clearly says that relevant ‘actual knowledge or awareness cannot be considered to be obtained solely on the ground that that provider is aware, in a general sense, of the fact that its service is also used to store illegal content’. Second, for the first time, the law specifies the common Union requirements for notification in Article 16 DSA, which are based on previous case law. These requirements act as statutory clarifications of what type of notifications can lead to the hosting providers opening up to liability. The book extensively describes these requirements in Chapter 11.

In short, according to the *eBay* decision, the CJEU does not limit the acquisition of knowledge to notification only. In *eBay*, the Court held that:

Moreover, if the rules set out in Article 14(1)(a) of Directive 2000/31 are not to be rendered redundant, they must be interpreted as covering every situation in which the provider concerned becomes aware, in one way or another, of such facts or circumstances. The situations thus covered include, in particular, that in which the operator

²⁵ DSA, arts 6(1)(a)–(b).

²⁶ *eBay* (n 17).

²⁷ Miquel Peguera, ‘The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems’ (2009) 32 *Columbia Journal of Law & the Arts* 481.

of an online marketplace uncovers, as the result of an investigation undertaken on its own initiative, an illegal activity or illegal information, as well as a situation in which the operator is notified of the existence of such an activity or such information. In the second case, although such a notification admittedly cannot automatically preclude the exemption from liability provided for in Article 14 of Directive 2000/31, given that notifications of allegedly illegal activities or information may turn out to be *insufficiently precise or inadequately substantiated*, the fact remains that such notification represents, as a general rule, a factor of which the national court must take account when determining, in the light of the information so transmitted to the operator, whether the latter was actually aware of facts or circumstances on the basis of which a diligent economic operator should have identified the illegality.²⁸

The standard of ‘sufficiently precise’ and ‘adequately substantiated’ notifications is now cemented in the DSA through various provisions—Recitals 22 and 53 and Articles 16(2) and 20(3). The key summary is provided by Recital 53, which also incorporates *YouTube and Cyando’s*²⁹ recent clarification of the underlying standard of assessment of facts:

Where a notice contains sufficient information to enable a diligent provider of hosting services to identify, without a detailed legal examination, that it is clear that the content is illegal, the notice should be considered to give rise to actual knowledge or awareness of illegality.

A diligent economic operator serves as a benchmark for care with which providers must assess any sources of information. This is also the reading given to the provision by the national courts.³⁰ The CJEU is slowly developing the standard across various legal instruments. For instance, in data protection law, the delisting requests concerning factual inaccuracies in search engines must meet the threshold of the ‘manifest’ or ‘obvious inaccuracy’ that must be corroborated by evidence that ‘can reasonably be required’ in the circumstances.³¹ In *TU and RE v Google*, the Court explained the underlying rationale most vividly:

... when assessing the conditions for application laid down in Article 17(3)(a) of the GDPR, that operator cannot be required to *play an active role in trying to find facts* which are not substantiated by the request for de-referencing, for the purposes of determining whether that request is well founded ... the operator of the search engine

²⁸ *eBay* (n 17) paras 121–22 (emphasis mine).

²⁹ *YouTube and Cyando* (n 18).

³⁰ In *CG v Facebook Ireland Limited and McCloskey (Joseph)* [2016] NICA 54 [69]–[72], the Northern Irish Court of Appeal found that omission of the correct form of legal characterisation of the claim ought not to be determinative of the knowledge of facts and circumstances; rather, the perspective should be one of the diligent economic operators.

³¹ Case C-460/20 *TU and RE v Google LLC* ECLI:EU:C:2022:962, paras 68 and 72 (using the word ‘obvious’).

concerned *cannot be required to investigate the facts and, to that end, to organise an adversarial debate with the content provider seeking to obtain missing information concerning the accuracy of the referenced content ... such an obligation would impose on that operator a burden in excess of what can reasonably be expected of it in the light of its responsibilities, powers and capabilities ...* would thereby entail a serious risk that content meeting the public's legitimate and compelling need for information would be de-referenced and would thereby become difficult to find on the internet. In that regard, there would be *a real risk of a deterrent effect on the exercise of freedom of expression and of information if the operator of the search engine undertook such a de-referencing exercise quasi-systematically*, in order to avoid having to bear the burden of investigating the relevant facts for the purpose of establishing whether or not the referenced content was accurate.³²

The Court's reasoning thus makes clear that the knowledge standard prevents the providers from being subject to a post-notification obligation 'to play an active role in trying to find facts'. As was argued in Chapter 5, this is entirely in line with the overarching principle of a shared burden for social harms.

The DSA, however, puts more pressure on the notification process through due diligence obligations. Post-DSA, it will be much harder for hosting providers to disregard notifications. The DSA specifies *who* and in *what form* shall receive them. However, the broad scale of possibilities might be limited by the availability of evidence in practice. If a hosting provider acts on its own initiative (Article 7 DSA) and uncovers unlawful content that it disregards, the outside world might not have sufficient evidence to prove that this omission happened unless they get access to non-public information held by such providers. Therefore, notifications remain the most important and documentable vehicle for imparting knowledge about certain illegal acts.

In *YouTube and Cyando*, the Court clarifies that in determining whether the provider intervened, the relevant factors to consider include even circumstances where the provider who 'despite the fact that it knows or ought to know, in a general sense, that users of its platform are making protected content available to the public illegally via its platform, refrains from putting in place the appropriate technological measures that can be expected from a reasonably diligent operator in its situation in order to counter credibly and effectively copyright infringements on that platform'.³³ As explained in Chapter 6, I see this requirement as pertaining to the neutrality of the hosting provider, and not as a separate knowledge standard. It speaks to the issue of whether the hosting provider collaborates with its infringers. The CJEU's re-statement of the *YouTube and Cyando* ruling in *Poland* seems to confirm this.³⁴ As a result, general awareness is never sufficient to trigger knowledge. However, a failure to keep up with the threats on one's

³² *ibid* paras 70–71 (emphasis mine).

³³ *YouTube and Cyando* (n 18) para 84.

³⁴ *Poland* (n 18) para 28; *YouTube and Cyando* (n 18) paras 117–18.

own platform, to the extent that the provider is unwilling to counteract them by any credible means, can allow the courts to *infer* that platforms deliberately and intentionally collaborate with their lawless users. The evidence bolstering such inference should be serious (Chapter 6.2.4).

Since a good part of the DSA concerns hosting providers, a great deal of attention will be dedicated to them in the following chapters. Hosting exemption is, without a doubt, the heart of the DSA Regulation. Its preservation was never questioned by the Commission in its proposal or by co-legislators during negotiations.³⁵ The category of online platforms, including very large online platforms, is only its subset of hosting services. The DSA disentangles the due diligence obligations that apply to all hosting service providers by dividing them into several categories: ‘just’ hosting (eg cloud and web hosting) and online platforms, including very large online platforms (VLOPs). This is clearly explained in Recital 13, where co-legislators reinforced the need to exclude infrastructure services from the category of platforms:

... For the purposes of this Regulation, cloud computing or web-hosting services should not be considered to be an online platform where dissemination of specific information to the public constitutes a minor and ancillary feature or a minor functionality of such services. Moreover, cloud computing services and web-hosting services, when serving as infrastructure, such as the underlying infrastructural storage and computing services of an internet-based application, website or online platform, should not in themselves be considered as disseminating to the public information stored or processed at the request of a recipient of the application, website or online platform which they host.

However, the DSA drafting also shows that some types of services are under separate regulatory scrutiny, even among online platforms. The most vivid example is online marketplaces, which I will discuss next.

7.4.1 Specifics of online marketplaces as hosts

During the legislative debate, the biggest pressure to deviate from horizontal rules concerned online marketplaces and their situation in consumer law.³⁶ In Chapter 6.2.4, I explained why providers that fail to disclose the source of content could lose their neutrality. This was a key concern for the consumer interest groups. Online platforms that act as marketplaces and sellers in those marketplaces can cause a risk of confusion for average consumers.³⁷ In the legislative process, the

³⁵ Folkert Wilman, ‘The EU’s System of Knowledge-Based Liability for Hosting Service Providers in Respect of Illegal User Content—Between the e-Commerce Directive and the Digital Services Act’ (2021) 12(3) *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 317, 318.

³⁶ Interview with Irene Roche Laguna, Deputy Head of Unit for Coordination and Regulatory Compliance, European Commission (2021–23).

³⁷ While the Commission proposal referred to an ‘average and reasonably well-informed consumer’, the co-legislators, particularly the EP, limited the reference to an ‘average consumer’. However, this should not have any

questions around the specific liability of online marketplaces for product safety were considered to be ‘too sector-specific’ and better suited for the concurrent discussions around the review of the General Product Safety Directive³⁸ and the Product Liability Directive.³⁹ These negotiations ran in parallel and were equally informed by the existing and upcoming CJEU case law.

Article 6(3) of the DSA eventually states the following:

Paragraph 1 shall not apply with respect to the liability under consumer protection law of online platforms that allow consumers to conclude distance contracts with traders, where such an online platform presents the specific item of information or otherwise enables the specific transaction at issue in a way that would lead an average consumer to believe that the information, or the product or service that is the object of the transaction, is provided either by the online platform itself or by a recipient of the service who is acting under its authority or control.

Based on the definition of online marketplaces under the consumer acquis,⁴⁰ the provision seems limited to ‘B2C’ relationships and thus excludes consumer-to-consumer exchanges. However, as explained in Chapter 6.2.4, in my view, this provision only represents a broader rule grounded in the condition of neutrality of providers. The standard is clearly inspired by pre-existing CJEU case law in EU consumer protection law⁴¹ and the general neutrality requirement.⁴² Moreover, as shown below, it was recently further validated by certain developments in EU trademark law.

Following an Opinion of AG Szpunar,⁴³ the CJEU recently held in *Louboutin v Amazon* that the operator of a marketplace could itself directly violate the trademark law when it sells products of others:

practical effects; as for the CJEU, the two are in a relationship of a concept and a benchmark in many areas, including consumer and trademark law; see Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts [1993] OJ L095/29, Rec 18; and Case C-470/93 *Verein gegen Unwesen in Handel und Gewerbe Köln eV v Mars GmbH* ECLI:EU:C:1995:224.

³⁸ European Parliament and Council Regulation (EU) 2023/988 on general product safety, amending Regulation (EU) No 1025/2012 and Directive (EU) 2020/1828, and repealing General Product Safety Directive 2001/95/EC and Directive 87/357/EEC [2023] OJ L 135/1 (General Product Safety Regulation).

³⁹ Commission, ‘Proposal for a directive of the European Parliament and of the Council on liability for defective products’ COM(2022) 495 final (still in the legislative process at the time of writing).

⁴⁰ Art 2(n) of Directive 2005/29/EC as amended by Directive (EU) 2019/2161: “online marketplace” means a service using software, including a website, part of a website or an application, operated by or on behalf of a trader which allows consumers to conclude distance contracts with other traders or consumers; European Parliament and Council Directive 2005/29/EC concerning unfair business-to-consumer commercial practices in the internal market [2005] OJ L149/22, as amended by Directive (EU) 2019/2161 (Unfair Commercial Practices Directive).

⁴¹ Case C-149/15, *Sabrina Wathelet v Garage Bietheres & Fils SPRL* ECLI:EU:C:2016:840, para 41.

⁴² *Frank Peterson v Google LLC and others and Elsevier Inc v Cyando AG* ECLI:EU:C:2020:586, Opinion of AG Øe, para 152.

⁴³ Joined Cases C-148/21 and C-184/21 *Christian Louboutin v Amazon and others* ECLI:EU:C:2022:422, Opinion of AG Szpunar, paras 67, 71, and 73.

... where, in view of all the circumstances of the situation in question, such a user may have the impression that that operator itself is marketing, in its own name and on its own account, the goods bearing that sign. In that regard, the following are relevant: the fact that that operator uses a uniform method of presenting the offers published on its website, displaying both the advertisements relating to the goods which it sells in its own name and on its own behalf and those relating to goods offered by third-party sellers on that marketplace; the fact that it places its own logo as a renowned distributor on all those advertisements; and the fact that it offers third-party sellers, in connection with the marketing of goods bearing the sign at issue, additional services consisting inter alia in the storing and shipping of those goods.⁴⁴

The proposed reading of the neutrality test in Chapter 6 would produce the same outcomes as the *Louboutin* case and Article 6(3) DSA.

The Commission's proposal of the text of Article 6(3) was subject to strong discussions, in particular in the European Parliament (EP) Committee on the Internal Market and Consumer Protection (IMCO). The IMCO Committee favoured a much more radical approach. It proposed a new provision entitled 'liability of online platforms allowing consumers to conclude distance contracts with traders'.⁴⁵ The provision would (a) make the liability exemption conditional to the compliance with due diligence obligations or information requirements under consumer law;⁴⁶ (b) exclude the exemption of liability to online marketplaces for traders from third countries when there is no economic operator inside the EU, or the product is non-compliant; and (c) exclude the liability exemption where the online marketplace exercises 'decisive influence'. The concept of 'decisive influence' was proposed by some academics,⁴⁷ and consumer protection organisations have adopted it as their recommendations.⁴⁸ The concept was a combination of the neutrality test, further expanded by the criteria extracted by the CJEU in the *Uber* case to conclude that UberPop was not an information society service, but rather a transport service.⁴⁹

⁴⁴ Joined Cases C-148/21 and C-184/21 *Christian Louboutin v Amazon and others* ECLI:EU:C:2022:1016, para 54.

⁴⁵ Committee on the Internal Market and Consumer Protection, 'Draft Report on the proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (DSA) and amending Directive 2000/31/EC (COM(2020) 0825) (2021) 66.

⁴⁶ Adding such a link would, for instance, mean that (a) online marketplaces can be held liable for any infringement to the due diligence obligations, for instance, not to appoint a legal representative, which could be seen as disproportionate; and (b) compliance with such due diligence obligations would happen to be almost voluntary, as it would merely be an incentive to be covered from liability.

⁴⁷ Christoph Busch, Gerhard Dannemann, Hans Schulte-Nölke, Aneta Wiewiorowska-Domagalska, and Fryderyk Zoll, 'The ELI Model Rules on Online Platforms' (2020) 9 *Journal of European Consumer and Market Law* 61.

⁴⁸ The European Consumer Organisation (BEUC), 'Making the Digital Services Act Work for Consumers—BEUC's Recommendations' (BEUC 2020) 6.

⁴⁹ Case C-434/15 *Asociación Profesional Elite Taxi v Uber Systems Spain* ECLI:EU:C:2017:9811.

The proposal was rejected by the EP plenary, and it was not included in the EP's mandate. However, some elements were adopted in the recitals as potential guidance to interpret two important elements of the liability exemption for marketplaces. Recital 23 states that where the provider of an online platform allows consumers to conclude distance contracts with traders and it determines the price of the goods or services offered by the trader, it 'could' act under the control or authority of the provider of hosting services for Article 6(2) of the DSA. Article 6(3) of the DSA is further explained by Recital 24, which states some of the examples that 'could' be subsumed here, such as a failure to display clearly the identity of the trader pursuant to the DSA, withholding the identity or contact details of the trader until after the conclusion of the contract, or where an online platform markets the product or service in its own name rather than in the name of the trader who will supply that product or service.

The legislature's rejection of the concept of 'decisive influence' clearly rejected three specific criteria. Firstly, whether contracts were concluded in a 'closed environment', as it was felt that this could worsen the consumer experience and safety. Secondly, where the platform operator helps to prepare the terms of the trader-consumer contract, such as the form of consent, deadlines for withdrawal of consent, or delivery, feared to discourage uniformity and, once again, user safety. Finally, the idea of using the provision to discourage specific payment systems was also rejected because such systems are seen as great enhancers of trust rather than aggressive control techniques by providers. This was previously also recognised by the CJEU in *Airbnb*.⁵⁰

In conclusion, Article 6(3) is merely a further statutory manifestation of the underlying neutrality test that underlines the entire framework (Chapter 6.2.4).

7.5 Search Engines

It seems that European regulation of digital services has been, for more than two decades, unable to decide how to explicitly deal with at least one set of services—search engines. These services help to organise information for users. Specialised price-comparison search engines help consumers to select service providers and producers of their liking. Search engines, like Google Search or Bing, build an index of information and market offerings from all around the world, helping users to navigate the Web by crawling the Web and creating an index, often without seeking permission. While these services already existed at the time of the ECD's drafting, they were not explicitly addressed in the liability exemptions. The DSA largely repeats this course of action.

⁵⁰ Case C-390/18 *Airbnb Ireland* ECLI:EU:C:2019:1112, paras 62, 64.

The US Digital Millennium Copyright Act (DMCA), the ECD's counterpart and direct inspiration, included search engines as a separate category of exempted services.⁵¹ Recital 18 of the ECD mentions search engines only in a recital as an example of information society services. The legislative history seems unclear, but from the historical documents, it appears that the revision clause in Article 21 of the ECD could have been added as a response to the Irish insistence to create a separate rule for search engines.⁵² In its first implementation report (2003) on the ECD, the Commission reported that:

In addition to the matters dealt with by Articles 12–14, some Member States decided to provide for limitations on the liability of providers of hyperlinks and search engines. This was motivated by the wish to create incentives for investment and innovation and enhance the development of e-commerce by providing additional legal clarity for service providers. Whilst it was not considered necessary to cover hyperlinks and search engines in the Directive, the Commission has encouraged Member States to further develop legal security for internet intermediaries. It is encouraging that recent case-law in the Member States recognizes the importance of linking and search engines to the functioning of the internet.⁵³

Hungary, Poland, Portugal, and Spain have opted to extend the hosting immunity to the activities of search engines, while Austria, following an intense legislative debate, switched to the conduit model.⁵⁴ However, the practical impact of such exemptions is often unclear. In Austria, Article 14 of the Austrian E-Commerce Law does not allow any 'selection' or 'modification' of the information, and the provision was inapplicable to liability in image search due to modification of the indexed content, which could be equally problematic for text search results.⁵⁵

⁵¹ 17 USC § 512.

⁵² Permanent Representatives Committee, 'Extract of the Summary Record of the 1853rd Meeting of the Permanent Representatives Committee on 17 and 19 November 1999' (1999) Doc 12957/99 Ext 1 CRS/CRP 44 ECO 387 CONSOM 73 CODEC 714, 4 <https://resources.law.cam.ac.uk/cipil/travaux/ecommerce_directive/ecommerce_travaux_complete.pdf#page=325> accessed 5 August 2023 ('[Ireland] continued to propose an additional article on search engines'). However, Hoboken reports that proposals covering search engines were also tabled by the European Parliament, Joris van Hoboken, *Search Engine Freedom: On the Implications of the Right to Freedom of Expression for the Legal Governance of Web Search Engines* (Kluwer Law International 2012) 230 (however, with an unclear reference to sources).

⁵³ Commission, 'Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee - First Report on the application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)' COM(2003) 0702 final, para 67.

⁵⁴ *ibid.* See Austria: art 14 of E-Commerce-Gesetz (BGBl I Nr 152/2001) (ECG); Portugal: art 17 of Decreto-Lei n° 7/2004 de 7 de Janeiro (Electronic Commerce Law); Spain: art 17 of Ley N° 34/2002, de 11 de julio de 2002, de servicios de la sociedad de la información y de comercio electrónico (Act on Information Society Services and Electronic Commerce); Hungary: Act 153 of 2001 on Electronic Commercial Services and Certain Legal Aspects of Information Society Services, promulgated 24 December 2001; Poland: Ustawa o świadczeniu usług drogą elektroniczną (DZ U 2002 Nr 144, poz 1204) (Law Concerning the Provision of Electronic Services). See debate of national implementations in van Hoboken (n 52) 233ff.

⁵⁵ Austrian Supreme Court, OGH 20.09.2011, 4 Ob 105/11m ('the defendant's chosen presentation, which 'cut out' the photographs from the original page, altered the original information to the extent that the photographs were—in contrast to the original page were visible on the screen without a manufacturer's note').

Unsurprisingly, this situation led many to argue that search engines of various kinds are *not* covered by any of the three liability exemptions and remain subject to national experimentation foreseen by the review clause of Article 21 ECD.⁵⁶ In the only CJEU case dealing with the question, AG Maduro in *Google France* suggested, however, the opposite. He was of the view that Article 21 does not exclude application to search engines but only instructs the Commission to see if the potential (in) application of the existing framework needs to be adopted.⁵⁷ Based on that, he concluded that:

In my view, it would be consistent with the aim of Directive 2000/31 for Google's search engine to be covered by a liability exemption. Arguably Google's search engine does not fall under Article 14 of that directive, as it does not store information (the natural results) at the request of the sites that provide it. Nevertheless, I believe that those sites can be regarded as the recipients of a (free) service provided by Google, namely of making the information about them accessible to internet users, which means that Google's search engine may fall under the liability exemption provided in respect of 'caching' in Article 13 of that directive. If necessary, the underlying aim of Directive 2000/31 would also allow an application by analogy of the liability exemption provided in Articles 12 to 14 thereof.⁵⁸

Because the case concerned advertising in the search results and not organic search results, the above text was an obiter dictum, which the CJEU never had to address. However, the Court found that keyword advertising in web search results qualifies as hosting.⁵⁹

In the legislative process surrounding the DSA, the Commission's DSA proposal, they remained entirely silent in this regard, preferring to leave the questions to case law. The European Parliament proposed to add that search engines may qualify as caching services ('as to information included in the results') but also as hosting services (as to 'elements displayed alongside those results, such as online advertisements') on a case-by-case basis.⁶⁰ The Council proposed to introduce a new fourth category of liability exemptions for search engines with a regime similar to caching⁶¹

⁵⁶ van Hoboken (n 52), 229 ('Article 21 ECD on the re-examination by the European Commission suggests that search engines [information location tools] and hyperlinks are not covered by the intermediary liability regime of the Directive').

⁵⁷ Joined Cases C-236/08–C-238/08 *Google France SARL and Google Inc v Louis Vuitton Malletier SA* ECLI:EU:C:2009:569, Opinion of AG Maduro, paras 133–34.

⁵⁸ *ibid* fn 72.

⁵⁹ *Google France* (n 20) para 106.

⁶⁰ European Parliament, 'Amendments adopted by the European Parliament on 20 January 2022 on the proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (DSA) and amending Directive 2000/31/EC (COM(2020)0825 — C9-0418/2020 — 2020/0361(COD))' [2022] OJ C336/48, 65

⁶¹ General Secretariat of the Council, 'Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (DSA) and Amending Directive 2000/31/EC – General Approach' (2021) Document 13203/21, art 4 on "Caching" and online search engines' <<https://data.consilium.europa.eu/doc/document/ST-13203-2021-INIT/en/pdf>> accessed 1 August 2023.

and expand risk management to ‘Very Large Online Search Engines’ in the due diligence chapter.⁶² The Council’s liability exemption proposal was controversial because search engines would suddenly be free from notice and action procedures that are required from hosting but not from caching providers. Moreover, this would have granted them broader immunity than the one existing under the US copyright or current case law concerning the right to be delisted under the General Data Protection Regulation (GDPR).

According to Roche Laguna, the discussions around specific liability exemptions for search engines became a complicated battlefield during the negotiations with opposing and sometimes contradictory interests between creative industries, civil rights associations, and search engines of various sizes and types.⁶³ At a later point in the negotiations, the Council modified its negotiating position towards a fourth category of liability exemption to that of hosting services and subject to a similar knowledge standard. However, this was rejected by the European Parliament due to concerns about the risks to freedom of expression and information.

The final result is the introduction of the definition of search engines in the DSA, mimicking that of the Platform to Business Regulation, but the liability chapter remains silent on search engines (as did the Commission’s original proposal). Search engines are only mentioned as a generic type of intermediary provider that facilitates proper functioning of the internet, that can also benefit from the exemptions from liability, ‘to the extent that their services qualify as ‘mere conduit,’ ‘caching’ or ‘hosting’ services’ (Recital 27). With this, ‘very large online search engines’ are put at the same level in terms of due diligence obligations as ‘very large online platforms’, although they do not have one universal exemption.

The situation of search engines is further complicated because today’s generalist search engines are composite services that package many different technical activities into one product. However, these technical activities ‘source content’ differently: a) natural search results consisting of hyperlinks and short excerpts collected from websites on an opt-out basis, b) advertising results designed by advertisers who also select keywords to trigger them, c) suggestions in the search bar resulting from an algorithm that processes the most frequent queries of users, and d) finally, the archival copies of webpages interlinked with some results. To complicate things further, a subset of indexed websites has a more managed relationship with the search engine through various webmaster tools.

Thus, when discussing search engines and their liability exemptions, the discussion must always first clarify which part of the search engine is discussed. There is no single regime for all the above technical functions. Usually, the talks about a ‘missing’ liability exemption for search engines refer to liability for text indexed in the natural search results. This must be distinguished from *advertising results* that are clearly

⁶² *ibid* 64, Rec 69.

⁶³ *Interview with Irene Roche Laguna* (n 36).

covered as hosting following *Google France* ruling or *search suggestions* delivered via autocomplete that are not because they are content produced by search engines themselves.⁶⁴

In my view, the historical argument for the positive exclusion of any part of search engines based on Article 21 ECD was never too strong. The legislative history, at best, shows that given the US model, it was not clear how the lack of an explicit category would be applied by European courts. Thus, one cannot infer that search engines were not meant to be covered by the framework *if* the conditions of one of the exemptions are met simply because the review clause of the ECD stressed the need to review the situation. Natural search results store and organise other people's information (excerpts and links). Recipients of search results are the indexed website owners. However, to qualify for the hosting service, Article 3(g)(ii) DSA, as the ECD before, requires 'the storage of information [to be] provided by, and at the request of, a recipient of the service'. The key problem is whether websites that do not opt out of indexing by search bots can be said to 'provide' the information to search engines at the website owners' 'request'. So far, no CJEU case has confirmed this. Nevertheless, in my view, we can say that at least for some natural results displayed in the generalist search engines, there is little reason not to qualify them as hosting (see option three below).

Thus, 22 years after the adoption of the ECD, the attempt to create an explicit liability exemption failed. This outcome creates a lot of uncertainty. Unless the CJEU explicitly addresses the status of natural search results, national case law among the Member States will likely diverge. In contrast to the days of the ECD, the proper classification of natural search results under the DSA carries some immense consequences.

Firstly, proper interpretation determines whether the Member States can create or maintain their specific liability exemptions for search engines or whether they are pre-empted by the full harmonisation effect of the DSA. Secondly, search engines, their users and victims might not know which baseline legal expectations apply. Should providers put in place a notice and action mechanism like hosting providers? Should they send statements of reasons? If so, to whom? Should they then forward those statements of reasons to feed the database to be put in place by the Commission?⁶⁵ If natural search results are hosting services, are they also platforms if they disseminate content to the public? Moreover, not all search engines function the same way. Will clarity as to what the classical, big search engines must do also apply to those who do not generate their own index of the internet and only syndicate the indexes of some other search engines? Will these standards also apply to specialist search engines?

⁶⁴ German Supreme Court, BGH v 14 May 2013—Case No VI ZR 269/12, paras 19ff; Austrian Supreme Court, OGH 30 March 2016, 6 Ob 26/16s, para 3.3 (rejects liability exemptions).

⁶⁵ As Google already does today to the Lumen database; see the Lumen Database <<https://www.lumendatabase.org>> accessed 1 August 2023.

In my view, the Court has four options.

The *first option* is to deny the applicability of any liability exemptions to natural search results with an argument that the legislature excluded such services through the original review clause of the ECD. Very large online search engines (VLOSEs) would be subject to uniform European due diligence obligations but diverging national liability regimes. However, this will cause difficulties for the DSA because such providers are asked to assure the same level of risk mitigation across the Union even though their liability question would be treated differently. For instance, if Austrian law imposing the conduit regime was respected, the due diligence obligations could hardly request notice-based content moderation to mitigate risks. Not only is this option sub-optimal from the perspective of the EU single market, but it also does not find much support in history.

The *second option* would be to accept that storing and ranking natural search results concerning all websites constitutes the activity of hosting despite search engines dispatch crawlers to collect such information without seeking opt-in. The CJEU would need to recognise that even implicit provision of information by recipients of the service, that is, by not opting out of the industry standard, is sufficient to ‘provide’ such information at the ‘request’ of those websites. To date, similar logic was accepted in copyright law, but never for a liability exemption itself.⁶⁶ However, even if the Court did this, the question of the provider’s neutrality would need to be addressed to provide a complete answer. The additional advantage would be that while the Court would have to see to what extent the content moderation due diligence obligations can be applied to search, they would form a common baseline for the special risk management system foreseen by the DSA. The Court could easily synchronise its reading with the GDPR.

The *third option* would be to limit hosting liability exemption to only websites with more managed relationships with search engines. Some websites proactively submit information about themselves to search engines, sometimes using the provided interfaces, such as webmaster tools. In these cases, there is explicit provision and request to store information in some form. While this would only solve the problem of search engines’ liability for some websites, arguably, it would apply to the key parts of the digital ecosystem. It would incentivise search engine providers to treat the content of websites with less-managed relationships differently.

The final *fourth option* would be to liken the search engines to caching. That said, I personally see little reason why storing and sorting content in a quasi-permanent index should be viewed as temporary storage that facilitates access to information. Many hosting services already facilitate access, too, and are not treated as caching. Moreover, if one accepts that caching services should be inherently less involved in

⁶⁶ German Federal Supreme Court, BGH v 29 April 2010—I ZR 69/08 (*Vorschaubilder*).

modifying the information compared to hosting, natural search results could easily lose such exemptions due to a lack of neutrality, exemplified by some national case law cited above.

In my view, the second option seems possible, and the third option seems safe. If the Court recognised natural search results as hosting, as some courts already do,⁶⁷ the DSA would gain a better grip on the services. Not only do many search engines already operate under hosting's notice and takedown choreography, but some other areas of EU law already impose liability on them, which seems to replicate (in effect) the hosting exemption model. In EU copyright law, it was found that placing unauthorised content in the natural results implicates the search engine only upon notification⁶⁸ and that search engines should not be subject to general monitoring.⁶⁹ Even in right-to-be-delisted cases under the GDPR, the CJEU accepted that requests trigger the obligations.⁷⁰ The decisions concerning search engines often emphasise their importance for the health of the digital ecosystem and the freedom to convey and receive ideas within it.⁷¹ According to *AG Maduro*, search engines are neutral⁷² and some national courts already argued that such results are not perceived as the search engine's own content.⁷³ Finally, this option would be in line with the US copyright regime and the way how many companies already operate even in other areas that are clearly outside of the liability exemptions.⁷⁴

If the Court were to decide in favour of the first option, the Court would find it hard to avoid harmonising law through due diligence obligations. For instance, the rules prescribing mitigation of risks, including preventing over-removal, can hardly achieve the same effects in two countries that expose the search engine to two different liability schemes: knowledge-based standards or stricter forms of liability. The Court will, therefore, have to consider how the accountability rules and the need for their effectiveness might indirectly shape the liability frameworks that are not explicitly harmonised. For instance, it can consider the pre-emptive effect of rules, such as Articles 34–35, on the national liability frameworks.

Even more so than in other areas, the CJEU's interpretation of this will be key. I will show in the due diligence chapters (Part III of this book) that applying

⁶⁷ The most recent example is when the Italian Supreme Court found that search engines are, in principle, eligible for the hosting liability exemption (Italian Supreme Court, Cass, 8 June 2022, n 18430) and hence should honour valid notices to be exempted from liability.

⁶⁸ German Federal Supreme Court, BGH v 15 September 2017—I ZR 11/16 (*Vorschaubilder III*) paras 63, 67.

⁶⁹ *ibid* para 62; this is part of the assessment in InfoSoc Directive, art 3.

⁷⁰ Case C-136/17 *GC and others v CNIL* ECLI:EU:C:2019:773, para 47 ('the prohibitions and restrictions in Article 8(1) and (5) of Directive 95/46 and Articles 9(1) and 10 of Regulation 2016/679 ... can apply to that operator only by reason of that referencing and thus via a verification, under the supervision of the competent national authorities, on the basis of a request by the data subject') (emphasis mine).

⁷¹ For instance, in Germany: German Federal Supreme Court, BGH v 27 February 2018—VI ZR 489/16 (defamation, for results in SE), paras 32–33 and 35–36; *Vorschaubilder III* (n 68) paras 54–56 and 60. In the Dutch case law, Hoboken reported a similar hosting-like regime in 2012, van Hoboken (n 52) 235.

⁷² *Google France (Opinion of AG Maduro)* (n 57) para 144.

⁷³ German Federal Supreme Court, BGH v 27 February 2018—VI ZR 489/16, paras 28–29.

⁷⁴ BGH v 14 May 2013—Case No VI ZR 269/12 (n 64) (notice-based liability for defamation even though suggestions are not covered by a liability exemption); similarly, in BGH v 27 February 2018—VI ZR 489/16 (n 73) para 36.

content moderation safeguards is crucial for many of the existing problems across a wide range of areas. While the DSA's content moderation chapter needs some adjustment to reflect the specifics of search engines, the problem is not dissimilar from the Court's task of adjusting the data controller responsibilities of search engines in data protection law.

7.6 Liability Exemptions Overlaps and Voids

Some providers of technical services were not included among the covered relevant technical activities by the EU legislature's choice. National laws can offer them additional liability exemptions or make them subject to different due diligence obligations; however, they must first rightly establish that the DSA does not regulate such services. This is more easily said than done, as seen in the example of search engines.

Moreover, one product might sometimes fall under more than one liability exemption, and such an *overlap* of exemptions can trigger a potential clash.

Firstly, some services might be concurrently described as 'storage' (hosting) and 'transmission' (conduit).⁷⁵ The typical case is messaging apps—cloud-based apps are hosting, while cloudless apps are conduits (Chapter 9). Secondly, sometimes 'access' could rival 'caching', such as in the case of CDNs. In both situations, if two exemptions cover the same activity, the CJEU will have to decide which of the two exemptions should be preferred. As discussed in the section about mere conduits, the temporal character of storage should be able to resolve many of these cases (ie more permanent storage leading to hosting). Similar considerations could be employed between the overlap of mere conduits and caching (see, respectively, Articles 4(2) and 5(1)(c) DSA).

In contrast to an overlap, a more frequent situation encountered is that of bundled and composite services.

Bundled services offer separable services in one consumer bundle. For instance, in the same product package, telecommunication companies can provide conduit services (eg the Internet connection, a public wi-fi hotspot), caching services (eg to ensure smooth streaming), hosting services (eg cloud space for private use), along with other retransmission of editorial content (eg TV 'on-demand'). The liability exemption under Articles 4–6 DSA only cover the particular services covered under such category, but not the others (eg TV on demand). In most cases, it is irrelevant that such services are offered together. This differs from what I call *composite* services, such as search engines—where several technical functions are integrated into a single service. The DSA tries to surgically separate the technical functions of such services for the purposes of liability exemptions. Thus, two different regimes can be applied if one can easily separate advertising from autocomplete results.

⁷⁵ The CJEU very indirectly touched on the issue in *Google France* without providing much guidance. *Google France* (n 20) para 111.

However, accountability under the DSA operates with a broader notion of the ‘service’ that includes the entire separable user experience. Thus, an online platform might be accountable for respecting due diligence obligations for product features that do not qualify as hosting if they are built as inseparable components of the same business product (Chapter 9.2.2). This means that for due diligence obligations, even own editorial content integrated with non-editorial content can become regulated to some extent (eg the sale of own goods and those of others; the publication of one’s own articles along those of the users).

8

Injunctions and Orders

8.1 Introduction	145	8.4 Content Orders (Article 9)	153
8.2 Scope of Permitted Injunctions	146	8.5 Information Orders (Article 10)	156
8.3 DSA Rules on Orders Issued by Authorities	151	8.6 Conclusion	157

8.1 Introduction

The liability exemptions block the majority of legal claims within their scope. One notable exception is orders or injunctions issued by the administrative or judicial authorities. Such orders are *exempted* from the liability exemptions. The rationale here is simple. Liability assurances should not thwart the ability of the state to enforce the law in individual cases. In the E-Commerce Directive (ECD), each liability exemption was thus accompanied by the following *injunction clause*:

This Article shall not affect the possibility for a judicial or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.¹

In the Digital Services Act (DSA), this wording did not change at all. The injunction clauses guarantee but do not grant the power of *authorities* to issue requests 'to terminate or prevent' unlawful acts. The legal basis for such state powers is usually to be found in national law. The injunction clauses serve only as a 'green light' and not as a 'push'.² Furthermore, the green light is only given to the authorities who must approve such measures to be able to pierce the liability exemptions; everyone else wishing to impose such obligation will see a red light.

¹ ECD, arts 12(3), 13(2), and 14(3).

² Martin Husovec, 'Holey Cap! CJEU Drills (yet) Another Hole in the e-Commerce Directive's Safe Harbours' (2017) 12(2) Journal of Intellectual Property Law & Practice 115, 120.

8.2 Scope of Permitted Injunctions

The permitted injunctions are arguably broad enough to cover the majority of the orders of authorities. In *Glawischnig*, the Court interpreted Article 18(1) ECD, which complements the injunction clauses, as affording the Member States ‘a particularly broad discretion in relation to the actions and procedures for taking the necessary measures.’³

The main goal of injunctions is to compel the cooperation of providers. The ECD and the DSA both permit injunctions ‘to terminate or prevent an infringement’ of users using the services.⁴ Article 18(1) ECD, which imposes a positive obligation on the Member States to introduce ‘court actions’ to provide for rapid responses to infringements, specifies that the resulting measures must be ‘designed to terminate any alleged infringement and to prevent any further impairment of the interests involved’. The objective of the provision is to protect rights in *individual cases*. Thus, any individual whose rights are wronged, regardless of the exemption, should be able to approach authorities in accordance with the national law and get orders to protect their interests. In contrast, the goal is not to dissuade the providers themselves from doing something, but is to oblige providers to cooperate to protect individuals in specific situations. The measure should assist in effective law enforcement and, at most, discourage the future unlawful actions of users of services that might be committed against that individual.

The Court of Justice of the European Union (CJEU) accepted, for instance, that website blocking,⁵ password-locking,⁶ termination of accounts,⁷ filtering,⁸ or information disclosures,⁹ constitute such orders. In contrast, ‘shutdown injunctions’ directed at intermediary services prohibiting the provision of service itself due to users’ content would exceed the scope of the injunction clauses. Such an injunction would be preempted by Articles 4(1), 5(1), and 6(1) DSA because it is not foreseen by Articles 4(3), 5(2), and 6(4) DSA. It aims to hold the service liable for the actions of its users. Instead of remedying an individual situation, it forces the shutdown of an entire service. The injunction would thus violate the objective to enforce cooperation within the framework of liability exemptions and instead rewrite the expectations set by the legislature.

The DSA now provides two examples of the most common types of orders:

³ Case C-18/18 *Eva Glawischnig-Piesczek v Facebook Ireland Limited* ECLI:EU:C:2019:821, para 29.

⁴ This language is present in the injunction clauses and in art 18 ECD. Historically, the language was broadened in the legislative process since the proposal at first limited injunctions to prohibitive injunctions. See KJ Koelman, ‘Online Intermediary Liability’ in PB Hugenholtz (ed), *Copyright and Electronic Commerce, Information Law Series-8* (Kluwer Law International, 2000) 38–39, 48–68.

⁵ Case C-314/12 *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH* ECLI:EU:C:2014:192.

⁶ Case C-484/14 *Tobias McFadden v Sony Music Entertainment Germany GmbH* ECLI:EU:C:2016:689.

⁷ Case C-324/09 *L’Oréal SA and others v eBay International AG and others* ECLI:EU:C:2011:474.

⁸ Case C-360/10 *SABAM v Netlog NV* ECLI:EU:C:2012:85; *Glawischnig* (n 3).

⁹ See for instance: Case C-275/06 *Productores de Música de España (Promusicae) v Telefónica de España SAU* ECLI:EU:C:2008:54; Case C-461/10 *Bonnier Audio AB and others v Perfect Communication Sweden AB* ECLI:EU:C:2012:219.

- *Content orders*: order ‘to act against’ specific ‘illegal content’ issued by the relevant national judicial or administrative authorities (Article 9).
- *Information orders*: order ‘to provide’ specific ‘information about recipients of the service’, issued by the relevant national judicial or administrative authorities (Article 10).

There are other orders issued by the authorities that will not qualify as either of the two but still require ‘termination or prevention’, such as preservation orders. Some sectorial European Union (EU) rules, such as the Terrorist Content Regulation (TCR), can impose additional requirements. For instance, Articles 3–6 TCR regulate removal and preservation orders targeting terrorist content more elaborately. In another instance, under intellectual property law, some orders are prescribed to the Member States in the Internet Protocol (IP) Enforcement Directive.¹⁰ In the third sentence of Article 11, the IP Enforcement Directive obliges the Member States to introduce injunctions against intermediaries to assist in the enforcement of IP rights if they are not themselves liable under tort law.¹¹ The IP Enforcement Directive outlines a broad set of requirements, some of which are now echoed in Articles 9–10 DSA.

Injunctions permitted by injunction clauses represent a form of liability otherwise caught by the liability exemptions.¹² Thus, only those injunctions permitted explicitly by injunction clauses are legally possible. The wording of injunction clauses is limited to orders issued by authorities to ‘terminate or prevent’ unlawful acts. The CJEU in *McFadden* spoke of ‘seeking before a national authority or court to have the service provider prevented from allowing that infringement to continue’.¹³ Under the ECD, some have tried to argue that it does not contain a requirement for supervision by an authority or a court because the wording only reflects the nature of a Directive addressed to the Member States.¹⁴ The reinsertion of the same language in a Regulation should dispel any doubts about the meaning of the injunction clauses.

Supervision by the state is a must to receive the so-called ‘green light’ from the provision. The Member States have the discretion to decide which authorities to choose and how to exercise these powers; however, they must allocate such powers to some state bodies. Historically, this procedural safeguard was imposed to make sure that measures exempted from liability exemptions do not endanger the internal market. The rationale was that only the authorities can be trusted.

This reading is also clear in the *Glawischnig* ruling, where the Court rightly conceptualises the injunction clauses in light of a general positive obligation to create rapid

¹⁰ Same as art 8(3) InfoSoc Directive.

¹¹ See Martin Husovec, *Injunctions against Intermediaries in the European Union: Accountable but Not Liable?* (CUP 2017).

¹² See more extensively, Husovec, ‘Holey Cap! CJEU Drills (yet) Another Hole in the e-Commerce Directive’s Safe Harbours’ (n 2).

¹³ *McFadden* (n 6) para 77.

¹⁴ For this view, see Daniel Holznagel, ‘Der neue § 7 Abs. 3 Satz 1 TMG: Richtervorbehalt für die zivilrechtliche Störerhaftung von Host Providern?’ (2017) 11 *Computer und Recht* 738; for the opposite view, Husovec, *Injunctions against Intermediaries in the European Union* (n 11) 63.

measures in the national law to facilitate the enforcement of rights following Article 18 ECD.¹⁵ According to the Court:

Recital 52 of that directive states that the specific character arising from the fact that the damage which may arise in connection with information society services is characterised both by its rapidity and by its geographical extent, and also by the need to ensure that national authorities do not endanger the mutual confidence which they should have in one another, *led the legislature of the European Union to request Member States to ensure that appropriate court actions are available*.¹⁶

Next to injunctions, the CJEU also exempts associated *costs* incurred when seeking them before authorities. In *McFadden*, the Third Chamber held that an intermediary could be requested to comply with an injunction and asked to reimburse the associated costs.¹⁷ However, the Court did *not* clarify whether such compensation is provided on the condition that the injunction proceedings of Article 12(3) ECD are eventually instituted.¹⁸ It also did not clarify if exemptions offer a way to moderate these costs. I have previously criticised this approach extensively.¹⁹ Its practical consequences are quite clear. The Member States can use the costs to influence whether providers even wait for an order to comply with their requests. For instance, the authorities could impose procedural fees on providers whenever they issue a blocking order. Such national laws risk incentivising providers to block websites without awaiting such orders to avoid paying the costs. This undermines the very idea of authorities overseeing the balancing and issuing of such decisions. In the coming years, the Grand Chamber of the CJEU should consider how to add nuance to *McFadden*'s very unclear standard to avoid these consequences.

AG Szpunar in *McFadden* proposed one potential interpretation. In his view, one has to be careful not to 'compromise the objective pursued by Article 12 of Directive 2000/31 of ensuring that no undue restrictions are imposed on the activities to which it relates'.²⁰ To avoid this, providers 'may incur liability only *after* a specific obligation contemplated by Article 12(3) of Directive 2000/31 has been imposed on him' and thus not before the exemption is lost or an injunction granted.²¹ This reading would still allow the imposition of costs for non-compliance with injunctions in the follow-on enforcement. Thus, a provider unwilling to comply with an order, eg to block a website, could still be fined. Alternatively, the CJEU could moderate the costs of seeking such orders

¹⁵ ECD, art 18: 'Member States shall ensure that court actions available under national law concerning information society services' activities allow for the rapid adoption of measures, including interim measures, designed to terminate any alleged infringement and to prevent any further impairment of the interests involved.' See *Glawischnig* (n 3) paras 27–30.

¹⁶ *Glawischnig* (n 3) para 28 (emphasis mine).

¹⁷ *McFadden* (n 6) paras 75–79.

¹⁸ Husovec, 'Holey Cap! CJEU Drills (yet) Another Hole in the e-Commerce Directive's Safe Harbours' (n 2) 117–20.

¹⁹ *ibid*.

²⁰ Case C-484/14 *Tobias McFadden v Sony Music Entertainment Germany GmbH* ECLI:EU:C:2016:170, Opinion of AG Szpunar, para 77.

²¹ *ibid* para 79.

to prevent the circumvention of the state supervision. This would afford the Member State full procedural autonomy when fashioning their tools while allowing the CJEU to control whether the DSA's objectives are compromised.

The state supervision of orders has far-reaching consequences in some areas, such as copyright law.

After adopting the Copyright in the Digital Single Market (CDSM) Directive and the CJEU's acceptance of filtering in its case law, there have been attempts to impose similar filtering through a backdoor—injunctions against intermediaries. The logic is as follows. If injunctions can be imposed on providers of hosting services, irrespective of their liability, then filtering could be imposed as part of the measures to prevent infringement. This is correct if the filtering measures comply with the prohibition of general monitoring obligations and fundamental rights. However, some courts take an additional step, which makes it highly problematic. Some national courts keep deciding that such filtering obligations can be imposed whenever a copyright holder asks a provider to implement filtering for its protected material without a need to go to the courts or authorities.²² Effectively, this 'nonjudicial stay-down' replicates the filtering under Article 17(4)(b) CDSM Directive. In my view, it clearly violates Article 6(1) and (4) DSA and previously violated Article 14 ECD.

The courts and authorities can issue orders mandating the implementation of compliant filtering measures; however, this should only be for individual works of plaintiffs subject to the lawsuit. Thus, stay-down is possible, subject to limitations of the CJEU case law, but only in order and stay-down choreography.²³ This assures that the state oversees the grant and implementation of such filtering measures.

Injunction clauses in Articles 4(3), 5(2), and 6(4) DSA represent a broader safeguard of the independent oversight of any measures imposed on providers. They assure that orders, such as website blocking requests, account terminations, or information disclosures, should be overseen by authorities subject to the Rule of Law safeguards. They allocate oversight and thereby protect against abuse. It is worth highlighting that intermediaries are usually not prohibited from complying with private requests. In the absence of such prohibitions,²⁴ incentives to comply with requests dressed as claims for injunctions endanger the safeguards the DSA puts in place for these exact scenarios.

The references to authorities in Articles 4(3), 5(2), 6(4), and 9–10 also cover the EU bodies. Article 8 prohibits general monitoring obligations from any state power. Articles 4(3), 5(2), and 6(4) speak of authorities which act 'in accordance with Member States' legal systems'. When EU bodies act according to the law, they must inevitably

²² The German Supreme Court, BGH v 2 June 2022—Cases Nos I ZR 140/15, I ZR 53/17, I ZR 54/17, I ZR 55/17, I ZR 56/17, I ZR 57/17, and I ZR 135/18 (*Uploaded and YouTube*); The Czech Supreme Court, Case No 23 Cdo 1840/2021 [2022].

²³ This also includes state authorities.

²⁴ Arguably, mere conduits subject to net neutrality regulation might be subject to oversight by authorities as well; although this was never explicitly mentioned, the court may interpret relevant legislation in a way that leads to derogation.

Table 8.1 EU law limits on orders issued by authorities

Horizontal limits	Sectorial limits (examples only)
Injunction clauses (Articles 4(3), 5(2), and 6(4) DSA): <i>eg a decision of authorities is required; the only acceptable goals are to end or prevent an infringement</i>	Removing terrorist content on hosting services (Articles 3–6 TCR): <i>eg specificity, deadlines, forms, and procedures</i>
General monitoring prohibition (Articles 8 DSA): <i>eg only specific monitoring is permitted</i>	Reactive and preventive orders imposed on providers in intellectual property cases (Article 3 IP Enforcement Directive): <i>eg proportionality, equity, effectiveness, barriers to trade, dissuasiveness, etc</i>
EU Charter of Fundamental Rights: <i>eg procedural safeguards and the outcome cannot violate fundamental rights</i>	Orders imposed on some mere conduits (Article 3 Open Internet Regulation): <i>eg existence of a legal basis for blocking, etc</i>

act in accordance with Member States' legal systems, as the EU rules are part of that system. Even the newly inserted Recital 25 speaks only of authorities.²⁵

The injunction clauses are limited by the applicability of the liability exemptions.²⁶ Any injunctions against providers that do not benefit from the liability exemptions are not limited by the DSA.²⁷ However, even these services can be brought into the scope of the EU law by other sectorial EU instruments, such as rules about IP enforcement,²⁸ sanctions, or child abuse material.²⁹ The applicability of EU rules is important for the applicability of the EU Charter,³⁰ which in turn is essential for the prohibition of general monitoring obligations (Chapter 5).³¹ Even where the Union law does not apply, similar prohibitions of general monitoring can be based on national constitutions. Table 8.1 provides a basic overview of the various limits that the DSA and related instruments place on the orders issued by authorities, whether judicial or administrative. The majority of the above limits apply to orders directed *only* to providers subject to some liability exemptions. This is the case for all the DSA and TCR limits.³² I discuss the prohibition of general monitoring in Chapter 5 and fundamental rights in Chapter 3.

²⁵ The trickier situation concerns arts 9–10 whose language and a long list of recitals (eg Rec 31) are explicitly limited to 'national' authorities. The analogous application should nevertheless be possible.

²⁶ For instance, payment providers are outside the scope of the DSA.

²⁷ Art 8 of the DSA does not apply either, thus allowing the possibility of the imposition of general monitoring obligations. The providers of such services could be subject to requests without independent oversight by the authorities, to require general monitoring, or to avoid formalities and procedures of the DSA.

²⁸ See Case C-580/13 *Coty Germany GmbH v Stadtsparkasse Magdeburg* ECLI:EU:C:2015:485.

²⁹ European Parliament and Council Directive 2004/48/EC on the enforcement of intellectual property rights [2004] OJ L157/45 (IP Enforcement Directive), art 11; InfoSoc Directive, art 8(3); Council Regulation (EU) 2022/350 of 1 March 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine [2022] OJ L65/1; Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse' COM(2022) 209 final (Child Abuse Material Proposal).

³⁰ EU Charter, art 52.

³¹ See the German Supreme Court, BGH v 21 September 2017—I ZR 11/16, para 70ff.

³² Open Internet Regulation applies to services that qualify as mere conduits anyway.

8.3 DSA Rules on Orders Issued by Authorities

The original Commission's DSA proposal avoided reforming the injunction clauses and further developing the concept of injunctions against non-liable intermediaries. In Chapter 5, I explain the last-minute failed attempts by co-legislatures to codify the case law.

The only novelty in the DSA is the insertion of content and information orders in Articles 9–10. Like Article 18 ECD, they complement and build upon injunction clauses in Articles 4(3), 5(2), and 6(4), but their effects are limited. The provisions neither harmonise minimum or maximum conditions for injunctions nor provide a legal basis to issue them. They are not 'empowering provisions'. The main purpose of Articles 9–10 is to facilitate cross-border enforcement of the most common orders by clarifying their status in the internal market and imposing an obligation to respond. They envisage an opening mechanism that probably is not compulsory and whose keys must be given to authorities by the national parliaments.

During the negotiations, the Council requested several discussion rounds on the legal nature of these two provisions.³³ It was not clear to the Council whether the intention was to harmonise injunctions, to provide a legal basis for injunctions directed to intermediaries, or to limit the current legal framework as regards injunctions. The result of these discussions is that the provisions do neither of these things now clarified in the recitals.

One of the main drivers for the two provisions is explained in Recital 38:

Orders to act against illegal content and to provide information are subject to the rules safeguarding the competence of the Member State in which the service provider addressed is established and the rules laying down possible derogations from that competence in certain cases, set out in Article 3 of Directive 2000/31/EC, only if the conditions of that Article are met. *Given that the orders in question relate to specific items of illegal content and information, respectively, where they are addressed to providers of intermediary services established in another Member State they do not in principle restrict those providers' freedom to provide their services across borders.* Therefore, the rules set out in Article 3 of Directive 2000/31/EC, including those regarding the need to justify measures derogating from the competence of the Member State in which the service provider is established on certain specified grounds and regarding the notification of such measures, do not apply in respect of those orders.

Even post-DSA, the ECD's country of origin principle redistributes the competencies of the states to regulate providers. Because the ECD seemed to imply that national civil

³³ Interview with Irene Roche Laguna, Deputy Head of Unit for Coordination and Regulatory Compliance, European Commission (2021–23).

court decisions needed to be notified under Article 3 ECD,³⁴ unlike orders related to criminal matters (Recital 26 ECD),³⁵ the Commission wanted to clarify their status quo to avoid overwhelming the notification system (Chapter 17.4). Articles 9–10 are meant to provide a ‘safe harbour’ against potential competence objections level against the issuing authorities. The provisions are not exactly amendments of Article 3 ECD, but they are in line with the position that was already signalled by the CJEU in *Glawischnig* or *Airbnb* as regards well-known cross-border injunctions.³⁶

Thus, the DSA’s starting point is that an order to remove a specific piece of content or produce a specific piece of information does not amount to a relevant restriction to providing services. Recital 38 requires a case-by-case basis to avoid the misuse of the provision for competence grabs by the other Member States. For instance, an order imposing a burdensome continuous obligation to collect information, to actively seek new material, or request a service shutdown would likely still ‘restrict the freedom to provide’ that service in the territory of a different Member State and have to follow the relevant procedure according to Article 3 ECD.

Articles 9–10 DSA foresee uniform requirements for removal orders and orders for information, a clear obligation for feedback on the action taken, as well as a uniform language regime. This is all meant to ensure that providers across Europe can comply with the orders issued under national laws in a swift manner. While the Commission’s Impact Assessment claims that the intention was to ‘harmonise certain conditions for court and administrative orders to impose measures for the removal and detection of illegal content, goods or services by intermediaries’,³⁷ the resulting language is less clear. According to Recital 31 DSA:

[T]his Regulation *should harmonise only certain specific minimum conditions that such orders should fulfil in order to give rise to the obligation of providers of intermediary services to inform the relevant authorities about the effect given to those orders.* Therefore, this Regulation does not provide the legal basis for the issuing of such orders, nor does it regulate their territorial scope or cross-border enforcement.

Thus, the harmonising effect is probably explicitly limited to situations when the authorities decide to rely on the mechanisms in Articles 9–10 DSA because of the clarity and expected feedback. An alternative and less likely reading, probably relying on the

³⁴ ECD, Rec 25: ‘National courts, including civil courts, dealing with private law disputes can take measures to derogate from the freedom to provide information society services *in conformity with conditions established in this Directive*.’

³⁵ ECD, Rec 26: ‘Member States, in conformity with conditions established in this Directive, may apply their national rules on criminal law and criminal proceedings to take all investigative and other measures necessary for the detection and prosecution of criminal offences, without there being a need to notify such measures to the Commission.’

³⁶ *Glawischnig* (n 3); Case C-390/18 *Airbnb Ireland* ECLI:EU:C:2019:1112.

³⁷ Commission, “Impact Assessment” (Commission Staff Working Document) Accompanying the Document “Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (DSA) and Amending Directive 2000/31/EC” SWD(2020) 348 final, annex 9, 213.

second sentence of Recital 31 DSA, would be that these provisions provide minimum conditions for such orders.

To summarise, Articles 9–10 DSA likely do not harmonise the only conditions under which an injunction ‘fits’ under Articles 4(3), 5(2), and 6(4) DSA. There is no link between these two sets of provisions because their focus is very different. National authorities can issue injunctions against intermediaries that do not comply with the conditions stipulated in Article 9 or 10 DSA *if* they comply with Articles 4(3), 5(2), and 6(4) and other provisions of the DSA. Thus, apart from the clarity regarding competence in cross-border affairs, the only added value of Articles 9–10 DSA is that they trigger an obligation to provide feedback to the received orders.

That said, it is undeniable that these provisions intend to interpret how a ‘good injunction’ should look. The conditions envisaged in the provisions are codifying existing case law, international law comity principles, and fundamental rights. The articulation of the minimum conditions suggests what injunctions should be smoothly enforced in the cross-border setting. In the next two sections, I closely examine the conditions spelt out for content and information orders.

8.4 Content Orders (Article 9)

If a provider receives an order from an authority asking it to ‘act against’ specific content, it must notify it ‘without undue delay, specifying if and when effect was given to the order’ (Article 9(1) DSA). Recital 33 DSA clarifies that specific time limits can be created under specific national or Union laws. While the underlying content of these orders must be enforced through national law, non-compliance with the obligation to notify constitutes the only DSA violation (see Recital 32 DSA). Thus, the DSA’s enforcement mechanism can be used.

What exactly qualifies as an order is not specified in the DSA. It constitutes an autonomous concept of the EU law that the CJEU has the power to interpret. The goal of Article 9 DSA is clearly to cover all possible criminal, administrative, or civil orders that one might find in national law. This is evident from Recital 34 DSA, which tries to mitigate the broad scope of the notion by allowing some adjustment of specific obligations for criminal and other procedures. It is unclear when a demand of authorities to act concerning individual pieces of content would not constitute an order. Would a formal letter sent by a parliamentary committee or the head of an authority institute such an order? Implicitly, an order must have a legal basis and thus be subject to some coercive powers of the state. If the demands in the letter from authorities are not of such quality, then they probably do not qualify as orders. To understand what an order is, therefore, it is impossible to avoid looking at the legal basis.

Article 9 DSA only creates baseline rules. Recital 31 DSA, therefore, reminds us that the national law can go beyond these conditions when giving rise to the obligation to inform the authorities about the effective given to orders. Recital 31 DSA also emphasises that no guarantee of territorial scope or cross-border enforcement is

implied in Article 9 DSA. In fact, Recital 34 DSA explains at length that general provisions concerning cooperation in civil and criminal matters, including rules of international private law, continue to apply. It even formulates an unusual priority of such rules as follows:

Therefore, where those laws in the context of criminal or civil proceedings provide for conditions that are additional to or incompatible with the conditions provided for in this Regulation in relation to orders to act against illegal content or to provide information, the conditions provided for in this Regulation might not apply or might be adapted.

The example mentioned as a possible deviation is a circulation obligation for Digital Services Coordinators (DSCs) (Article 9(3)) in criminal cases. Article 9(2) prescribes the following minimum conditions for each content order:

- (i) reference to the legal basis;
- (ii) a statement of reasons explaining why the information is illegal content by reference to a specific legal basis;
- (iii) information identifying the issuing authority;
- (iv) clear information enabling the provider of intermediary services to identify and locate the illegal content concerned, such as one or more exact URL and, where necessary, additional information;
- (v) information about redress mechanisms available to the provider of the service and to the recipient of the service who provided the content;
- (vi) where applicable, information about which authority is to receive the information about the effect given to the orders;
- (vii) the territorial scope of that order.

The order containing the above information must be sent to the electronic point of contact designed by the provider in one of the languages declared by the provider of intermediary services pursuant to Article 11(3) unless otherwise agreed. The authorities who function in other languages are thus required to translate their orders, at least as far as they are concerned with the above elements. For any other elements that might be required under the national law but are not required by Article 9(2), a translation is not necessary. While the DSA does not allude to that, practically, it is expected that the authorities will be heavily using machine translation.

National DSCs of the issuing state are obliged to share such orders with the other DSCs (Article 9(4)) through the information-sharing system created by the DSA. Unless the authority prescribes a specific legal requirement, when the order is effective at the latest, providers of intermediary services shall equally inform the recipient of the service about the effects given to the content order. Such notification must ‘include a statement of reasons, the possibilities for redress that exist, and a description of the territorial scope of the order’ (Article 9(5)).

However, Article 9(6) includes a broad set of obligations: notification to authorities, recipients of the service, and a circulation obligation. It provides that '[t]he conditions and requirements laid down in this Article shall be without prejudice to national civil and criminal procedural law'. Recitals 34–35 provide several references to national, in particular criminal law, where some of these obligations might need to be adjusted to protect other interests, such as effective prosecution of crimes. The obvious candidates for such adjustment of content orders are cases in which the issuing authority might want to conceal that it is conducting investigations into the person for a limited period.

While the DSA does not regulate the territoriality or proportionality of orders, it provides a framework for balancing interests for both questions. Because all orders, according to Article 9, implement the EU law, their underlying legal basis and material scope will not escape the EU Charter. Similarly, while the territorial scope is up to national law to determine, Recital 36 states that:

The order should balance the objective that the order seeks to achieve, in accordance with the legal basis enabling its issuance, with the rights and legitimate interests of all third parties that may be affected by the order, in particular their fundamental rights under the Charter. In particular in a cross-border context, the effect of the order should in principle be limited to the territory of the issuing Member State, unless the illegality of the content derives directly from Union law or the issuing authority considers that the rights at stake require a wider territorial scope, in accordance with Union and international law, while taking into account the interests of international comity.

This language is a stronger version of the CJEU's call in *Glawischnig* that national courts when granting orders with worldwide effects which the ECD does not preclude, should consider the 'global dimension of electronic commerce' and consistency 'with the rules applicable at international level' by taking 'due account of those rules'.³⁸ What follows from Article 9(2) together with Recital 36 is that the minimum that recipients of the order, and ultimately its users, deserve is an explanation on why a given territorial scope has been chosen. To limit undue removal of lawful content, the general principle of enforcement should be territorial enforcement unless the subject matter justifies the broader scope. If the target of the content orders is clearly illegal in the other Member States or even globally, the scope might be appropriately extended. However, it should not be possible for authorities to try to enforce their own version of right and wrong at the expense of freedoms enjoyed by individuals in other states. The issue of global removals will clearly resonate in the coming years. Some courts, such as the Italian Supreme Court, recently signalled that they consider global orders to be acceptable for some types of claims.³⁹

³⁸ *Glawischnig* (n 3) paras 50–52.

³⁹ The Italian Supreme Court, Cass, 24 November 2022, n 34658 (regarding the right to be delisted); The Austrian Supreme Court, OGH 30 March 2020, 4 Ob 36/20b (*ORF/Facebook Ireland Limited*) (assumed that the CJEU's start point are removal orders to have a worldwide effect—see paras 5.2 and 5.5).

8.5 Information Orders (Article 10)

If a provider receives an order from an authority asking it to ‘provide specific information about one or more specific individual recipients of the service’, it must ‘without undue delay’ confirm the receipt and explain ‘the effect given to the order, specifying if and when effect was given to the order’ (Article 10(1) DSA). The copy of the order is equally subject to the circulation requirement to other DSCs (Article 10(4) DSA). Moreover, the information obtained through the order must be shared with the DSC (Article 10(3) DSA). However, with content orders, these obligations are without prejudice to national civil and criminal procedural law (Article 10(6) DSA).

Article 10(2) DSA spells out the following minimum requirements for such orders:

- (i) a reference to the legal basis;
- (ii) information identifying the issuing authority;
- (iii) clear information enabling the provider of intermediary services to identify the specific recipient or recipients on whom information is sought, such as one or more account names or unique identifiers;
- (iv) a statement of reasons explaining the objective for which the information is required and why the requirement to provide the information is necessary and proportionate to determine compliance by the recipients unless such a statement cannot be provided for reasons related to the prevention, investigation, detection, and prosecution of criminal offences;
- (v) information about redress mechanisms available to the provider and to the recipients of the service concerned;
- (vi) where applicable, information about which authority is to receive the information about the effect given to the orders;
- (vii) the statement that the order only requires the provider to provide information already collected to provide the service, which lies within its control.

To give a practical example: if a local authority has regulated short-term rentals in its territory, and it needs to identify a host offering an apartment in its municipality illegally, it could send an order to the short-term rental platform to request the identification of that user.⁴⁰ For that purpose, it will need to refer to its powers under local or national laws to request such information, identify itself, share the account name or identifier of the user whose identity is seeking to obtain, explain why such identity is necessary to enforce the local rules on short-term rentals, and inform about the administrative channels to challenge that order.

⁴⁰ See Commission, ‘Proposal for a Regulation of the European Parliament and of the Council on data collection and sharing relating to short-term accommodation rental services and amending Regulation (EU) 2018/1724’ COM (2022) 571.

The information order must be sent to the electronic point of contact designated by that provider in one of the languages declared by the provider (Article 11(3)) or other agreed language. The authorities who function in other languages are thus required to translate their orders, at least as far as they are concerned with the above elements. For any other elements that might be required under the national law but are not required by Article 10(2), a translation is not necessary.

Like content orders, Article 10(5) requires that unless the order specifies the period, the provider must inform the affected recipient of the service about what it has done at the latest when it discloses the information. The notification must include ‘a statement of reasons and the possibilities for redress that exist’. The extent of information and reasons should be sufficient for the individual to use the redress possibilities. This suggests that in principle, the order itself shall be disclosed as well.

8.6 Conclusion

The DSA offers very few tangible changes to the issuance of injunctions. The newly inserted articles do not preclude the alternative fashioning of such orders. At best, they incentivise and nudge the use of some minimum safeguards across the Member States.

The key limit on injunctions and the source of future harmonisation continues to be found in the injunction clauses in the liability exemptions, the prohibition of general monitoring obligations, and the EU Charter. The legislative process surrounding the DSA has shown that the interface between national orders and these limitations is very controversial. This explains the lack of political will to codify the existing case law or improve it by introducing various safeguards that are becoming settled case law in the Strasbourg jurisprudence (Chapter 3). At the moment, it is clear that various stakeholders are simply hoping that by not engaging with the issue through legislation, they can, in the long run, convince the Court of a more favourable reading for their own agenda.

The political agreement behind the DSA should, however, at the very least lead to more frequent scrutiny of the injunctions and orders from the EU perspective. Too often, national courts pay lip service to EU law considerations. While some issues simply are left unharmonised, such as global injunctions, others have clear legal footing and are neglected. For instance, the injunction clauses—established to assure that the state supervises any reactive and preventive obligations on the national level for potential hindrances to the internal market and fundamental rights—are continuously ignored by some national systems.⁴¹

Finally, considering the developing case law in Strasbourg, the EU Charter can become a very potent force to further align some of the basic safeguards that the national law must introduce before the orders are allowed in the system by the injunction clauses.

⁴¹ See for instance, the German system, explained further in Martin Husovec, ‘Asking Innocent Third Parties for a Remedy: Origins and Trends’ in Franz Hofmann and Franziska Kurz (eds), *Law of Remedies: A European Perspective* (Intersentia 2019).

The attempts to introduce such safeguards in the case law, such as *UPC Telekabel*'s requirement to allow a fair trial of affected internet users,⁴² mostly failed to achieve their results. The national courts did not take them too seriously (Chapter 5.6). It is preferable that the legislatures at the national and European levels soon create a DSA-like due process framework for injunctions, too.

⁴² *UPC Telekabel* (n 5) para 57 ('the national procedural rules must provide a possibility for internet users to assert their rights before the court once the implementing measures taken by the internet service provider are known').

PART III

ACCOUNTABILITY

Introduction to Accountability Framework

9.1 The EU Landscape of Digital Services	161	9.2.1 Determining ‘Big Tech’ by counting users	168
9.1.1 VLOSEs, VLOPs and other platforms	161	9.2.2 Digital services vs relevant technical activity	171
9.1.2 Runners-up and other platforms	163	9.2.3 A notion of the service	174
9.1.3 Online platforms vs mere hosting services	164	9.2.4 On mini platforms	177
9.1.4 Infrastructure services	166	9.3 Judicial Review of VLOP/VLOSE Designation Decisions	178
9.1.5 Non-regulated services	167	9.4 Separation of Liability and Accountability	181
9.2 Determining Regulatory Layers	167		

9.1 The EU Landscape of Digital Services

It is hard to think about digital services in the abstract. This chapter, therefore, outlines the European Union’s (EU) Digital Services Act (DSA) regime and how it will likely apply to specific services in the coming years. The goal is not to be exhaustive, and it is possible that the services mentioned might have changed by the time you read this book. My hope is that having some specific names behind abstract concepts will give you a more concrete view of the ecosystem.

9.1.1 VLOSEs, VLOPs, and other platforms

On 25 April 2023, the European Commission published the first list of designated very large online platforms (VLOPs) and very large online search engines (VLOSEs).¹ The designations are based on the first round of disclosures from 17 February 2023. The first designation round covered 19 separate services, comprising two search engines, two app stores, four marketplaces, eight social media, one encyclopaedia, one price comparison site, and one online map service. Many of the providers will have their European base in Ireland. This matters particularly in the event of violations of the DSA’s standard due diligence obligations, where the European Commission shares competence with the national Digital Services Coordinators (DSCs). In December 2023, the Commission designated three further VLOPs. All three are content-sharing services

¹ European Commission, ‘DSA: Very Large Online Platforms and Search Engines’ (*Shaping Europe’s Digital Future*, 25 April 2023) <<https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops>> accessed 10 August 2023.

hosting pornography. Finally, in April and May 2024, the European Commission designated another two marketplaces as a VLOP. Table 9.1 provides an overview of existing 22 VLOPs and 2 VLOSEs at the time of writing.

Table 9.1 Designations as VLOPs and VLOSEs.

	Company	Digital Service	Type	DSC-COO	Users (mil): 1st disclosure (Feb 2023) ^a	Users (mil): 2nd disclosure (Aug 2023) ^b
Search	Alphabet	Google Search	VLOSE	Ireland	332+	364
	Microsoft	Bing	VLOSE	Ireland	107	119
Social media	Alphabet	YouTube	VLOP	Ireland	401+	416+
	Meta	Facebook	VLOP	Ireland	255	258
	Meta	Instagram	VLOP	Ireland	250	257
	Bytedance	TikTok	VLOP	Ireland	125	134
	Microsoft	LinkedIn	VLOP	Ireland	122+	132+
	Snap	Snapchat	VLOP	Netherlands	96+	102
	Pinterest	Pinterest	VLOP	Ireland	n/a	124
	X (formerly Twitter)	X	VLOP	Ireland	100+	112+
App stores	Alphabet	Google App Store	VLOP	Ireland	274+	284+
	Apple	Apple App Store	VLOP	Ireland	n/a	123
Online Marketplaces	Amazon	Amazon Marketplace	VLOP	Luxembourg	n/a	181+
	Alibaba	AliExpress	VLOP	Netherlands	n/a	135+
	Booking.com	Booking.com	VLOP	Netherlands	n/a	n/a
	Infinite Styles Services	Shein	VLOP	Ireland	n/a	108
	Whaleco Technology	Temu	VLOP	Ireland	n/a	75
	Zalando ^c	Zalando	VLOP	Germany	30+	27+
Wiki	Wikimedia	Wikipedia	VLOP	none	151+	151+
Price comparison	Alphabet	Google Shopping	VLOP	Ireland	74+	70+
Maps	Alphabet	Google Maps	VLOP	Ireland	278+	275
Porn sites	Aylo Freesites	PornHub	VLOP	Cyprus	n/a	n/a
	Technius	Stripchat	VLOP	Cyprus	n/a	n/a
	Webgroup	Xvideos	VLOP	Czechia	n/a	160

^a For an archive of the first wave of disclosures made in February 2023, see <<https://husovec.eu/wp-content/uploads/2023/09/DSA-MAU-First-Disclosure-Feb2023.pdf>>.

^b For an archive of the second wave of disclosures made in August 2023, see <<https://husovec.eu/wp-content/uploads/2023/09/DSA-MAU-Second-Disclosure-Aug2023.pdf>>. For the December 2023 round of designations, see <<https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses>>.

^c Zalando has sought to invalidate its VLOP status; section 9.2.1.

Table 9.2 Runners-up online platform services.

Online platforms	Digital Service	Users (mil): 1st disclosure (Feb 2023)	Users (mil): 2nd disclosure (Aug 2023)
Social media	BeReal	18	18
	Reddit	10+	11+
Messaging services	Telegram	38+	n/a
	Viber	30+	n/a
	Discord	n/a	n/a
Marketplace	Airbnb	30+	38+
	Apple Books	n/a	< 1
	Vinted	n/a	27+
	Allegro	23+	23+
	Cdiscount	19+	17
	Leboncoin	26+	27+
	Roblox	25+	27+
	eBay	n/a	n/a
Comparison & review sites	Tripadvisor	n/a	n/a
	Trustpilot	23+	n/a
	Gutefrage	30+	28+
	Heureka	23	23
	Skyscanner	34+	41+
Content-sharing services	OnlyFans	n/a	n/a
	Spotify Podcasts	n/a	n/a
	DailyMotion	n/a	n/a
	GitHub	10+	11+
Maps	Waze	40+	40+

9.1.2 Runners-up and other platforms

In addition to the above companies, the major services listed in Table 9.2 likely constitute mid-size or bigger online platforms, and thus, some of them are likely runners-up to become VLOPs in the coming years.

Among these services, the European Commission is rumoured to explore whether Spotify and eBay truly do not meet the threshold as declared.² It is not entirely unlikely that some of them end up designated as new VLOPs in late 2023. On the whole, the exact number of online platforms that are active in the EU for the purposes of the DSA is currently not known and may be difficult to determine, especially since they

² Clothilde Goujard, 'European Retailer Protests against Big Tech Platform Label' *POLITICO* (13 June 2023) <<https://www.politico.eu/article/zalando-big-tech-label-protest-european-retailer/>> accessed 1 September 2023.

need to meet the company size threshold to be relevant. Some DSCs, such as Germany, have recently carried out empirical mapping to determine the number of European and non-EU-based providers that might fall under the regime.³ The study found a total of 4,501 potential regulated providers relevant for Germany alone, of which almost a third are online platforms. Existing registers for video-sharing platforms, one of the most common types of platforms, list less than 100 such services for the entire EU.⁴

9.1.3 Online platforms vs mere hosting services

Not all services that store other people's information are online platforms. They must also publicly distribute other people's information and store it at their request. Providers that do *not* distribute information publicly remain regulated as hosting services only—something that I prefer to call 'mere hosting services'. Unlike other hosting services (Chapter 7), online platforms' main functionality is also the public distribution of stored information. If public distribution of information is 'a minor and purely ancillary feature of another service' or 'a minor functionality of the principal service' it is not the main functionality (Article 3(i)). The ancillary or minor nature arguably refers to technical *and* economic aspects of integration. Recital 13 mentions newspaper comment sections as a typical example that should be distinguished from social media platforms. However, even newspapers could become more valued for their user comment sections than editorial content. Finally, if the company providing an online platform is only small or micro, such services remain regulated as mere hosting services until they grow in the size due to the carve-out in Article 19.

Public distribution can be described as *creation of new audiences* for user-generated content. Mere hosting services, in contrast to online platforms, do not themselves 'distribute' information to the public. If the information goes out to the public, it is distributed by their users (Article 3(i) DSA), such as owners of the websites hosted on web servers. This is emphasised by Recital 13:

cloud computing services and web-hosting services, when serving as infrastructure, such as the underlying infrastructural storage and computing services of an internet-based application, website or online platform, *should not in themselves be considered as disseminating to the public information* stored or processed at the request of a recipient of the application, website or online platform which they host.⁵

The typical examples of such services are *consumer cloud solutions*, such as Dropbox, Google Drive, and Apple's iCloud, or *business cloud solutions*, such as AWS, Stripe, and

³ See Bundesnetzagentur, Umsetzung des Digital Services Act in Deutschland Bestandsaufnahme der relevanten Akteure, available at <https://www.bundesnetzagentur.de/DE/Fachthemen/Digitalisierung/DSA/studie_dsa_akteure.pdf?__blob=publicationFile&v=3>.

⁴ 'Search Results for "Video Sharing Platforms"' (European Audiovisual Observatory, 30 June 2023) <<http://mavise.obs.coe.int/f/ondemand/advanced?typeofservice=4>> accessed 1 September 2023.

⁵ Emphasis mine.

Shopify; classical *web hosting services* like GoDaddy, Ghandi, and Websupport, or even *webmail*, such as Gmail or Hotmail.⁶

Two main considerations keep such providers from tighter regulatory scrutiny. They are less public-facing, which means they create fewer direct risks. In enforcement, mere hosting services often play only a supplementary role after their clients—individual online shops or websites—fail to play their part. All ‘mere hosting’ services run by companies that employ more than 50 employees or have a turnover of more than €10 million must also issue annual reports about their content moderation practices and algorithmic moderation tools (Article 15 DSA).

The borders between ‘online platforms’ and non-platform ‘mere hosting services’ are fluid and complex. Recital 13 DSA mentions that even consumer cloud solutions could become online platforms if the distribution of information becomes more than a minor feature. An open-source content management system, such as WordPress, is arguably only a mere hosting service if the hosted content is distributed independently by websites using its technology (eg independent websites using WordPress’s system, including its hosting). However, if a WordPress-like system also starts *creating an audience* for the websites it helps to host, such as by offering aggregating features, it can easily become an online platform. Moreover, a news website hosting and distributing blogs of other bloggers can be an online platform for blogs, and its bloggers hosting providers (possibly even platforms) vis-à-vis user comments. Thus, some providers can look like a matryoshka that contains other providers within.

For some commerce, advertising, and content management systems, a further problem arises from their relative proximity to the public, particularly where one must register to use a service. For instance, on a content management system, all kinds of plug-ins are offered to registered users via a marketplace. Recital 14 DSA explains its notion of public as follows:

the making available of information to a *potentially unlimited number of persons*, meaning making the information easily accessible to recipients of the service in general without further action by the recipient of the service providing the information being required, irrespective of whether those persons actually access the information in question. Accordingly, *where access to information requires registration or admittance to a group of recipients of the service, that information should be considered to be disseminated to the public only where recipients of the service seeking to access the information are automatically registered or admitted without a human decision or selection of whom to grant access.*⁷

Thus, the mere existence of a registration process does not make such services *private*. Only a manual registration process overseen on an ad hoc basis by humans who select whom to admit can turn the service, or its parts, private. This is key for messaging

⁶ Rec 14 of the DSA says that email falls outside the scope of the definition of an online platform because the criterion of the public is not met, as ‘they are used for interpersonal communication between a finite number of persons determined by the sender of the communication’.

⁷ Emphasis mine.

services hosting various groups and channels that either require the permission of administrators to enter or can be joined by anyone automatically, depending on the settings. It is also why the distribution of plug-ins to registered users by content management systems or marketplaces organised by advertisers can constitute online platforms.

9.1.4 Infrastructure services

Infrastructure services provide the hidden services that allow the internet to function. The mere conduit provisions, after clarification in the DSA’s language, arguably cover most of them. The caching provision covers content delivery networks whose importance for the security of the internet is increasing. All these services are subject to only light touch *universal* due diligence obligations, such as points of contact and terms and conditions. The biggest impact is on the non-EU-based services, which will have to appoint a legal representative (Article 13 DSA) if they offer their services in the EU in exchange for becoming regulated in only one of the Member States.

Only when providers employ more than 50 people or have over €10 million turnover do they publish annual transparency reports about how they conduct content moderation (Article 15 DSA). This means, for instance, that big emailing or storageless messaging services, content delivery networks, domain name services, VPN services, and internet access providers should have started issuing reports about their practices as of February 2024. This also includes transparency about tools used for such content moderation, such as how they operate website blocking measures, deregister domain names, block customers, or filter spam and malicious messages.

Table 9.3 provides examples of infrastructure services under the DSA.

Table 9.3 Infrastructure services.

Internet ‘access’ providers	Domain name services	Storageless messaging	Other potential services	CDNs ^a
Telecommunication companies (O2, Vodafone, Orange)	Domain registries (.de by DENIC, .nl by SIDN, .sk by SK-NIC, etc)	Signal	Certification authorities	CloudFlare
Providers of open WiFi (cafes, hotels)	Domain name registrars (GoDaddy, Gandi)	WhatsApp	Transit services (Level(3), NTT)	Akamai
VPN providers	Recursive DNS (Google, Open DNS)	Email services (as regards emailing, not storage)	Browsers (Mozilla, Chrome)	CacheFly
Tor node operators	Authoritative DNS (Dyn, CloudFlare)		Voice over IP services	Azure Front Door

^a See ‘Global Map of CDNs and Cloud Services’ (26 July 2023) <https://opentelecomdata.org/cdns/?trk=feed_main-feed-card_feed-article-content> accessed 28 August 2023.

9.1.5 Non-regulated services

The DSA only applies if a digital service incorporates a user-generated content (UGC) component into the service, and extends to its other parts that are inseparable from the perspective of the user experience. This might be missing from purely editorial services, like Netflix, Disney +, and Amazon Prime. However, when these services introduce user reviews viewed by others, they might start falling into the DSA's scope. For instance, Google Maps is an online platform despite the fact that mapping service is largely editorial. In the user experience, user-generated parts (eg shop reviews, profiles of shops, etc.) are defining for navigation as much as the editorial maps. Another example is Spotify whose playlists or podcasts could pull also more editorial parts of the service, such as curated music libraries, into the category of online platforms. At the same time, the DSA does not apply to some important services, such as some ride-hailing apps, due to their EU classification as transport services.⁸ Some uncertainty remains about digital services, which have purely non-profit character due to the criterion of the economic activity (Chapter 6.2.6). However, in most cases, such services should arguably remain regulated if their assets can be commercialised due to their potential economic value.

9.2 Determining Regulatory Layers

The DSA has several tiers of obligations. Midsized companies that operate online platforms have more obligations in content moderation than small and micro companies. Digital services with the biggest foothold in Europe—45 million monthly active users—are subject to the most extensive risk management regime. The DSA's design takes into account three important criteria:

- a) technical functionality embedded in a digital service;
- b) size of a company offering a digital service; and
- c) average monthly users of a digital service in the EU.

Very few due diligence obligations apply to *infrastructure services* (mere conduit and caching), such as internet access providers. Some of the DSA's content moderation obligations apply to all digital services that simply store other people's information as an economic activity (*mere hosting*). However, transparency and other more resource-intensive content moderation provisions (eg dispute resolution) apply only to those mid-sized companies that store and distribute it to the public as a main functionality (*online platforms*). These same companies are also subject to specific obligations concerning their recommender systems, advertising, and user interfaces. If they serve

⁸ Case C-320/16 *Uber France* ECLI:EU:C:2018:221.

users who are children, they owe a specific due diligence obligation to children. Finally, online platforms with 45 million average monthly users in the EU must comply with all the previous rules and their special obligations as *very large online platforms*. The most far-reaching among them is a general risk management obligation.

9.2.1 Determining ‘Big Tech’ by counting users

According to Article 24(2) DSA, all online platforms and search engines must publish their numbers concerning average monthly active users at least in two annual windows. The goal is to keep who is or might soon become ‘Big Tech’ visible (ie VLOPs/VLOSEs). Providers can publish their numbers on their websites, but their competent DSC and the European Commission can also approach them at any time to request specific information about user numbers (Article 24(3)). The Commission may issue a delegated act concerning methodology for counting *active monthly recipients of services* (Article 33(3)). At the time of writing, this has not yet happened. The Commission has only published an FAQ, which does not address the methodology.⁹

Article 3 DSA defines the concept of active recipient as follows (emphasis mine):

(p) ‘active recipient of an online platform’ means a recipient of the service that *has engaged* with an online platform by either requesting the online platform to host information or being *exposed to* information hosted by the online platform and disseminated through its online interface;

Thus, the crucial term is ‘engagement’, which can be a ‘request to host information’, such as by sellers or content creators, or an ‘expos[ure]’ to such information. An active user is either a content creator or a consumer of content. As noted by Recital 77, ‘engagement is not limited to interacting with information by clicking on, commenting, linking, sharing, purchasing or carrying out transactions on an online platform’ and is most certainly not limited to registered users. For public social media, active recipients include both content creators who actively post or share content and those who only read it, even though they do not have a registered account. That said, for social media services that allow only registered users to share and see the content, this suggests only registered users count.

A specific complication is whether the readership of content from the service embedded in other services, such as online news articles, also increases the user count. Article 3(p) speaks of ‘being exposed to information ... disseminated through its online interface’. Arguably, embedded content that relies on its own interface created for this purpose by the provider should also count these additional readers. However, if the

⁹ EU Commission, ‘DSA: Guidance on the Requirement to Publish User Numbers’ (*Shaping Europe’s digital future*, 1 February 2023) <<https://digital-strategy.ec.europa.eu/en/library/dsa-guidance-requirement-publish-user-numbers>> accessed 28 August 2023.

embedding technique does not use the providers' own interface, such users arguably do not need to be counted.

Recital 77 states that the count should 'reflect all the recipients *actually engaging* with the service at least once in a given period, by being exposed to information disseminated on the online interface of the online platform, such as viewing it or listening to it, or by providing information, such as traders on an online platform allowing consumers to conclude distance contracts with traders'.¹⁰ The concept depends on 'market and technical developments' (Recital 77). Providers are, however, allowed to deduce 'incidental users' who visit the websites.

All five pending designation cases, concern methodology. For instance, Zalando is contesting its designation, arguing that its hybrid marketplace does not reach the threshold because the traffic for goods sold by Zalando and third-party goods can be separated.¹¹ Given what I said above, this is unlikely to succeed. The buyers of both products are exposed to them on the same interface; thus, there is no clear separation. A consumer who buys goods sold by Zalando is likely exposed to goods from third-party sellers during the search stage, even though she did not buy them. Zalando thus seems to be an easier case.¹² If a provider is separating its online retail business from its marketplace platform by actually using different interfaces (eg separate apps), it can be argued that the numbers concerning online retail should not be counted.

Article 3 DSA defines the concept differently for search engines:

(q) 'active recipient of an online search engine' means a recipient of the service that has submitted a query to an online search engine and been exposed to information indexed and presented on its online interface;

For search engines, only the searching side is crucial. Thus, website owners, who benefit from the search results and can be considered recipients of the service in that broader sense, are irrelevant for defining active recipients (Recital 77). Otherwise, any search engine aspiring to be comprehensive would be immediately classified as a VLOSE due to the large number of resources it can index. The presumption is that they do not 'actively engage' with the search engine, although this might not be true for all website owners, particularly those who use dedicated interfaces to communicate with the search engine about their websites. However, in those cases, they can become VLOPs because the content is submitted to them (eg Google Shopping). Going forward, a question might arise as to whether search engines that also fulfil the definition for online platforms should follow the counting rules established for VLOSEs or VLOPs.¹³ In

¹⁰ Emphasis mine.

¹¹ Molly Killeen, 'Zalando Files Suit against Commission over Very Large Platform Designation' (*Euractiv*, 27 June 2023) <<https://www.euractiv.com/section/platforms/news/zalando-files-suit-against-commission-over-very-large-platform-designation/>> accessed 4 September 2023.

¹² Disclosure: The author is representing a consumer organisation, EISI, intervening on the side of the Commission in this case.

¹³ See the discussion in ch 7.

my view, in such a case, VLOSE counting constitutes *lex specialis* and should prevail for the reasons stated above.

When counting the users, *bots and scrapers* can be excluded in the first step.¹⁴ Nothing prohibits companies from overclaiming and thus from counting even users they do not have to. Recital 77 clarifies that multi-device use by the same person should not count as multiple users. The companies can further exclude ‘incidental’ users (Recital 77) who land on services through linking or search tools. Such users do not ‘actually engage’ with the services. Thus, the concept tries to approximate the real number of unique human beings using the service. This can be tricky to calculate. Using proxies (eg the average number of devices per person) to calculate the final number of unique users is unavoidable. Whatever the final number, it is inevitably only a better or worse approximation of the real user base. That being said, Article 24(2) demands a number. The provision affords discretion to companies to establish their estimates of the user base relying on the methods that are compatible with the goals of the DSA. Thus, while adopting different thresholds for incidental use might be acceptable, relying on irrelevant criteria, such as attributable revenue, should not.

Furthermore, the counting must be on a per-service level (Recital 77). This can be difficult for hybrid services that incorporate several aspects, of which only some constitute platforms, such as marketplaces that sell their own goods, video-sharing services that promote their own content, or messaging services whose chats are not always public. The features that drive user engagement also do not necessarily have to be user-generated. For instance, online maps with user-generated content, such as Google Maps, expose to usually inextricably to both editorial and user-generated content when offering its navigation services. In these cases, the question is when can we separate *non-platform activities* for the purposes of counting of users.

To some extent, an imprecise but justifiable methodology should be an acceptable methodology. Privacy considerations demand that companies not engage in additional tracking just to calculate a number for the DSA. Therefore, it should be possible to use proxies when calculating the average monthly users. For instance, DuckDuckGo used survey data to estimate a device-per-person estimate,¹⁵ and Wikipedia used some of the existing device-per-person estimates to approximate the number of unique users.¹⁶ Google, on the other hand, published its data separately for signed in and non-signed in users.¹⁷

Judging by the first disclosures, some companies have apparently inferred that because Article 24(2) requires the publication of ‘information on the average monthly

¹⁴ According to Rec 77, the DSA does not require providers of online platforms or online search engines to perform specific tracking of individuals online. Where such providers can discount automated users such as bots or scrapers without further processing of personal data and tracking, they may do so.

¹⁵ DuckDuckGo, ‘Regulatory Reporting’ (*DuckDuckGo Help Pages*) <<https://help.duckduckgo.com/duckduckgo-help-pages/r-legal/regulatory-reporting/>> accessed 28 August 2023.

¹⁶ Wikimedia, ‘EU DSA Userbase Statistics’ (*Wikimedia Foundation Governance Wiki*) <https://foundation.wikimedia.org/wiki/Legal:EU_DSA_Userbase_Statistics> accessed 27 August 2023.

¹⁷ Google, ‘Information about Monthly Active Recipients under the Digital Services Act (EU) (1 Jul 2022–31 Dec 2022)’ (2023) <https://storage.googleapis.com/transparencypdf/report-downloads/pdf-report-24_2022-7-1_2022-12-31_en_v1.pdf> accessed 27 August 2023.

active recipients of the service in the Union,¹⁷ companies do not need to publish any numbers or methodology. As demonstrated in the tables above, some companies did not publish their numbers, but merely a descriptive statement and most did not publish their methodologies. These companies usually argue that Article 24(2) does not use the word ‘number’, and thus a simple disclosure of whether a company is above or below the threshold will suffice. Upon a closer look, it is clear that this is not very convincing.

The DSA uses the phrase in many places to indicate simply that something must be published. For instance, Article 31(1) states that providers are obliged ‘to provide information on the name, address, telephone number and email address of the economic operator.’ The argument above conveniently gives the phrase ‘information on’ a very broad meaning to allow companies to comply in ways they find convenient, particularly to avoid potentially publishing information useful for competitors. The question is whether such discretion is really granted by Article 24(2). In my view, it undermines the effectiveness of the DSA because disclosures cannot be examined by the public on their plausibility. The DSA, by asking for public disclosures instead of in private, wanted to relieve companies of the extra work of notification but also to enable public scrutiny.

The failure to disclose a number is particularly perplexing for those providers who end up being VLOPs or VLOSEs. They have the following obligations according to Article 42(3): ‘shall include in the reports referred to in paragraph 1 of this Article the information on the average monthly recipients of the service for each Member State.’ Now, while one might argue that a precise number is not necessarily the only intended meaning of the term ‘information on’ in Article 24(2), it is fairly impossible to argue that a document that must report such ‘information on ... for each Member State’ need not contain an actual number. If the Court or the Delegated Act ever interprets the notion, ‘information on’ is likely to mean a specific number, possibly accompanied by methodology.

9.2.2 Digital services vs relevant technical activity

The DSA does not rely on the term digital service. In fact, the entire regulation is entirely agnostic to the actual service that incorporates the regulated technical activity. What triggers the DSA’s application is the integration of technical activity into a broader digital service. If the regulated technical activity—storage and public distribution of other people’s information—can be separated from their other activities, particularly the public distribution of their information, these two distinct activities do not have to be regulated together. However, if these activities are not severable, they can be regulated as non-UGC design features of the same overall service.¹⁸ Figure 9.1 illustrates this in the context of an online marketplace.

¹⁸ For similar problem, see Case C-347/14 *New Media Online GmbH v Bundeskommunikationssenat* ECLI:EU:C:2015:709 (on dissociability of principal and complementary activity for AVMS Directive).

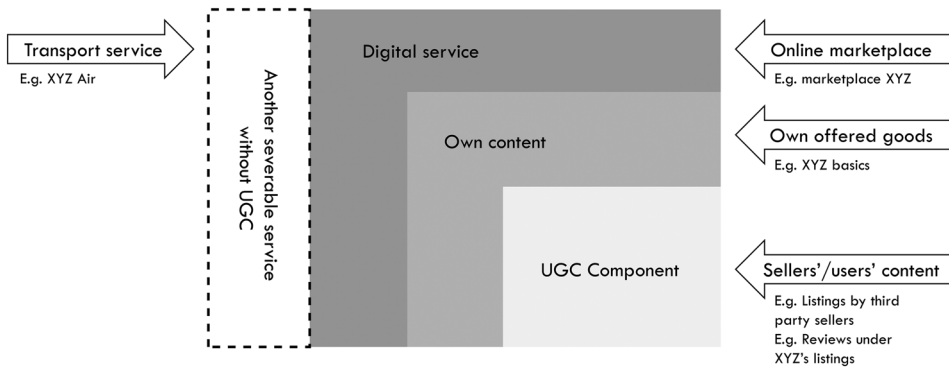


Figure 9.1 Scope of digital services: online marketplace

This is why Google Maps is regulated in its entirety, even if a lot of content on the service is not user-generated. Its UGC content that overlays editorial content can be viewed separately but is ultimately inextricably mixed in the user-experience. This logic explains why marketplaces often must report the number for the entire service because the digital service cannot be easily demarcated for its platform and non-platform side. Such hybrid platforms thus end up being more likely to be regulated, which can be justified by the fact that the user experience, and thus the impact on users, is inseparably mixed. The providers can always seek decoupling of two types of content, but often the UGC content will be ‘too useful’ for popularity of the service. Streaming services can be sometimes an example of a service whose user experience (eg podcasts as UGC component and music as editorial content) are separable. The same can be said about messaging services, such as Telegram, for their public and private communication channels. However, it ultimately depends on the usage of the service whether there are spill-overs between two types of content, and hence impact on the user experience. Moreover, for some streaming services, music could be consider UGC content too. If the licensed music would be uploaded without editorial control, such as by artists themselves, such uploaded music could constitute ‘information provided by a recipient of service’. The copyright licensing regime is not determinative from the perspective of qualifying as a hosting service or an online platform. (Chapters 6–7). Figure 9.2 depicts such a situation.

At the time of writing, porn websites are very likely trying to use such separation technicalities to deflate the actual size of their services. This is clear from the fact that services like YouPorn, PornHub or Xvideos, which are in the top 20 websites around the world,¹⁹ initially either did not report any or report very low numbers²⁰—perhaps to

¹⁹ ‘Top Websites Ranking - Most Visited Websites in July 2023’ (*Similarweb*) <<https://www.similarweb.com/top-websites/>> accessed 1 September 2023.

²⁰ Youporn, ‘EU Digital Services Act’ <<https://www.youporn.com/information/#eudsa>> accessed 1 September 2023 (‘7.3 million average monthly recipients’).

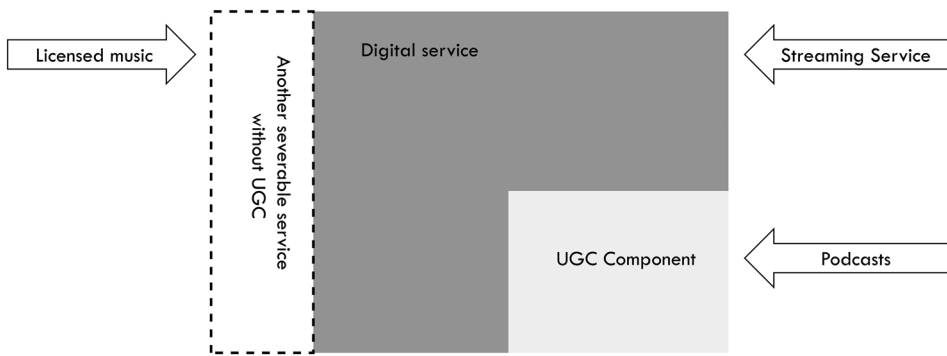


Figure 9.2 Scope of digital services: streaming service

avoid regulation and more scrutiny. Xvideos eventually conceded to be big enough to become a VLOP.²¹

Another set of issues concerns search engines specifically. Since search engines and online platforms have the same threshold, the problem only arises if two types of services are combined. Bing's search qualifies as a VLOSE. Even its integration of a ChatBot could count as a regulated non-UGC design feature. However, it is less clear whether its advertising intermediation arm constitutes only part of the service or an entirely separate VLOP. The storage of advertising and keywords qualifies as hosting, and the publication of the former should arguably constitute an online platform. If this is the case, the question is whether Bing's search size also elevates its advertising arm into a VLOP. Arguably, the answer should be yes since the advertising appears in the same search results. This can have consequences for the content moderation side of advertising and its relationship with advertisers, such as their disputes.

Finally, messaging services are regulated differently depending on how they operate. Cloud-based messaging such as Telegram or Messenger constitutes hosting (Chapter 7), while storageless messaging such as Signal qualifies as a mere conduit service. If the groups or channels on cloud-based messaging services are public, they can constitute online platforms. In Messenger's case, it is a feature integrated into a social network that remains regulated along with the main product. However, in Telegram's or Viber's case, this again begs the question of how to count the users. Arguably, if the user base for two functionalities is severable, the provider can deduce the numbers for non-platform activities, such as private messaging. But, as noted above, if the spillovers between two functionalities are strong, it might be hard to count users separately.

Finally, providers are not prohibited from using methodology that inflates their numbers. While Article 24(2) asks for specific information, if more methodologies are

²¹ Xvideos initially did not disclose the numbers. But after a while, they disclosed having 160 million users which puts them among VLOPs (see Chris Köver, 'XVideos wird erste Pornoplattform in der Liga der Riesen' (*Netzpolitik.org*, 28 September 2023), <<https://netzpolitik.org/2023/digitale-dienste-gesetz-xvideos-wird-erste-pornoplattform-in-der-liga-der-riesen/>> accessed 28 September 2023).

acceptable, it is unlikely that the providers will be punished for higher than actual disclosures. In the absence of a common methodology, the numbers thus are not entirely comparable between providers. This is why the European Commission uses its own methodology to calculate the supervision fee.

One of the difficulties in practice is determining the borders of a particular service. This will be soon addressed by the General Court in *Zalando v European Commission*.²² As mentioned, Zalando argues that it can separate the average number of monthly users of its marketplace platform from those for its own online retail business. Such hybrid marketplaces pose several problems. If separation does not exist in the user experience, can it be created to count users? If the same users can browse the provider's own products and third-party products in the same interface and move seamlessly between them, can we split the user base?

My view is that unless such providers can show some strong evidence of separation in the user experience, providers need to count all user numbers together. While this might over-include some providers which pose fewer systemic risks, the DSA (unlike the Digital Markets Act) does not need interrogation of the actual impact on the markets or society, even if it does impose additional special obligations on the providers.²³ The 'reach threshold' of 45 million monthly active users is an arbitrary yardstick agreed upon in the legislative process. Thus, all that matters is the presence of users on the user interface. This is why Amazon's lawsuit²⁴ against the designation is so baffling. It seems clear that the company meets the threshold, and it is irrelevant whether the impact of its marketplace is incomparable with that of social media. The legislature's will is fairly clear.

As can be seen here, the definition of the recipient of the services in the DSA is very broadly worded in Recital 77:

Accordingly, the number of average monthly active recipients of an online platform should reflect all the recipients actually engaging with the service at least once in a given period of time, by *being exposed to information disseminated on the online interface of the online platform*, such as viewing it or listening to it, or by providing information ...²⁵

Thus, as long as the interface exposes its own offers to the same users as those of third-party traders, I am sceptical that an artificial separation, such as by considering attributable turnover, can be made to determine the reach of the service.

9.2.3 A notion of the service

The above examples show that the DSA sometimes needs to separate the UGC and non-UGC components (eg hybrid marketplaces or streaming services) to decide

²² Case T-348/23 *Zalando v Commission* (case in progress, lodged 27 June 2023).

²³ However, see section 9.3.1 on the broader implications of being designated as a VLOP/VLOSE.

²⁴ Case T-367/23 *Amazon Services Europe v Commission* (Case in progress, lodged 5 July 2023).

²⁵ DSA, Rec 77 (emphasis mine).

which surface it applies to under the concept of a ‘service’. In other cases, the DSA must separate the platform from the non-platform side (eg messaging services) for the same purpose. In both cases, the separation revolves around the notion of an ‘online platform’ and the scope of the concept of ‘service’. One possible approach to test the separation is as follows.

Article 3(i) defines an online platform as a ‘service’ that ‘*also* disseminates information to the public’. The definition provides a carve-out for a service which disseminates information to the public as ‘purely ancillary features’ or ‘minor functionalities’ of another principal service. However, such features or functionality must be inseparable to be excludable. *Inseparability* is defined as a situation when a functionality or feature ‘cannot be used without that other service, and the integration of the feature or functionality into the other service is not a means to circumvent the applicability of this Regulation’ (Article 3(i)).

Thus, the DSA potentially includes the following test for *separability* between a service and its parts that should fall under a different regime: *If a feature or functionality can be used without the principle service and is not split only to circumvent the application of the DSA, it is severable.*

Now, this would suggest several criteria. First, the words ‘can be used’ suggest that the user experience, rather than technological design, business side, or corporate organisation, determines the outcome. Second, the separability in the user experience must be somewhat ‘natural’ and cannot be forced, having been motivated by a desire to circumvent the DSA. Thirdly, the definition says nothing about the companies providing the ‘service’, which suggests that they are irrelevant for legal classification.

Equipped with such a derived test, one can try to resolve some of the thorny DSA questions ranging from which parts of the service should count users (Article 24) and who becomes a VLOP (Article 33), to the question whether the service is provided by a mid-sized company or not (Article 19), and what is the place of (main) establishment of the company behind the service for the purposes of allocating the public supervision (Article 56).

The DSA does not define which company or companies are responsible for the service. Problems arise if one company provides two or more services used by users or when one or more companies provide one service, whether jointly, or independently, used by users.

First, consider a somewhat simpler situation when a provider has several interfaces through which it provides a service (eg ‘.de’, ‘.fr’, apps, user-accounts, etc.) and different companies operate such versions of the service. The key legal question can arise, for instance, regarding whether two language versions of one product are still the same service for VLOP counting, or whether they have common or separate places of establishment. Based on the DSA’s goal to capture ‘online platforms’ whose number of users ‘reaches a significant share of the Union population’,²⁶ it would seem logical to ignore minor version differences within the European market if the users

²⁶ DSA, Rec 76.

experience essentially the same product operated from one center. The argument would be that users who switch between country versions are still exposed to the same product, only on different addresses and different language versions. Arguably, the outcome should not be any different, even if the same provider uses a different company for each language version. Accepting such strategy when counting users would create a simple way for companies to keep the number of monthly active users almost *always* below the VLOP threshold and to undermine the idea that there should be only one main place of establishment if the service has several establishments in the EU.

Now, imagine another strategy. A provider splitting an online platform into two services operated by two companies. One which operates the UGC component and has less than 50 employees, or €10 million turnover, and the other which sells advertising and exceeds the threshold. The company thus potentially does not become regulated as an online platform. Again, the DSA does not have explicit provisions against such tactics. However, the relevant Recommendation foresees the notions of partner and linked enterprises whose employee headcount and turnover must also be considered (e.g., in case one company controls the other).²⁷ Thus, as long as two companies would be linked or viewed as jointly responsible for the service, the strategy to separate into several small economic entities would not work.

As argued above, a possible unifying argument in all these cases is that the regulation's goal is to capture a service organised around a specific user experience. Thus, even if the functionality is not operated by the same company, as long it is not *experienced as distinct by users*, it should count as unitary service. During review of the DSA, the legislature should consider adopting definition of 'service' and 'responsible companies' that can capture several entities, such as the term 'undertaking' in competition law. For instance, the Delegated Act on Supervisory Fees, which foresees a situation where a fee decision is 'addressed to more than one legal person' who are then 'jointly and severally liable for the payment' (Article 6(4)).²⁸ This clearly indicates that two or more companies could be understood as providing one service.

Intuitively, we understand the above situations as attempts to circumvent the DSA. However, drawing the boundary might be even harder in some cases. For instance, if a conglomerate starts buying different local marketplaces around the EU with the idea to keep their local brands but starts giving them the same systems, back-end, and support, at which point does it become a single service for the purposes of online platform definition, but also for counting its users? Again, intuitively, we understand that if a company starts harnessing the economies of scale and increases the integration of various products, thus creating an equivalent user experience, it will constitute one service at some point. However, at which exact point? The DSA has no answer to this question.

²⁷ Commission Recommendation 2003/361/EC concerning the definition of micro, small and medium-sized enterprises [2003] OJ L124/36, Art 3.

²⁸ Commission Delegated Regulation (EU) 2023/1127, Art 8.

Consider franchising in the digital space. If a Finish franchisor offering a platform with job adverts has ten independent franchises across the EU, how do we determine the user numbers and the place of establishment? If we examine the question from the user's perspective, the argument, depending on the circumstances, could be: that even franchising leads to one product with the same design that is being offered across the EU. However, one could have also a situation where the franchising only concerns technology and know-how but all key operations regarding the digital service, such as pricing, and similar key business decisions, are independently controlled locally. On the other hand, for services with local deliveries (eg food), it is often the case that the users remain in the local siloes and never interact with across the different versions. Accepting this argument tries to inject too much social media logic into the user counting. The DSA never states that users must be exposed to each other on the same interface so that we can conclude that they are part of the same service. Arguably, at least for VLOP counting, the better approach is to focus on the number of users exposed to the same service rather than their ability to interact with each other. These considerations will also be key to determine the place of main establishment of the service that allocates the competence to different public authorities (Article 56).

Finally, a related problem is when one provider gives space to another provider within its service to do its own business with a heavy UGC component. An end-user sees layers of providers and does not always know who determines what. For instance, a social network creates a space for others to create their pages, allowing their owners to moderate content and users. In this case, the social network is clearly an online platform, maybe even a VLOP. However, how about the page owner, who also moderates content? Such an owner could qualify for the status of a hosting provider (see Chapter 6.2.1). Being a hosting provider brings advantages, such as the availability of a liability exemption, but also obligations (eg having a contact point and giving a statement of reasons). Would the DSCs in such matryoshka-style situations insist on their enforcement even though such hosting providers are themselves part of a broader online platform ?

In the DSA review, it will be worth revisiting how digital services are delimited to avoid these qualification problems, which are likely to result in a lot of litigation. While some of the issues can be solved by interpretation, other problems require explicit changes to the DSA.

9.2.4 On mini platforms

The DSA consciously excludes micro and small enterprises that operate online platforms from its most prescriptive regulations. Article 19 carves out such 'mini platforms' from the most onerous platform-specific (advanced) obligations, such as internal and external dispute settlement. The only exceptions to this rule are providers whose digital services reach a threshold of a VLOP or VLOSE. For them, the small company size is overshadowed by their large user base (Article 19(2)).

Small enterprises are defined by a Council Recommendation²⁹ as ‘an enterprise which employs fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million.’ Micro enterprises are those which employ ‘fewer than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 2 million.’³⁰ As a result, online platforms that do not exceed either 50 employees or €10 million annual turnover/balance sheet remain only subject to basic obligations for hosting services, and intermediary services. This notion, however, depends also on the linked and partner enterprises (Article 3 of the Recommendation), which means that a big parent holding company can easily disqualify smaller daughter companies from the status. Article 4 of the Council Recommendation and Article 19(1) moreover have transitory periods which means that reclassification is not immediate. It can take one or two years.

The DSA says nothing about whether companies operating DSA-regulated digital services must be exclusively or partly devoted to the DSA-regulated portion of a business. Thus, a media house earning 80% of its revenue from newspapers and 20% from a social network under the same company will have to be considered as a whole, despite the fact that most revenue is attributable to the DSA-irrelevant parts of the business. The company can legitimately restructure and spin out its less successful social network to a separate company that does not exceed the small enterprise threshold.

9.3 Judicial Review of VLOP/VLOSE Designation Decisions

Amazon, Pornhub, Stripchat, Xvideos, and Zalando, are currently litigating their designation as a VLOP before the General Court.³¹ The obvious reason why companies might seek invalidation is to avoid being regulated by the DSA. An ancillary motivation can be to avoid being regulated by other acts of EU law that are increasingly relying on the status of VLOPs as the regulatory thresholds. At the time of writing, five other legislative proposals are already relying on the concept: the Commission’s Proposal for the European Media Freedom Act,³² the European Parliament’s proposed addition to the Artificial Intelligence Act,³³ the Commission’s Proposal for the Political Advertising

²⁹ As defined in Commission Recommendation 2003/361/EC concerning the definition of micro, small and medium-sized enterprises [2003] OJ L124/36, art 2(2). Other EU laws do not necessarily use the same concepts, see Article 3 of Directive 2013/34/EU of the European Parliament and of the Council of 26 June 2013 on the annual financial statements, consolidated financial statements and related reports of certain types of undertakings, amending Directive 2006/43/EC of the European Parliament and of the Council and repealing Council Directives 78/660/EEC and 83/349/EEC (2013) OJ L 182 (anticipating higher thresholds).

³⁰ *ibid* art 2(3).

³¹ *Zalando v Commission* (n 22); *Amazon Services Europe v Commission* (n 27); *WebGroup Czech Republic v Commission* T-139/24; *Aylo Freesites v Commission* T-138/24; *Technius v Commission* T-134/24.

³² Commission, ‘Proposal for a Regulation of the European Parliament and of the Council establishing a common framework for media services in the internal market (European Media Freedom Act) and amending Directive 2010/13/EU’ COM(2022) 457 final, art 17.

³³ European Parliament, ‘Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021) 020—C9-0146/2021—2021/0106(COD))’ Document P9_TA(2023)0236, amendment 740 (‘AI systems intended to be used by

Regulation,³⁴ and the Commission's Proposal for the European Digital Identity Regulation.³⁵ Thus, in the years to come, the designation disputes can gain importance beyond the obligations imposed by the DSA.

The validity of the Commission's designation decisions pursuant to Article 33(4) of the DSA can be reviewed according to Article 263 Treaty on the Functioning of the European Union (TFEU), which provides that:

Any natural or legal person may, under the conditions laid down in the first and second paragraphs, institute proceedings against an act addressed to that person or which is of direct and individual concern to them, and against a regulatory act which is of direct concern to them and does not entail implementing measures.

The designation decisions are undoubtedly 'challengeable acts' because they are legally binding on the designated companies,³⁶ are based on a proper legal basis (Article 33(4))³⁷ and produce additional specific legal effects.³⁸ The direct annulment action can be undoubtedly initiated by affected companies who are on the receiving end of the designation because such designations are 'capable of affecting the interests of the applicant by bringing about a distinct change in his legal position.'³⁹ The companies can also seek preliminary injunctions to suspend the application of some of the special obligations of the DSA before the Court examines the status. For instance, Amazon succeeded in temporarily suspending the application of Article 39 about the advertising archives in its pending case with the argument that it 'enable third parties to access significant trade secrets concerning the advertising strategies of the applicant's advertising customers.'⁴⁰ The President of the General Court, however, declined to grant the same order regarding Article 38, the mandatory opt-out mechanism for the recommender systems. On appeal, the European Court of Justice lifted the interim measures with reference to the balance of interests.⁴¹

While such designations also produce legal effects on third parties, such as consumers or researchers who gain new rights, their standing to challenge designations is less likely. Firstly, since they need to challenge an act of the Commission, they would be

social media platforms that have been designated as very large online platforms within the meaning of Article 33 of Regulation EU 2022/2065, in their recommender systems to recommend to the recipient of the service user-generated content available on the platform.')

³⁴ Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the transparency and targeting of political advertising' COM(2021) 731 final, art 7(6).

³⁵ Commission, 'Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity' COM(2021) 281 final, art 12b.

³⁶ Case C-911/19 *Fédération bancaire française (FBF)* ECLI:EU:C:2021:599, para 36.

³⁷ Case T-113/89 *Nefarma* ECLI:EU:T:1990:82, para 68.

³⁸ Case T-258/06 *Germany v Commission* ECLI:EU:T:2010:214, para 27.

³⁹ C-322/09 P *NDSHT v European Commission* ECLI:EU:C:2010:701, para 45.

⁴⁰ Case T-367/23 R *Amazon Services v Commission* ECLI:EU:T:2023:589, para 64.

⁴¹ See C-639/23 P(R)), *Amazon v European Commission*, ECLI:EU:C:2024:277: 'it must be held that the interests defended by the EU legislature prevail, in the present case, over Amazon's material interests, with the result that the balancing of interests weighs in favour of dismissing the application for interim measures' (para 164).

effectively arguing against the designation and, thus, against the additional rights they might derive from it. It is quite clear that third parties are more likely to support, rather than contest, the Commission's designation that gives them rights. Second, even if it would make sense to challenge designations for third parties, they would need to demonstrate 'direct' and 'individual concern' (Article 263).⁴²

Consumers, researchers, and civil society are more likely to either *intervene* to support the Commission in designation disputes initiated by providers according to Article 40 of the Protocol on the Statute of the Court⁴³ or seek a declaration that the Commission is unlawfully failing to designate some providers which costs them extra rights according to Article 265 of the TFEU. As regards interventions, the threshold for standing differs. Article 265 TFEU speaks of 'establish[ing] an interest', which the case law interprets to mean a 'direct [and] existing interest' in the result of a case pending before the Court.⁴⁴

This route is used by NGOs less frequently in Luxembourg than in Strasbourg, and the Court of Justice of the European Union tends to be somewhat strict with the applications, usually favouring associations rather than individuals.⁴⁵ For representative associations composed of a broad membership, the Court tends to waive the requirement if the case is 'raising questions of principle liable to affect those members.'⁴⁶ For instance, the European Consumer Organisation (BEUC) has been repeatedly accepted as an intervener in this way.⁴⁷ Under the DSA, the same should be possible for associations of researchers, consumers, and possibly even of users in general. For NGOs, the Court cautiously accepts some that have shown to be directly involved with the issues.⁴⁸ Thus, the NGOs involved in the Codes of Conduct and give input for risk management by VLOP/VLOSEs could argue their standing. In *Zalando*, the General Court recently issued a pioneering decision that allowed a consumer organisation to intervene invoking the rights derived from Article 86.⁴⁹ This is an encouraging signal that interventions by NGOs in the DSA-related direct cases in Luxembourg might become more commonplace. In my view, this is necessary given that industry usually asks

⁴² Case C-25/62 *Plaumann v Commission* ECLI:EU:C:1963:17 (direct concern); C-486/01 *Front national v European Parliament* ECLI:EU:C:2004:394 (individual concern).

⁴³ Protocol (No 3) On the Statute of the Court of Justice of The European Union [2004] OJ C-310/210, art 40.

⁴⁴ Case T-138/98 Order of the President of the First Chamber of the Court of First Instance of 3 June 1999 in *ACAV and others v Council* ECLI:EU:T:1999:121, para 14; Viktor Luszcz, *European Court Procedure: A Practical Guide* (Hart Publishing 2020) 629ff.

⁴⁵ Jasper Krommendijk and Kris van der Pas, 'To Intervene or Not to Intervene: Intervention before the Court of Justice of the European Union in Environmental and Migration Law' (2022) 26(8) *International Journal of Human Rights* 1394, 1403.

⁴⁶ C-151/97 P(I) Order of the President of the Court of 17 June 1997 in *National Power and PowerGen v British Coal and Commission* ECLI:EU:C:1997:307, para 66.

⁴⁷ Case T-612/17 Order of the President of the Ninth Chamber of the General Court of 17 December 2018 in *Google and Alphabet v Commission* (Google Shopping) ECLI:EU:T:2018:1007.

⁴⁸ Case T-37/04 R Order of the President of the Court of First Instance of 7 July 2004 in *Região autónoma dos Açores v Council* ECLI:EU:T:2004:215, para 57ff; see the debate in Luszcz (n 48) 634ff.

⁴⁹ Following initial rejection by the President of the General Court in 2023, the General Court permitted the European Information Society Institute (EISI), a consumer organisation, to intervene on behalf of the consumers on the side of the European Commission (Order of the Seventh Chamber of the General Court, T-348/23, 20th of March 2024) after successful appeal (C-647/23 P(I) - EISI v Zalando and Commission). The author acted as a lawyer for the NGO.

its own associations to support their positions. Involvement of NGOs is thus a question of equality of arms.

As regards actions against *failures to act*, the standing of individuals and organisations requires their ‘direct’ and ‘individual concern’ as is the case for actions for annulment.⁵⁰ Contrary to the wording of Article 265 of the TFEU, the applicant does not need to be potentially ‘addressed’ by such a decision, which means that even consumers, researchers, and civil society could qualify. According to the case law, if such an applicant could seek direct annulment of an act according to Article 263, it can also pursue an action against a failure to issue an act.⁵¹ A designation decision is clearly not discretionary.⁵² The Commission has a duty to designate if the conditions of the DSA are met.⁵³ The obligation according to Article 33(4) of the DSA is sufficiently well-defined and unconditional to be reviewed by Article 265 TFEU.⁵⁴

9.4 Separation of Liability and Accountability

The DSA’s significant regulatory contribution is splitting due diligence obligations from the liability for underlying content. Prior to the DSA, most laws tried to influence providers’ behaviour by threatening joint liability for their users’ actions. Save for some areas of law, the courts often faced a binary decision: impose a duty of care or deny it and confirm a liability exemption.⁵⁵ The DSA ends this binary. It comes up with its own expectations formulated as due diligence obligations. Providers violating them can be held to account. These legal obligations are separate from those of their users. The violations of the DSA have no bearing on the provider’s preservation of the liability exemptions. Even providers who are not liable for users remain accountable for their failings to be diligent. They are *accountable but not liable*.

The E-Commerce Directive (ECD) also acknowledged this separation between *liability* and *due diligence* obligations. Recital 48 ECD clarified that ‘this Directive does not affect the possibility for Member States of requiring service providers, who host information provided by recipients of their service, to apply *duties of care*, which can reasonably be expected from them, and which are specified by national law, in order to detect and prevent certain types of illegal activities’. Such duties of care referred to autonomous obligations, distinct and unrelated to the (tortious) liability issues. Hence, under the ECD, the Member States could legislate to impose such distinct measures, such as establishing complaint mechanisms or hotlines, to the extent that they did not violate liability exemptions. Given the divergences and fragmentation arising across

⁵⁰ Luszcz (n 48) 260ff.

⁵¹ C-68/95 *T Port v Bundesanstalt für Landwirtschaft und Ernährung* ECLI:EU:C:1996:452, para 59.

⁵² cf Case T-521/14 *Sweden v Commission* ECLI:EU:T:2015:976 (conditionality to issue delegated acts).

⁵³ Case T-164/10 *Pioneer Hi-Bred International v Commission* ECLI:EU:T:2013:503.

⁵⁴ Luszcz (n 48) 246ff.

⁵⁵ Martin Husovec, ‘Remedies First, Liability Second: Or Why We Fail to Agree on Optimal Design of Intermediary Liability’ in Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020).

Europe, the DSA removes that margin of manoeuvre from the Member States and introduces its own catalogue of ‘duties of care’ through harmonisation.

The DSA’s accountability-but-not-liability design was not an automatic choice. In the legislative process, the European Parliament strongly pushed to make the liability exemptions *dependent* on compliance with due diligence obligations. Thus, any violation of Chapter III of the DSA would make liability exemptions unavailable. The argument was that such conditionality would create a strong incentive for compliance. The liability exemptions would become a truly hard-earned ‘prize’ or a ‘privilege’ given only to those who respected the law in its entirety. A similar approach exists under section 79 of the Indian Information Technology Act 2000,⁵⁶ which makes the liability exemptions conditional upon ‘the intermediary observ[ing] due diligence while discharging his duties under this Act and also observ[ing] such other guidelines as the Central Government may prescribe in this behalf’. Related governmental acts, such as one applicable to social media, then further specify what such ‘due diligence’ duties mean.⁵⁷

The European Commission justified this design as follows:

Structuring due diligence obligations as a condition of the liability exemption would imply that compliance would be ultimately voluntary: the intermediary service would only be ‘incentivised’, but not ‘required’ to comply with the rules. It could make a calculation of risks, and consider that, based on national or Union laws, it would still not be held liable by a court, or that the costs of complying could be lower than the costs incurred through potential sanctions. In certain cases, the incentive for intermediaries to comply with the conditions to qualify for the liability exemption may well be limited, for example, when damage claims are not a realistic threat. However, intermediaries should not be left the choice whether or not to comply with the relevant requirements and self-standing obligation are required to achieve this objective.⁵⁸

In other words, the Commission argued that *conditionality* would not immediately improve compliance. It would also mean that those who stop qualifying for liability exemptions do not have to comply with due diligence obligations anymore, although they are performing the relevant technical function (eg non-neutral hosts). For platforms, the

⁵⁶ S 79, Indian Information Technology Act, No 21 of 2000 <https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf> accessed 29 August 2023.

⁵⁷ Part II(4)(4), Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, Notification of 25 February 2021, GSR 139(E) <<https://mib.gov.in/sites/default/files/IT%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20English.pdf>> accessed 29 August 2023 (‘A significant social media intermediary shall endeavour to deploy technology-based measures, including automated tools or other mechanisms to proactively identify information that depicts any act or simulation in any form depicting rape, child sexual abuse or conduct, whether explicit or implicit, or any information which is exactly identical in content to information that has previously been removed or access to which has been disabled on the computer resource of such intermediary under clause (d) of sub-rule (1) of rule 3, and shall display a notice to any user attempting to access such information stating that such information has been identified by the intermediary under the categories referred to in this sub-rule’).

⁵⁸ Commission, “Impact Assessment” (Commission Staff Working Document) Accompanying the Document “Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (DSA) and Amending Directive 2000/31/EC” SWD(2020) 348 final, annex 9.

application of liability privileges would become a nightmare because they are subject to many open-ended obligations. In my view, such conditionality would tilt the incentives even more in the direction of over-removal because any misstep would have grave consequences. It would put the DSA's balanced and tailored rules under a one-sided incentive structure. Moreover, given the vagueness of some of the due diligence obligations, the liability exemption would be useless as a legal defence. Already under section 512 DMCA, some providers preferred to confront liability norms directly rather than liability exemptions because of the long laundry list of the conditions that the provider must meet.⁵⁹

A regulatory design that makes liability exemptions conditional upon observance of all the due diligence obligations has two potential outcomes: in a better case, it pronounces them redundant, or in a worse case, it suggests to the courts that to be free of liability for others, a long list of conditions must first be met. To make liability exemptions conditional upon satisfying due diligence obligations would be to force providers to balance on the edge of a cliff, knowing that one small slip would send them tumbling into national liability chaos.

In my view, the most important debate gets lost when we bundle due diligence obligations and the liability for third-party content. Any non-compliance can potentially mean dramatic consequences. The key calibration of the system should be in deciding what tailored incentives for compliance are proportionate, proper, and effective. If everything is lumped together in one lot, the enforcement system is under strain to target its responses. The DSA's design allows for a better escalation of enforcement and tailoring of its demands. Plus, the DSA's mixture of private and public enforcement of two separate systems—liability for content and accountability for due diligence obligations—is arguably superior to a 'one-size-fits-all system.' In fact, this design feature is part of what sets the DSA apart as a better regulatory model (see Chapter 21).

That being said, due diligence obligations continue to have some meeting points with liability exemptions. If a provider is obliged to conduct a check of some information and, while doing so, acquires actual knowledge, the two obligations can run a very similar course. However, the opposite is also easily true. A provider that fails to act upon knowledge but provides properly presented but legally incorrect explanations acts correctly in terms of procedure but can still become liable along with its users for failing to take down illegal content. Similarly, a provider that fails to issue a content creator with the statement of reasons and thus violates its procedural due diligence obligation might still correctly assess the case on substance.

⁵⁹ In the decisions of the United States Court of Appeals, Ninth Circuit in *Perfect 10 Inc v Visa International Service Association* 494 F 3d 788 (9th Cir 2007), the Court notes at fn 4 that: 'Because Defendants are not "service providers" within the scope of the DMCA, they are not eligible for these safe harbors. The result, under Perfect 10's theories, would therefore be that a service provider with actual knowledge of infringement and the actual ability to remove the infringing material, but which has not received a statutorily compliant notice, is entitled to a safe harbor from liability, while credit card companies with actual knowledge but without the actual ability to remove infringing material, would benefit from no safe harbor. We recognize that the DMCA was not intended to displace the development of secondary liability in the courts; rather, we simply take note of the anomalous result Perfect 10 seeks'. For a broader debate of s 512 from the European perspective, Martin Husovec, 'Rising Above Liability: The Digital Services Act as a Blueprint for the Second Generation of Global Internet Rules' (2023) 38 Berkeley Technology Law Journal 883, https://btlj.org/wp-content/uploads/2024/01/0002_38-3_Husovec.pdf).

In the following chapters, the book takes the reader through three basic areas of obligations: content moderation, risk management, and transparency. Although demarcated as such, these three areas are not water-tight compartments; the separation allows me to better explain their different features. Content moderation rules are mostly about the process of how decisions are made. Transparency/oversight rules are about what gets published, controlled, and notified by whom. Finally, risk management rules are about how companies must redesign their services and further test, monitor, and improve the working of their systems to better manage risks posed by the functioning and use of their services. Table 9.4 provides a quick overview of Part III of the DSA.

Table 9.4 Overview of due diligence obligations.

Obligations	Universal <i>All providers of mere conduit, caching, hosting services</i>	Basic <i>all hosting services</i>	Advanced <i>medium-to-large online platforms</i>	Special <i>VLOPs & VLOSEs</i>
Content Moderation	Art 14 (fair rules)	Art 16 (notice submission) Art 17 (statement of reasons) Art 18 (notification of suspected relevant crimes)	Art 20 (internal redress) Art 21 (out-of-court mechanism) Art 22 (trusted flaggers) Art 23 (anti-abuse provisions) Art 30–32 (specific rules on B2C marketplaces)	Art 38 (recommender systems) Art 34–35 (general risk management) Art 45–48 (Codes of Conduct)
Risk-based Approach (design, functioning, use of a service)	N/A		Art 25 (fair design of user experience); Art 26(3) (profiling in advertising); Art 27 (recommender systems); Art 28 (protection of minors); Art 30 (traceability of traders); Art 31 (facilitating design for traders)	
Transparency and Oversight	Art 11 (regulator's contact point); Art 12 (recipient's contact point); Art 13 (legal representative); Art 15 (content moderation reporting);	N/A	Art 22 (reports by trusted flaggers); Art 24 (content moderation reports plus); Art 24(5) (database of all the statements of reasons); 24(2) (monthly users reporting); Art 26 (advertising disclosure)	Art 39 (advertising archives); Art 37 (auditing); Art 40 (data access); Art 41 (compliance function); Art 42 (content moderation transparency)

Content Moderation: Outline

10.1 Evolution of Practices	185	10.5 Due Process and Its Criticisms	193
10.2 Regulation as Division of Powers	188	10.5.1 Why binding rules?	196
10.3 Rule-Setting and Its Legitimacy	189	10.5.2 Can procedural rights help?	196
10.4 User-Empowerment and Customisation	192	10.5.3 Why privatising justice?	197
		10.5.4 What about costs of compliance?	198

10.1 Evolution of Practices

While the term ‘content moderation’ is relatively novel, it describes a practice that is as old as the internet itself.¹ Probably the oldest content moderation debate concerns the distribution of unsolicited emails, better known as spam.² The zero cost of emailing immediately invited abuse. Given that charging per email sent was not viable,³ the solutions ended up being social, technological, and legal. Email providers started classifying spam sent by people and automated technology and deprioritising it in inboxes.⁴ As every email user knows, none works perfectly. Technology gets the classification wrong occasionally, important messages get lost, and laws do not fully deter companies from abusing email. The problem is somewhat under control, but users must exercise care when using email. Despite being based on open protocols, today, Apple Mail and Google’s Gmail make up 87.02% of the total email client market.⁵ Senders who these two companies wrongly classify have difficulties delivering anything to anyone.

¹ The early cases decided at the dawn of the internet era, such as *Prodigy* in the US, or *CompuServe* in Germany, were about content moderation. They were only framed as intermediary liability problems—see ch 4.

² Before emails, spam was observed on Usenet newsgroups. See ‘History of Email Spam’ (*Wikipedia*, 7 May 2023) <https://en.wikipedia.org/w/index.php?title=History_of_email_spam&oldid=1153712174> accessed 2 September 2023.

³ In the 1990s, the question was debated under the notion of ‘bit tax’, see UNDP (ed), *Human Development Report 1999* (OUP 1999) 66 (‘There is an urgent need to find the resources to fund the global communications revolution—to ensure that it is truly global. One proposal is a “bit tax”—a very small tax on the amount of data sent through the Internet. The costs for users would be negligible: sending 100 emails a day, each containing a 10-kilobyte document [a very long one], would raise a tax of just 1 cent’).

⁴ See the famous 2002 essay by Paul Graham, ‘A Plan for Spam’ (August 2002) <<http://www.paulgraham.com/spam.html>> accessed 3 September 2023.

⁵ Oberlo, ‘Most Used Email Clients Worldwide’ (July 2023) <<https://www.oberlo.com/statistics/most-used-email-clients>> accessed 3 September 2023.

Content moderation on digital services, such as social media, suffers many of the same problems. Zero cost of use invites abuse. Again, we observe the implementation of social, technological, and legal solutions. And again, we observe how imperfect they are. What has changed, however, is that the range of content moderation surfaces and types of decisions are much wider (eg labelling, explaining, hiding, geotargeting, demonetising, etc).⁶ Unlike with spam, the debate about content moderation today is more visceral because the underlying standards are more political in nature. The decisions are now not only about what content is an unsolicited commercial message but also what content counts as legitimate, bad, or newsworthy. And the scale of decision-making is truly mind-boggling. In just three months, Facebook took down 914,500,000 pieces of content and YouTube 4,496,933 videos.⁷ To a large extent, content moderation has become a 'decision factory'.⁸

Content moderation has become an umbrella term for all activities of digital providers that affect users' content. Academics have offered many definitions over the years.⁹ Scholars of science and technology studies and law have been documenting and studying content moderation practices and challenges for years.¹⁰ In her influential work, Kate Klonick conceptualised content moderation as a new type of governance,¹¹ a 'bureaucracy',¹² drawing parallels to administrative and constitutional law.¹³ In a model like hers, providers are portrayed as powerful rule-makers and enforcers.¹⁴ The analogy with the administrative state invites us to think about the deficiencies of the process.¹⁵ It sheds light on the legitimacy of the underlying rules,¹⁶ and the extent of the state's pressure on such decision-making.¹⁷

⁶ See extensively, in Evelyn Douek, 'Content Moderation as Systems Thinking' (2022) 136(2) *Harvard Law Review* 526.

⁷ *ibid* 537–38.

⁸ Robyn Caplan, 'Content or Context Moderation?' (Data & Society 2018) 23 <<https://datasociety.net/library/content-or-context-moderation/>> accessed 3 September 2023.

⁹ eg Grimmelmman defines it as 'the governance mechanisms that structure participation in a community to facilitate cooperation and prevent abuse', see James Grimmelmman, 'The Virtues of Moderation' (2015) 17 *Yale Journal of Law and Technology* 42, 47; Tarleton Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media* (Yale UP 2018) 4, 6.

¹⁰ Gillespie (n 9); Rebecca MacKinnon, *Consent of the Networked: The Worldwide Struggle for Internet Freedom* (Basic Books 2012); Hannah Bloch-Wehba, 'Automation in Moderation' (2020) 53 *Cornell International Law Journal* 41, 56; Robert Gorwa, Reuben Binns, and Christian Katzenbach, 'Algorithmic Content Moderation: Technical and Political Challenges in the Automation of Platform Governance' (2020) 7(1) *Big Data & Society* 2053951719897945, 2; Grimmelmman (n 9) 63–70; Danielle Keats Citron, *Hate Crimes in Cyberspace* (Harvard UP 2014); Kate Klonick, 'The New Governors: The People, Rules, and Processes Governing Online Speech' (2018) 131 *Harvard Law Review* 1598; Nicolas P Suzor, *Lawless: The Secret Rules That Govern Our Digital Lives* (CUP 2019); Sarah T Roberts, *Behind the Screen: Content Moderation in the Shadows of Social Media* (Yale UP 2019); David Kaye, *Speech Police: The Global Struggle to Govern the Internet* (Columbia Global Reports 2019).

¹¹ Klonick (n 10).

¹² The term is used by Douek to describe what she regards as standard content moderation scholarship, pointing to, among others, the works of influential works of Kate Klonick and Rebecca MacKinnon, see *ibid*; MacKinnon (n 10) 153–54.

¹³ Klonick (n 10) 1163; Douek, 'Content Moderation as Systems Thinking' (n 6) 538.

¹⁴ Klonick (n 10) 1163.

¹⁵ *ibid* 1664–65; Gillespie (n 9); Suzor (n 10); Roberts (n 10).

¹⁶ Suzor (n 10).

¹⁷ Jack Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (OUP 2006); Evelyn Douek, 'The Rise of Content Cartels' (*Knight First Amendment Institute at Columbia University*, 11 February 2020) <<https://knightcolumbia.org/content/the-rise-of-content-cartels>> accessed 3 September 2023. Most recently, this topic has been debated with respect to so-called Twitter files, see Adam Rawnley and Asawin Suebsaeng, 'Twitter

The conceptualisation is also helpful when diagnosing the human rights interferences (Chapter 3).¹⁸

However, viewing content moderation only as a new governing bureaucracy is a very static view. It directs our attention away from the deeply commercial nature of the practice. It potentially clouds our view of practical solutions that might lie in increasing consumer choice through competition or regulation. Regulators thinking of regulating the assembly line of decisions cannot ignore its intimate relationship with the product design and profit of these digital services. For instance, according to a theory paper in economics, providers with subscription and advertising models have very different incentives in terms of content moderation strategies.¹⁹ The advertising-based services tend to moderate more because they are more concerned about the size of their user base. Content moderation is, therefore, as much ‘trust and safety’ as it is ‘size and profit’. Companies set rules and enforce them, but they primarily do so to attract and retain their user base and advertisers with stricter standards²⁰ under conditions that also keep their employees happy and enforcement authorities at bay.

Content moderation should be viewed from different angles depending on the context. When it enforces the rules adopted by legislatures as a form of delegated enforcement, it is helpful to think of it as a bureaucracy, a co-regulatory form of governance where the rules are set by the state. When providers cross the legality lines and start ordering lawful content, it is better to think of them as optimisers whose ultimate goal is to make a profit. Because the two contexts are so inextricably mixed in daily practice, ultimately, the best way is to keep thinking about both angles all the time.

The Digital Services Act (DSA) arguably takes both views into account. Whenever it is relevant, the DSA draws the distinction between two sets of decisions: on the illegality or violation of the terms and conditions of services. The regulation confers almost uniform due process rights on all content moderation decisions but also leaves legitimate rulemaking of companies mostly unconstrained. The regulation is more about the standards the companies making these decisions must observe when deploying their solutions. It gives companies constraints within which they can optimise their rule-setting and enforcement without running afoul of the public interest.

Kept Entire “Database” of Republican Requests to Censor Posts’ *Rolling Stone* (8 February 2023) <<https://www.rollingstone.com/politics/politics-news/elon-trump-twitter-files-collusion-biden-censorship-1234675969/>> accessed 3 September 2023. The conservatives reacted by seeking an injunction before US federal Courts. In July 2023, a US federal judge restricted some agencies and officials of the administration of President Joe Biden from meeting and communicating with social media companies to moderate their content, see *State of Missouri et al v Joseph R Biden Jr et al* 3:22-CV-01213 (WD La Mar 20, 2023). For context, see Jon Brodtkin, ‘Judge Rules White House Pressured Social Networks to “Suppress Free Speech”’ *Ars Technica* (5 July 2023) <<https://arstechnica.com/tech-policy/2023/07/judge-rules-white-house-pressured-social-networks-to-suppress-free-speech/>> accessed 3 September 2023.

¹⁸ Kaye (n 10) 16; Timothy Garton Ash, *Free Speech: Ten Principles for a Connected World* (Yale UP 2016) 369.

¹⁹ Yi Liu, Pinar Yildirim, and Z John Zhang, ‘Implications of Revenue Models and Technology for Content Moderation Strategies’ [2021] Mack Institute Working Paper <<https://marketing.wharton.upenn.edu/wp-content/uploads/2021/09/09.2021-Liu-Yi-JMP.pdf>> accessed 3 September 2023.

²⁰ This point is also made by Facebook employees, see Klonick (n 10) 1627.

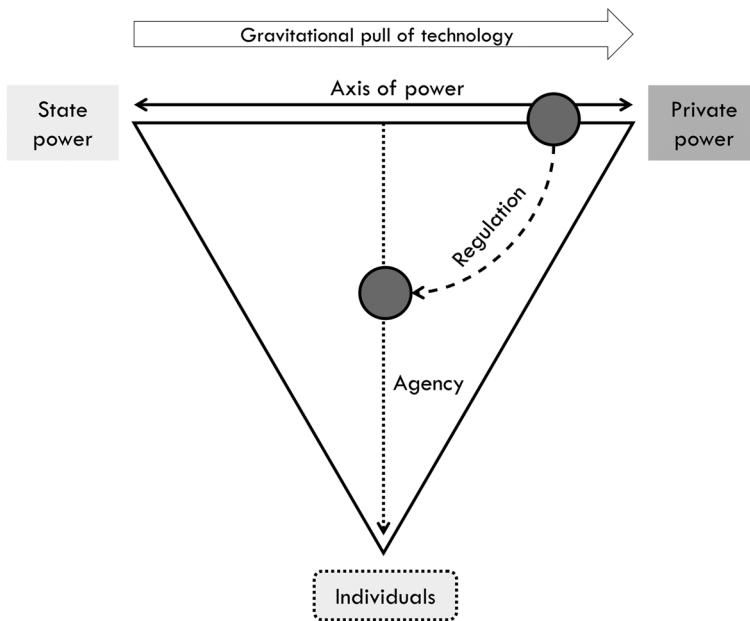


Figure 10.1 Redistribution of power

10.2 Regulation as Division of Powers

In his book, *Liberalism and its Discontents*, Francis Fukuyama argues that the digital ecosystem creates serious challenges for the classical conception of liberalism. He observes what many internet law scholars have over the last two decades,²¹ namely that ‘artificial concentrations of power over speech’²² threaten to undermine our liberties. In the 1990s, techno-libertarians took liberalism to the extreme by arguing against *any* public intervention in cyberspace and supporting limitless self-regulation. This argument is most famously embodied in John Perry Barlow’s 1996 Declaration of Independence of Cyberspace.²³ The last 20 years have shown that the period of inaction—where the state shies away from any state intervention—mostly cedes power from public to private hands (see Figure 10.1).

If one accepts that the only way of keeping any power in check is its division in a society,²⁴ it is inevitable that some form of state regulation is needed to divide the power

²¹ Without trying to be exhaustive, some of the early works include: Goldsmith and Wu (n 17); Rebecca Tushnet, ‘Power Without Responsibility: Intermediaries and the First Amendment’ (2008) 76 *The George Washington Law Review* 986; Jonathan Zittrain, *The Future of the Internet: And How to Stop It* (Yale UP 2008); Yochai Benkler, ‘A Free Irresponsible Press: Wikileaks and the Battle Over the Soul of the Networked Fourth Estate’ (2011) 46 *Harvard Civil Rights—Civil Liberties Law Review* 311.

²² Francis Fukuyama, *Liberalism and Its Discontents* (Profile Books 2022) 99.

²³ John Perry Barlow, ‘A Declaration of the Independence of Cyberspace’ (8 February 1996) <<https://www.eff.org/cyberspace-independence>> accessed 3 September 2023.

²⁴ For the critical and modern account of the separation of powers, see NW Barber, *The Principles of Constitutionalism* (OUP 2018), ch 3; Jean-Marc Sauvé, ‘The Judiciary and the Separation of Powers’ (*Conseil*

that markets and technology have allowed private firms to accumulate²⁵ through their popular products. However, the pendulum can swing too far in the state's corner, too. Proposals that want the state to assume too big a share of the powers over the digital ecosystem threaten to undermine people's liberties all the same, if not worse. In the ideal state, public power must negotiate with private power and people over the outcomes. Each side keeps the other in check (Chapter 1).

The DSA is a creature of European law-making, which might appear too heavy-handed for some jurisdictions.²⁶ However, it does get right arguably the most important aspect—the division of power between companies, states, and people. This aspect is most visible in how it regulates content moderation. Unlike laws that try to impose 'view-point neutrality',²⁷ it constrains without taking away all the power of private companies. It does so by recognising the salience of private decision-making about people's digital presence, which it tries to subject to due process procedures while leaving the formulation of policies regarding legal content mostly intact. Although companies lose their monopoly over the interpretation of their contractual policies,²⁸ they keep the ability to rewrite them. However, they lose their status as the final arbiters of disputes, but they can avoid new ones by clarifying contractual clauses and improving how they solve disputes with users internally.

Thus, the DSA constrains rule-interpretative powers without substantially challenging rule-making powers. The rule-making powers are obviously shared with the state forming rules for a polity through a parliament. The outcome is a greater division of powers: people have individual rights to contest decisions but can only make rules through elective representatives or lobbying their providers—in both cases, they must reconcile their interests with those of others.

10.3 Rule-Setting and Its Legitimacy

The power to make content moderation decisions can be vested with different actors. It can be vested exclusively with providers, content creators and their communities or variously shared among these actors. Thus, content moderation can manifest itself in the following four basic models: top-down, user-centric, community-driven, and mixed models. In addition, each of these models can outsource some content

d'État, 22 June 2011) <<https://www.conseil-etat.fr/publications-colloques/discours-et-interventions/the-judiciary-and-the-separation-of-powers>> accessed 3 September 2023.

²⁵ This point is made most repeatedly by Zittrain (n 21).

²⁶ This is especially the case for the risk mitigation part.

²⁷ See Florida Social Media Bill, SB 7072, 27th Leg, 1st Reg Sess (Fla 2021); Texas Social Media Bill, HB 20, 87th Leg, 2d CS (Tex 2021). The Polish bill was meant to protect against 'censorship' by prohibiting moderation of legal content, see Maria Wilczek, 'Law to Protect Poles from Social Media "Censorship" Added to Government Agenda' (*Notes From Poland*, 5 October 2021) <<https://notesfrompoland.com/2021/10/05/law-to-protect-roles-from-social-media-censorship-added-to-government-agenda/>> accessed 3 September 2023.

²⁸ In theory, courts were always present; in practice, not so much.

moderation to third parties—charities or for-profit firms—that provide tools or people to help with the decision-making.

For instance, a newspaper using social media to distribute its content can hire a company to detect and hide hate speech on its page. A provider can rely on its web hosting providers' tools to detect child abuse images. A short-rental platform might rely on the list of sex offenders compiled by charities. Webmail might rely on blacklists of spammers from some external companies. On most services today, content moderation can rarely be kept entirely in-house. It incorporates various inputs or outsourcing from others. Even a person who runs a personal blog on WordPress will likely use one of the spam plug-ins for the comments section.

The more complex the service and the bigger its content moderation surface, the more likely it is that a company is relying on some external tools. The industry is already developing some standard tools for typical challenges, such as child abuse material or terrorist content.²⁹ Going forward, as argued in Chapter 20, the DSA is likely only to accelerate standardisation and outsourcing. The size of the market is not negligible. One study estimated that Reddit, a company of 2,000 employees and 52 million daily users, benefits from approximately 170,000 hours of free content moderation labour from its engaged users, which would correspond to a price of \$3.4 million a year.³⁰

The *locus* of content moderation decision-making influences who can set the underlying rules of engagement—what can be said by whom. In the top-down model, the rules are set by a provider; in the user-centric model, by users; in the community-driven model, by communities of users; and finally, in the mixed model, by several actors acting independently. On social media, the mixed model is usually employed.³¹ Providers do some moderation, and so do the users.

The reliance on a particular model of content moderation is especially sensitive when it comes to the regulation of *legal* content. The issue is less pronounced when firms try to implement parliament-mandated rules on illegal content because a user's preference for illegal content is simply an illegal preference. In contrast, purely top-down content moderation is more often blamed for lacking *legitimacy* whenever firms behind services try to redefine what legal content the public should see. Providers contractually limiting disinformation, shocking, vulgar, or self-harm content are criticised for imposing their worldview on their users. According to Pew Research, most Americans think that social media censors what they read, especially political viewpoints.³² At the same time, academic research shows that the general public does not necessarily see restrictions on disinformation as illegitimate.³³

²⁹ Gorwa, Binns, and Katzenbach (n 10); Douek, 'Content Moderation as Systems Thinking' (n 6) 543.

³⁰ Hanlin Li, Brent Hecht, and Stevie Chancellor, 'Measuring the Monetary Value of Online Volunteer Work' <<https://arxiv.org/abs/2205.14528>> accessed 3 September 2023. For statistics about the company, see 'Reddit' (Wikipedia, 31 August 2023) <<https://en.wikipedia.org/w/index.php?title=Reddit&oldid=1173100194>> accessed 3 September 2023.

³¹ See the analysis of Klonick (n 10); Douek, 'Content Moderation as Systems Thinking' (n 6).

³² Emily A Vogels, Andrew Perrin, and Monica Anderson, 'Most Americans Think Social Media Sites Censor Political Viewpoints' (Pew Research Center 2020) <<https://www.pewresearch.org/internet/2020/08/19/most-americans-think-social-media-sites-censor-political-viewpoints/>> accessed 3 September 2023.

³³ Anastasia Kozyreva and others, 'Resolving Content Moderation Dilemmas between Free Speech and Harmful Misinformation' (2023) 120(7) Proceedings of the National Academy of Sciences of the United States of

The main legitimacy of purely contractual top-down centres is that they help to fund platforms. A free service must be optimised to make money from advertisers.³⁴ The problem is that the preferences of users and advertisers can grow apart substantially. In such cases, some users might feel they are taken hostage by advertisers who fund the platforms. In the absence of changes to who pays for the services, the only way to satisfy such personal preferences is more diversity through *competition* and more choice for users through *customisation* of their experience.

But even with these two approaches, without a common baseline of what constitutes illegal content across markets, it is hard to avoid some top-down alignment of otherwise legal content. This ‘bridging’ of various notions of illegality is necessary to allow scalability and uniform application of the same rules across the markets. A lot of Europe’s hate speech is free speech in America, but contractual arrangements can bridge the gap.

The legitimacy of rule-setting is especially problematic when markets do not offer choice. If the markets for digital services are competitive, we are usually less concerned about the different standards that various services adopt unilaterally top-down. After all, business partners of providers, including content creators, can vote with their feet and leave for alternatives. For instance, content creators have left Twitch in droves because of its content moderation and advertising policies.³⁵ This is David Post’s idea of a ‘market for rules.’³⁶ However, as noted by Klonick because media services in the same category, such as that of social media, are not perfect substitutes but rather complements, even the existence of several services does not guarantee the existence of such markets.³⁷

When market concentration is coupled with extensive top-down content moderation, this increases the risk for society whenever legal content is constrained. Such dominant firms lack the legitimacy of properly elected parliaments and yet can make rules that affect what others can say and share. As argued by Fukuyama and his colleagues, ‘[p]rivate power faces no checks like popular elections; it can be controlled only by the government (through regulation) or by competition among power holders.’³⁸

America 1 (‘The majority preferred quashing harmful misinformation over protecting free speech. Respondents were more reluctant to suspend accounts than to remove posts and more likely to do either if the harmful consequences of the misinformation were severe or if sharing it was a repeated offense’).

³⁴ Moreover, as Klonick points out, the companies also face numerous other pressures, such as that of their employees: Klonick (n 10) 1655.

³⁵ Luci S, ‘Why Twitch Streamers Are Moving to YouTube’ (*Game Rant*, 12 September 2022) <<https://gamerant.com/twitch-streamers-moving-to-youtube-fuslie-faze-swagg-dr-disrespect/>> accessed 3 September 2023. This is partly caused by account bans (Jake Selway, ‘Every Major Twitch Ban of 2022 So Far, Explained’ (*Game Rant*, 26 April 2022) <<https://gamerant.com/all-major-twitch-bans-2022-overview-adin-ross-sodapoppin-itssliker/>> accessed 3 September 2023) but also by changes to advertising models (Tom Gerken, ‘Twitch Scraps Ad Changes after Streamers Leave Platform’ *BBC News* (7 June 2023) <<https://www.bbc.com/news/technology-65834521>> accessed 3 September 2023).

³⁶ David G Post, ‘Anarchy State and the Internet’ (1995) *Journal of Online Law*, art 3 <<https://ssrn.com/abstract=943456>> accessed 3 September 2023.

³⁷ Klonick (n 10) 1630.

³⁸ <>Francis Fukuyama and others, ‘Report of the Working Group on Platform Scale’ (Stanford Cyber Policy Center 2020) 7 <<https://cyber.fsi.stanford.edu/publication/report-working-group-platform-scale>> accessed 3 September 2023.

Fukuyama and his colleagues argue that *regulation should guarantee* that users can choose content moderation experience from a new class of middle-ware firms. Their solution is to create competition for such moderation, which should weaken the power of providers who run the digital service.³⁹ Their paper is not specific regarding the level of integration of middle-ware firms. However, their goal is to reduce the ‘unaccountable power that dominant platforms possess’ by disciplining it through competition forces and consumer choice.⁴⁰ In this sense, the proposal is very close to the DSA and Digital Markets Act (DMA). The DMA opens the private infrastructure to competition by increasing contestability, and the DSA asks companies to grant users agency when moderating content.

10.4 User-Empowerment and Customisation

The DSA’s focus on user empowerment also supports the idea of more diversity of digital experiences within the same products. Consider the example of a Slovak start-up that offers its content moderation product to commercial users of social media, such as news organisations. Because large American providers tend to under-invest in small markets with distinct languages, commercial users of social media in those markets must moderate much more content themselves if they want to truly benefit from social media. And this is where companies like *TrollWall* come into the picture.⁴¹ They offer an Artificial Intelligence (AI) tool that helps to detect hate speech at scale. Its customers can tailor the detection and decide how to act, such as whether to hide or remove the content. The tool is not error-free, but it saves news organisations time and effort. It acts as a more sophisticated ‘spam filter’ for social media. Because it keeps its users in charge, it is also less problematic. The client can decide what rules to set and how to enforce them. The newspaper’s readers who dislike the experience can stop following it on social media.

In a purely top-down model, only a platform can moderate content; no one else has that capability. While this model of content moderation might still be typical for some services, such as online marketplaces, it does not capture the reality of most digital services. Today, users are often given tools to block or hide, and content creators can remove content or block users. Content creators on YouTube or Facebook set and enforce their own rules for what they accept. While Facebook operates a huge decision factory, what can be seen by the public is equally influenced by numerous individual decisions by page or channel administrators. Providers do some central rule-setting and enforcement, and their content creators engage in their own rule-setting and enforcement in the shadow of the providers’ rules. The system, thus already, is not purely top-down.

³⁹ *ibid* 33–35.

⁴⁰ *ibid* 36.

⁴¹ ‘AI Autopilot For Comment Moderation’ (*TrollWall*) <<https://trollwall.ai>> accessed 3 September 2023.

Most digital services, including social media, already operate mixed models of content moderation with some level of agency given to users. However, providers do not always have business incentives to open all parts of their content moderation practices. Under self-regulation, user empowerment is mostly determined by what is convenient for companies. Some features will be offered by providers because they help the business. For instance, a dating app that does not allow customers to block other users would be quickly resented by those who use it. From the company's perspective, facilitating too much empowerment weakens its ability to set uniform rules across the services and thus attracts some advertisers. For instance, if advertisers ask for bans on nudity and nudity is left to users' personal preferences, the providers might not be able to deliver such bans. Once they empower users to make that choice, they cede the power to users. This is especially sensitive for features, such as recommender systems, that are too close to the bottom line of companies.⁴² Thus, there remains a role for regulation to empower users.

The above debate shows why user empowerment is about more than just *who* gets to decide. It is inevitably about how companies earn money and how much competition they will face from new entrants. The ability to customise increases people's agency and autonomy over their information diet. Naturally, it has less space with respect to content where legislatures made their call for something to be illegal. Decentralisation is not a choice of the legislature. If the legislature is wrong, individuals need to use their share of political power to change the content of illegality rules.

The primary benefit of customisation is that instead of patronisingly banning people from consuming unhealthy 'low-quality' or 'dangerous' (yet still legal) information, it asks them to do it by choice. If people become obese due to eating unhealthy food, society does not ask supermarkets to stop selling them unhealthy items; instead they offer better product information, increase awareness about health risks, and provide health care services. This empowering approach cannot solve all problems related to people's unhealthy information diets; however, such are the limits imposed by our commitment to liberalism and human dignity.

The DSA's content moderation rules promote individual agency by giving individual tools and procedural rights. The DSA's risk management rules can also promote empowerment and decentralisation. However, the written rules are so vague that the precise effects will depend on how the European Commission conceptualises its own role. In Chapter 15, I offer a way of looking at the rules that view risk mitigation as an empowerment-first approach for legal content.

10.5 Due Process and Its Criticisms

The DSA regulates content moderation in three ways: by *ex ante* rules on risk management, due process rights, and transparency obligations. Due process rights give

⁴² The recent attempt of Amazon to invalidate some of the DSA regulations of the recommender system is a good example of this—Case T-367/23 *Amazon Services Europe v Commission* (case in progress, lodged 5 July 2023).

(mostly procedural) rights to individuals vis-à-vis providers, and transparency helps reduce the opacity of how companies make decisions. Procedural rights and transparency are largely inspired by a declaration of numerous non-governmental organisations (NGOs) known as the Santa Clara Principles,⁴³ although it explicitly comes with a note that '[s]tates should not transform the Santa Clara Principles directly into legal mandates'.

Nicolas Suzor made the most powerful case for the procedural legal rules adopted by parliaments in his book *Lawless*, where he writes:

The absence of government regulation is not freedom. This book is called *Lawless* because so many of the decisions about what we can do and say online are made behind closed doors by private companies. This is the opposite of the standards we expect of legitimate, legal decision-making in a democratic society. Where governments do not set laws to regulate the internet, platforms and other powerful telecommunications providers are constantly making decisions about what types of speech they will carry. The major social media platforms all have rules about the content they deem acceptable, and many of these have expressed limits on hatred and abuse. Without law, though, these rules are not enforced in any way that can be called legitimate. There's no easy way to ensure either that the rules are consistently enforced or that they are enforced in a way that is fair and free from bias.⁴⁴

Suzor speaks in favour of binding procedural rules from the perspective of the rule of law. He points out that the outcome is not legitimate without a fair process. His core message is that the process matters.⁴⁵ He positions his proposal around the idea that the private power of technology companies needs to be 'constitutionalised' to 'impose limits on how rules are made and enforced'. In his view, '[c]onstitutionalism is the difference between lawlessness and a system of rules that are fairly, equally, and predictably applied'.⁴⁶

To agree with Suzor's view, one does not also need to accept his or other digital constitutionalists' framework.⁴⁷ If the word regulation is substituted for the constitution, Suzor makes a perfectly understandable case for industry regulation that can be understood as consumer or business fairness regulation. While dressing due process rights as

⁴³ 'Santa Clara Principles on Transparency and Accountability in Content Moderation' (*Santa Clara Principles*) <<https://santaclaraprinciples.org>> accessed 3 September 2023.

⁴⁴ Suzor (n 10) 8.

⁴⁵ *ibid.*

⁴⁶ *ibid.* 9.

⁴⁷ The two leading proponents of digital constitutionalism are Suzor (n 10); Giovanni De Gregorio, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society* (CUP 2022). This approach has been criticised by Róisín Á Costello, 'Faux Ami? Interrogating the Normative Coherence of "Digital Constitutionalism"' (2023) 12(2) *Global Constitutionalism* 326 (arguing that while the goals might be noble, however, digital constitutionalism is not constitutionalism at all); Leonid Sirota, 'A Constitution without Constitutionalism: Re-thinking the "Digital Constitutionalism" Debate' (*Verfassungsblog*, 3 July 2023) <<https://verfassungsblog.de/a-constitution-without-constitutionalism/>> accessed 3 September 2023.

constitutional rights gives them more heft, the truth remains that liberal democracies must convince legislatures to adopt them. Unlike due process rights against the state, these rights are not directly guaranteed by any constitution known to me, even though the underlying idea of procedural fairness might be related.

The DSA's framework of due process rights has three component obligations: to disclose rules, to explain decisions and processes, and to justify decisions. Providers must disclose their rules upfront without hiding them from those bound by them (Article 14(1)). Providers can make rules on the go but cannot apply them retroactively. Once they apply the existing rules, they must explain why they adopt some content moderation decisions (Article 17). Finally, the companies must be open to revisiting the adopted decisions following an internal or external appeal and be able to justify them (Articles 20–21). In addition, they must report publicly on how they handle the decision-making. If companies build their internal decision systems to comply with the above due process rights envisaged by the DSA, they can mostly export the statistics from such systems (Article 15). These obligations will be discussed in detail in the next few chapters. However, before I delve into the details, I consider it important to explain the high-level aspirations and criticisms of the regulatory approach.

Most recognise that solutions to various challenges of content moderation cannot come from one intervention but require 'systemic thinking'.⁴⁸ However, what exactly that thinking entails is not always clear. Most likely, the clearest meaning is that content moderation should not be left entirely to firefighting once the fire is already raging but should also involve preventive risk management. Content moderation could be thus described as a combination of *ex ante* and *ex post* measures employed by companies. The typical *ex post* measures are the actions against individual users or their expressions, whether based on the content or their behaviour. The typical *ex ante* measures are the redesign of the product to curb the abuse. The DSA regulates many *ex post* measures by prescriptive procedural rules, while *ex ante* is left regulated by rather general risk management rules.

The following two chapters are devoted to *ex post* measures. In the literature, many forms of criticism have been levelled against *ex post* measures, sometimes, I would argue, unfairly so. The criticism of these rights could be clustered as follows:

- they are useful but should not be binding;
- they cannot possibly solve content moderation problems;
- they only further privatise justice; and
- they are going to be too costly and will stifle competition and innovation.

⁴⁸ This term was recently used by Evelyn Douek, Douek, 'Content Moderation as Systems Thinking' (n 6). However, it has also attracted criticism for describing something likely commonplace in the literature, Kate Klonick, 'Of Systems Thinking and Straw Men' (2023) 136(6) *Harvard Law Review* 339.

10.5.1 Why binding rules?

The first criticism makes the point that non-binding due process rights are less likely to be abused by various groups through litigation or state authorities.⁴⁹ While that might be true, they are also less likely to be observed by providers who also wish to abuse their users. Any such debate is about how much trust one has in the institutions and the likely market dynamics among providers. The unique mix of both depends on each jurisdiction. If the trust in institutions is low or should be low, and the market is robust, then non-binding rules are preferable. However, if the country has healthy institutions, such as authorities, courts, or civil society, they can filter and deter abuse. Structurally, there is no reason why due process rights arguably should be any more dangerous than any other rights of individuals, such as the right to data protection.

The DSA's design creates separately enforceable due diligence obligations (Chapter 9.4). This feature reduces stakes by ensuring that the observance of such rights is not a life-or-death question for companies. A failure to adopt a user-friendly notification process or issue explanations to users can earn company fines or lawsuits, but the system explicitly prohibits any eye-watering statutory damages.⁵⁰ With litigation cost-sharing and proportionality as the ultimate rule for any public fines, there is no obvious reason why obligations should be abused more than any legal instrument can always be.

10.5.2 Can procedural rights help?

The second criticism concerns whether such legislation is not only handwaving that leads to 'procedural theatre'⁵¹ or 'procedural fetish'⁵² with little practical impact. Often, it is argued that appeal rates are so low today that we should not rely on individuals to correct mistakes.

It is true that we should not rely *only* on individuals, but we must *also* rely on individuals. The low rates of appeals need to be viewed against the institutional set up that users today face. No remedy, apart from courts, that they had is credible. Why is it such a surprise then that they do not use them? If the remedial set up changes, thanks to external appeals and individual rights, and people internalise these rules, their behaviour can change, too. As I have argued elsewhere, there are many ways in which people's willingness to complain in the right cases can be incentivised.⁵³ We also need to rely

⁴⁹ Eric Goldman, 'How Will the Digital Services Act (DSA) Affect the European Internet?' (*Technology & Marketing Law Blog*, 12 July 2023) <<https://blog.ericgoldman.org/archives/2023/07/how-will-the-digital-services-act-dsa-affect-the-european-internet.htm>> accessed 3 September 2023.

⁵⁰ Art 54 prescribes compensation and thereby also pre-empts punitive damages: see ch 19.

⁵¹ Douek, 'Content Moderation as Systems Thinking' (n 6) 578.

⁵² *ibid.* Most prominently, this point is made by Douek. To support this view, she cites Nicholas Bagley, 'The Procedure Fetish' (2019) 118(3) *Michigan Law Review* 345.

⁵³ Lenka Fiala and Martin Husovec, 'Using Experimental Evidence to Improve Delegated Enforcement' (2022) 71 *International Review of Law and Economics* 106079.

on individuals because if the challenge to the top-down content moderation model is meant to rely on user empowerment, only the users can be in the driving seat of the change. Giving individuals rights against private power is the starting point.

The DSA leans heavily on individuals. If they do not use the tools, little will change in their positions⁵⁴ unless they are affected by ex ante risk mitigation interventions. While some might see this as a bug, I personally see this as a feature. The DSA invites civil society to assist individuals in their dispute resolution. They can represent them before providers, in external appeals, or even seek injunctions on their behalf.⁵⁵ Thus, numerous credible remedies are created. With different incentives, the behaviour of individuals is also likely to change. They might become less deferential to the providers and more conscious and assertive of their rights. While it is true that some problems, such as unequal distribution of errors,⁵⁶ cannot be resolved by simple ex post redress, as it relies on the ability of the affected individuals to defend themselves with a combination of collective structures (see Chapter 19), and ex ante risk management (Chapter 15), procedural rights can still be useful.

A rejection of procedural rights, or private rights more generally, means that we are putting all our faith in the public regulators and giving no agency again to individuals. This is wrong. If companies can rely on imperfect technologies to enforce the law or their contractual clauses, individuals must be given a way to correct them. Making them dependent on the priorities of authorities is problematic. This is why the DSA's mixed enforcement model (Chapter 20), in my view, is essential. Senders and receivers of information cannot become the eternal hostages of imperfect technologies that will continue to govern communication until the providers decide to change them. Individual rights should feed into the calibration of such tools and help to improve them. Even if they are only a *part* of the solution, they have a place.

10.5.3 Why privatising justice?

The third criticism⁵⁷ is about how giving procedural rights to private parties, especially allowing them to appeal to private dispute resolution bodies, will lead to fewer disputes being resolved by courts. The assumption is that only courts know how to resolve

⁵⁴ Martin Husovec, 'Will the DSA work?: On Money and Effort' (*Verfassungsblog*, 9 November 2022) <<https://verfassungsblog.de/dsa-money-effort/>> accessed 3 September 2023.

⁵⁵ DSA, arts 21, 86, and 90.

⁵⁶ Evelyn Douek, 'Governing Online Speech: From "Posts-As-Trumps" to Proportionality And Probability' (2021) 121(3) *Columbia Law Review* 759.

⁵⁷ Daniel Holznapel, 'The Digital Services Act Wants You to "Sue" Facebook over Content Decisions in Private de Facto Courts' [2021] *Verfassungsblog* <<https://verfassungsblog.de/dsa-art-21/>> accessed 3 September 2023 ('Member States' courts should already possess some of the necessary characteristics for dispute settlement in our context—expertise, impartiality, fair rules of procedure, and the capacity to deliver binding decisions. What may be lacking is speediness and cost-effectiveness. Reform efforts should focus on solving these specific weaknesses, which is less difficult than inventing and implementing a whole new layer of de facto courts from scratch'); Jörg Wimmers, 'The Out-of-Court Dispute Settlement Mechanism in the Digital Services Act' (2021) 12(4) *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 421 ('free speech disputes are strictly normative and do not lend themselves to a settlement by private bodies, but are reserved for the judiciary').

disputes, and reducing their agenda is harmful to society at large. The typical concerns are about the fairness of such procedures, their standard-setting nature, or their legitimacy. For some civil society groups, avoiding courts signals that human rights standards will not be respected similarly. The concern is that providers, or specialised dispute settlement bodies, will not be impartial enough.

While I understand that some disputes are so consequential that they should be channelled through courts, it should be stated that the DSA does not limit the jurisdiction of courts. Any party to the dispute can still go to the courts. Some scholars and judges⁵⁸ tend to promote judiciary as the only legitimate way to resolve disputes and tend to criticise the privatisation of dispute resolution. However, not all countries have a perfect judiciary. Many judiciaries are slow, less trained in novel issues, or simply expensive. Moreover, the degree of litigiousness differs across countries, and in some, there are serious mental barriers for people to resort to the courts.

If the judicial system is still available—which is the case under the DSA—I fail to see the problem when the law offers a new route to help resolve disputes. If private parties can resolve their differences without state intervention, we should embrace that. For one, society does not have to subsidise such dispute resolution through taxes. The public's finances can be spared from all the grievances that individuals have with platforms. Instead, only providers and users pay for their mutual disputes. The same principles underlie consumer or aviation compensation disputes (Chapter 11), and no one seems to be panicking about the 'disappearance of courts'.

10.5.4 What about costs of compliance?

Finally, the fourth argument concerns the cost of compliance and its impact on competition and innovation.⁵⁹ This criticism relates to the first. What if compliance with procedural rights is so costly that it can only be done by bigger players? Isn't the law inviting more than only market concentration? Isn't the DSA going too far in this respect? This criticism is legitimate, as increased regulation can lead to market concentration.⁶⁰ Incumbents can and do lobby for increased regulation to stop new entrants or at least slow them down.

However, one does not need to study market developments for too long to see that market concentration is already taking place in the absence of regulation. While it results from many factors unrelated to content moderation, email client concentration provides a unique example. Unlike social media, the email client market is less affected

⁵⁸ Holznapel (n 57); Wimmers (n 57).

⁵⁹ Goldman (n 49); Douek, 'Content Moderation as Systems Thinking' (n 6) 583 ('mandating a particular kind of process in every case will freeze the current equilibrium in place, ... disincentivise innovation, and create barriers to entry given the most well-resourced platforms will find it easiest to comply with such mandates').

⁶⁰ Oscar Guinea and Fredrik Erixon, 'Market Concentration, Regulation, and Europe's Quest for a New Industrial Policy' (*ProMarket*, 7 May 2019) <<https://www.promarket.org/2019/05/07/market-concentration-regulation-and-europes-quest-for-a-new-industrial-policy/>> accessed 3 September 2023.

by typical ‘digital tipping effects,’ such as direct network effects⁶¹ or data-driven competitive advantages.⁶² If anything, indirect network effects are created more by content moderation practices. Nevertheless, the email client market still results in a duopoly of companies controlling the absolute majority of the market. To add insult to injury, email protocol is heavily based on open standards. While one case is hardly conclusive, at least it allows us to study to what extent the cost of content moderation contributes to market concentration because it erects a high barrier to entry.

If the cost is significant, then the question is whether the DSA is not only adding fuel to the fire by increasing such costs for new entrants but potentially helping reduce the fire. This is ultimately an empirical question. The DSA has two countervailing effects: first, the new regulatory requirements initially increase the regulatory costs of operating content moderation and thus market entry; second, the regulation can facilitate more standardisation and market entry in content moderation solutions. If a bigger industry needs cheap and scalable solutions that comply with certain standardised legal metrics, it can be expected that other companies jump on the opportunity and start offering them. The industry’s steps in this direction are already visible. Cloudflare is offering a tool to catch child-sexual-abuse material as part of its Content Delivery Network services.⁶³ Amazon’s Amazon Web Services (AWS) is offering various content moderation systems for hosted services.⁶⁴

Arguably, the DSA softens the regulatory costs through its tiered approach, where bigger players attract more responsibility to give effect to the procedural rights of individuals. The main obligations apply to companies with at least 50 employees and a €10 million turnover. Only providers with over 45 million monthly active users in the EU are subject to a more elaborate ex ante risk management system requiring more in-house adjusting and customisation. One might argue about these thresholds as being low or high. However, while doing so, we should not forget that the DSA also helps companies do business across the border by lowering their cost of compliance with different rules. Thus, as explained below, there are potential substantial savings from harmonisation per se.

The online platform tier effectively limits the more expensive compliance to fewer companies because of the company size. Undoubtedly, in this tier, there could be companies that are merely local and thus cannot immediately reap the cross-border benefits. However, even such companies benefit whenever they seek expansion to the other EU markets. For the big tech, the threshold corresponds to roughly 10% of the EU population. Only a handful of single-language services can cross this threshold—namely,

⁶¹ Matthew T Clements, ‘Direct and Indirect Network Effects: Are They Equivalent?’ (2004) 22(5) *International Journal of Industrial Organization* 633.

⁶² Jens Prufer and Christoph Schottmüller, ‘Competing with Big Data’ [2017] TILEC Discussion Paper No 2017-006, CentER Discussion Paper 2017-007 <<https://papers.ssrn.com/abstract=2918726>> accessed 3 September 2023.

⁶³ Justin Paine and John Graham-Cumming, ‘Announcing the CSAM Scanning Tool, Free for All Cloudflare Customers’ (*The Cloudflare Blog*, 18 December 2019) <<http://blog.cloudflare.com/the-csam-scanning-tool/>> accessed 3 September 2023.

⁶⁴ Amazon Web Services, ‘Content Moderation | Machine Learning’ (*Amazon Web Services, Inc.*) <<https://aws.amazon.com/machine-learning/ml-use-cases/content-moderation/>> accessed 3 September 2023.

those offered in German, French, and Italian, and counting second language speakers, English, Spanish, and Polish.⁶⁵ Complying with the VLOP/VLOSE rules effectively means doing business across the border.

It is underappreciated that the DSA creates huge benefits for non-EU companies that provide businesses in the EU. Any provider not established in the EU is *not* shielded by the country-of-origin principle.⁶⁶ This meant that such companies pre-DSA might have dealt with hundreds of authorities from 27 countries speaking 24 different languages. Under the ECD, there was no system where a company would simply choose a legal representative to reduce that number to one, as it is now under Article 13 DSA for rules *harmonised by the DSA*.⁶⁷ According to ECD, foreign companies had to be ‘established’ in the EU to benefit from the country-of-origin principle. This involves ‘the actual pursuit of an economic activity through a fixed establishment for an indefinite period’ (Recital 19 ECD). The DSA thus offers non-EU companies a simple way to comply with one set of rules, and if they move their establishment later, those rules will remain the same because they are harmonised.

Therefore, to answer the original empirical question of whether the DSA compliance costs harm competition, one needs to look at the countervailing effects: the beneficial effects caused by standardisation and improved cross-border entry and the potential negative effects of lower entry caused by such regulation. The proposition that more rules only equal higher costs and less competition is far from immediately true for the above reasons.

Furthermore, deregulation is not necessarily socially cheaper. Content moderation of *illegal content* regulation has true distributive costs. If a platform is asked to moderate illegal content, its failure to do so means more work for users of such digital spaces (eg administrators of pages on social media dealing with illegal hate speech). A provider’s underinvestment raises costs for its users. A newspaper, as a content creator, needs to invest in people and technology to detect and moderate such content at speed and scale. A failure of platforms to moderate illegal content clearly creates externalities for its users. Regulating such underinvestment thus does not mean creating costs out of thin air but reallocates costs to the platforms asked to internalise the externalities of their design. Since users cannot change the design of the platforms (eg what content is incentivised), having them bear the high cost of externalities seems questionable. If we accept that the regulation of digital services should respect the principle of shared burden for societal costs (Chapter 21), each side should shoulder part of the burden.

I hasten to add that the situation is different, however, for content moderation of *legal content*—information or behaviour that is not prohibited by parliaments. There, the platforms and their users can have different views of what they want to see. If users

⁶⁵ TNS Opinion & Social, ‘Europeans and Their Languages’ (European Commission 2012) Special Eurobarometer 386 <https://web.archive.org/web/20160106183351/http://ec.europa.eu/public_opinion/archives/ebs/ebs_386_en.pdf> accessed 3 September 2023.

⁶⁶ This remains the same under the DSA, as emphasised by art 13(5) DSA.

⁶⁷ For the rules that the DSA does not harmonise, the pre-DSA situation applies—ie any national regulator can expect its rules to be enforced against such companies and potentially has jurisdiction.

fail to convince providers to change their content standards, they can still lobby for tools that allow them to enforce different standards in their own digital spaces. Thus, a Christian newspaper using social media can decide to restrict all content that is not aligned with its values or worldview. They can use external tools to do so at the required speed or scale. While such preferences on the individual level can be justified, they have serious consequences if rolled out for entire services. If individuals are unhappy with the lax default existing standards of content that are lawful, they can direct their attention to parliaments or competitors. Parliaments not only have the highest legitimacy to change what is prohibited, but they are also properly accountable to the public for their rulemaking in a public process, which is ultimately overseen by courts as the ultimate guardians.

Fair Moderation Process

11.1 The DSA's Approach to Content Moderation	202	11.4 Step 3: Internal Appeals (Article 20)	229
11.1.1 Scope of the procedural rules	203	11.4.1 Appeal scenarios	230
11.1.2 Design of interfaces	205	11.4.2 Scope and outcomes	233
11.1.3 Trusted flaggers	206	11.5 Step 4: External Appeals (Article 21)	234
11.2 Step 1: Notice Handling (Article 16)	209	11.5.1 Who can file an external appeal and when?	236
11.2.1 The mechanism	211	11.5.2 What decisions are subject to ODS appeals?	237
11.2.2 The 'notice'	212	11.5.3 Who counts as an ODS expert?	238
11.2.3 What is illegal content?	215	11.5.4 What content rules apply in the ODS procedure?	239
11.2.4 The 'action'	216	11.5.5 Is the ODS procedure binding?	240
11.2.5 Relationship with liability exemptions	218	11.5.6 What qualifies as an ODS body?	242
11.3 Step 2: Statement of Reasons (Article 17)	221	11.5.7 Who pays for ODS?	243
11.3.1 Scope of individual explanations	222	11.5.8 What is a fair ODS procedure?	246
11.3.2 Exceptions	224	11.5.9 What can an ODS body decide?	247
11.3.3 Who is owed what explanations?	225	11.5.10 What if an ODS body becomes a rogue?	247
11.3.4 Disclosure of the identity of the notifier	226	11.6 Conclusion	248
11.3.5 Notification of suspected crimes (Article 18)	227		

11.1 The DSA's Approach to Content Moderation

The Digital Services Act (DSA) foresees numerous procedural requirements to put pressure on the quality of content moderation decisions and allow due redress to *all* parties involved—not just users acting as content creators. The DSA prepares elaborate incentives for notifiers, providers, and affected third parties. It also introduces a series of incentives based on trust that can be earned and lost: for instance, notifiers with a track record of accurate notifications shall enjoy priority in the assessment; providers who fail to make the right decisions can face external complaints that they must reimburse. In my view, this incentive approach is well-suited to what has become an industry of its own, with large external suppliers of know-how and human expertise.¹

As a result, the DSA can be said to fuse some principles from constitutional and administrative law,² but its approach to content moderation is still a form of market

¹ Adam Satariano and Mike Isaac, 'The Silent Partner Cleaning Up Facebook for \$500 Million a Year Accenture' *The New York Times* (New York, 31 August 2021) <<https://www.nytimes.com/2021/08/31/technology/facebook-accenture-content-moderation.html>> accessed 29 August 2023.

² Nicolas P Suzor, *Lawless: The Secret Rules That Govern Our Digital Lives* (CUP 2019) 8.

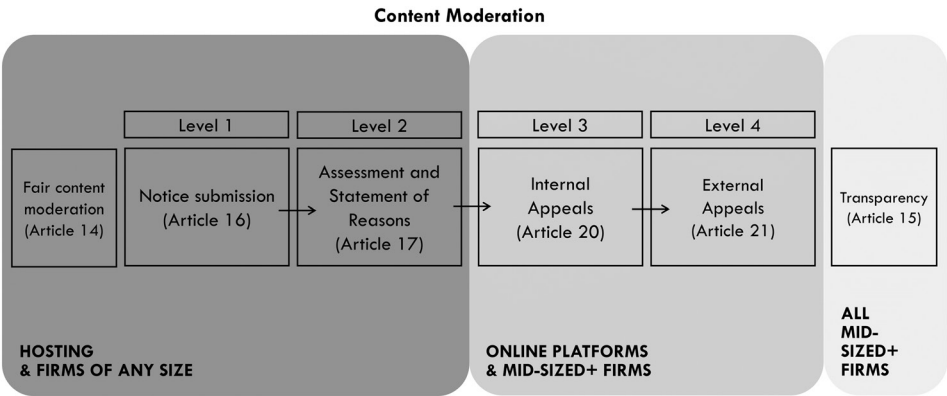


Figure 11.1 Content moderation rules

regulation. The DSA is probably better described as due process regulation for companies that includes a set of macro incentives for the ecosystem of content moderation. Such process fairness rules complement transparency and more limited substantive fairness rules that I discuss in the next chapter (Chapter 12). Only providers with a systemic role in the European Union’s (EU’s) digital ecosystem face more extensive fair design obligations which ask them to test, redesign, and improve their content moderation systems along with other parts of the design of their services.

11.1.1 Scope of the procedural rules

Not all providers of the digital ecosystem are regulated by the DSA equally. Due diligence obligations under the DSA follow an asymmetric logic that intends to tackle the more pertinent problems of content moderation where those arise without unnecessarily imposing red tape on services that are more removed from the relevant content, smaller, or have less impact on society. Figure 11.1 depicts the basic layering logic for content moderation rules.

Mere conduit- and caching-types of services, such as internet access providers, some messaging apps,³ or content delivery networks, are not obliged to moderate content. That being said, the DSA recognises that while many of these services traditionally did not moderate content, the trend is changing.⁴ If caching services decide to engage in content moderation, their decisions must be transparent and conform to some elementary requirements of fairness. Thus, for instance, if a content delivery network uses

³ See ch 6 of this book.
⁴ eg see Cloudflare, a global cloud platform, blocking Kiwifarms: Matthew Prince, ‘Blocking Kiwifarms’ (*The Cloudflare Blog*, 3 September 2022) <<http://blog.cloudflare.com/kiwifarms-blocked/>> accessed 3 September 2023.

child abuse scanning technology on its clients,⁵ such use will fall under Article 14 as it constitutes a content moderation practice. However, even though it can result in restriction of accounts, such practice will not be subject to explicit due process obligations, such as justifying decisions and reviewing appeals. The same applies to mere conduit services, but with the caveat that content moderation practices by some providers might be prohibited under net neutrality laws.⁶ For instance, an internet access provider is not allowed to block infringing websites without proper legal basis.⁷

Hosting-type services are subject to much more elaborate rules. They are expected to moderate illegal content because they could otherwise lose their liability exemption. However, due diligence obligations are independent of the question of liability of providers of intermediary services: providers could comply with all the DSA procedures and still expose themselves to liability for third-party content.⁸ Similarly, providers who already lost a liability exemption, are still required to comply with the DSA content moderation procedures. Thus, the availability of liability exemptions and compliance with the DSA rules on due diligence are entirely separate (Chapter 9).

Among hosting-type providers, online platforms are subject to most of the obligations. This reflects the magnitude of the problems posed by online platforms today, where such platforms constitute the main source of friction in their position as ‘public-facing’ providers. Finally, very large online platforms (VLOPs) have special obligations in content moderation, given their importance and reach ‘in facilitating public debate, economic transactions and the dissemination to the public of the information, opinions and ideas and in influencing how recipients obtain and communicate information online.’⁹

The DSA defines content moderation as follows:

the activities, whether automated or not, undertaken by providers of intermediary services aimed, in particular, at detecting, identifying and addressing illegal content or information incompatible with their terms and conditions, provided by recipients of the service, including measures taken that affect the availability, visibility, and accessibility of that illegal content or that information, such as demotion, demonetisation, disabling of access to, or removal thereof, or the recipients’ ability to provide that information, such as the termination or suspension of a recipient’s account¹⁰

Thus, the DSA’s definition of content moderation is very broad, covering any ‘activity’ by providers that ‘addresses’ the compliance of users’ content with rules introduced by

⁵ See the CSAM Scanning Tool: Justin Paine and John Graham-Cumming, ‘Announcing the CSAM Scanning Tool, Free for All Cloudflare Customers’ (*The Cloudflare Blog*, 18 December 2019) <<http://blog.cloudflare.com/the-csam-scanning-tool/>> accessed 3 September 2023.

⁶ See the Open Internet Regulation, although it does not apply to WiFi operators as mere conduits: European Parliament and Council Regulation (EU) 2015/2120 laying down measures concerning open internet access [2015] OJ L310/1 (Open Internet Regulation).

⁷ *ibid*, art 3(3)(a).

⁸ DSA, Rec 41.

⁹ DSA, Rec 75.

¹⁰ DSA, art 3(t).

parliaments or platforms themselves.¹¹ The term 'content', whether illegal or against terms and conditions, is also only a shorthand for users' content or their behaviour.¹² This effectively means that any activity can be viewed as content moderation if it addresses user-generated content. However, this legal definition is *not* used by the DSA to trigger due process rights. It mostly serves to delimit transparency obligations. Only a subset of content moderation activities trigger further process fairness obligations. The procedural rights are only owed for decisions exhaustively listed in Article 17(1). Still, some could argue, and I would agree to a limited extent, that the DSA should graduate the strength of procedural rights based on the severity of the intervention's impact, eg highly structured dispute resolution processes for account terminations or monetisation disputes, and lesser procedural protections for the mere labelling of sensitive content.¹³

11.1.2 Design of interfaces

The DSA regulates *procedural steps* for notification of illegal content and the *principles* for the design of communication interfaces, giving effect to those rights. Consider Article 16(1):

Those mechanisms shall be easy to access and user-friendly, and shall allow for the submission of notices exclusively by electronic means.

The DSA thus places an explicit requirement on all hosting providers to ensure widespread accessibility of their notification interfaces. The providers cannot hide them or make them cumbersome to use. If they impose restrictions, they must be able to justify why they have created additional friction and imposed a burden on notifiers and why other measures to achieve the same purpose cannot be implemented. Article 16(1) thus explicitly challenges the designs of notice submission systems that hide behind security or privacy to avoid obtaining large numbers of notices about illegal content by notifiers. In the past, some providers would undertake various measures to avoid receiving notices (eg by putting caps on them from specific IP addresses or accounts), or make their submission costly to limit their content moderation workload. These practices are explicitly prohibited. Any security measures must be justified because the notification mechanisms must be as user-friendly and accessible as possible.¹⁴

¹¹ DSA, art 3(t).

¹² See art 3(h) of the DSA, where it defines 'illegal content' as '*information that, in itself or in relation to an activity ... is not in compliance with [law]*' (emphasis mine). Compare this to art 3(t), where in the context of describing content that violates a provider's terms and conditions and is thus subject to content moderation, the DSA refers to such content merely as '*information incompatible with terms and conditions*' (emphasis mine). While the extension of the definition to include even 'information in relation to an activity' is not expressly replicated in art 3(t)'s description of content, the same extended scope should be adopted, given that the intention was clearly to cover the enforcement of both content and behaviour restrictions on the relevant services.

¹³ See Evelyn Douek, 'Content Moderation as Systems Thinking' (2022) 136(2) Harvard Law Review 526, 582.

¹⁴ Obviously, this does not mean that targeted measures cannot be taken against abusers of the notice submission systems. On the contrary, as explained in ch 12 when discussing art 23, the DSA sometimes even mandates actions against abusers.

While the binding principle of user-friendly design is not explicitly mentioned in the context of the statement of reasons (Article 17), in my view, it applies to the entire process of notice and action. The principle is reiterated for how the information about redress is communicated (Article 17(3)(f)), and even the statement of reasons must be ‘be clear and easily comprehensible’ (Article 17(4)). Finally, this also follows from Articles 12(1) and 14(1), and finally, Article 44(1)(b), which in the context of standardisation speaks of ‘templates, design and process standards for communicating with the recipients of the service in a user-friendly manner on restrictions resulting from terms and conditions and changes thereto.’ Thus, the principle of user-friendly design is a binding obligation underlying the entire notice and action system.¹⁵

The DSA explicitly provides that the means of notification must be exclusively ‘electronic’.¹⁶ Thus, a practice where providers ask for letters to be sent by post is clearly not allowed. After consulting the Board, the European Commission is tasked to support and promote the development of voluntary standards for the electronic submission of notices for all notifiers (Article 44(1)(a)). Trusted flaggers, unlike other notifiers, can gain access to more advanced programming interfaces to submit their notices, which can be standardised again (Article 44(1)(c)).

The standardisation coupled with ease of submission is hoped to create a system where notifications flow between various entities through interoperable systems (eg NGOs easily generate notifications for a range of services without high administrative costs). In combination with incentives for quality of notices (eg trusted flaggers) and content moderation redress options that the DSA creates (eg out-of-court dispute settlement and complaint processes), the hope is that while providers cannot reduce their workload, they can insist on quality. If the quality of the input level improves, that should translate to the quality of the output level, ie content moderation decisions. The design principles behind notice and action systems are thus important building blocks for setting up good incentives for all the players involved in content moderation.¹⁷

11.1.3 Trusted flaggers

While the DSA focuses firmly on providers, their actions can sometimes be only as good as the environment to which they are responding to. Thus, the DSA provides some rules for other actors who are relevant in content moderation, such as trusted flaggers and other notifiers.

¹⁵ While art 16 only applies to the processing of notifications regarding illegal content, arts 12 (contact point) and 14 (fair design of content moderation) apply universally, regardless of the basis for the provider’s actions. They, therefore, suggest that the principle is binding to both.

¹⁶ DSA, art 16.

¹⁷ For more on this, Lenka Fiala and Martin Husovec, ‘Using Experimental Evidence to Improve Delegated Enforcement’ (2022) 71 *International Review of Law and Economics* 106079; also Alexandre de Streel and Martin Husovec, ‘The E-Commerce Directive as the Cornerstone of the Internal Market – Assessment and Options for Reform’ (Study Requested by IMCO committee, PE 648797, European Parliament 2020) 35 <[https://www.europa.eu/regdata/etudes/STUD/2020/648797/IPOL_STU\(2020\)648797_EN.pdf](https://www.europa.eu/regdata/etudes/STUD/2020/648797/IPOL_STU(2020)648797_EN.pdf)> accessed 1 August 2023.

The role of trusted private actors has been long foreseen. Already the Communication on illegal content (2017)¹⁸ and the Recommendation on illegal content (2018),¹⁹ made it clear that independent 'third-party' experts could play a key role in addressing the challenge of tackling illegal online content. These documents encouraged online platforms to work closely with 'trusted flaggers'.²⁰ However, they were also thin on procedural safeguards and allocating roles and responsibilities.

By introducing the notion of trusted flaggers into regulation, the DSA tries to remedy in a roundabout way one of the original sins of the pre-DSA legal framework—ie its inability to distinguish between actors who notified with due care and those who were reckless while doing so. Prior to the DSA, everyone's notifications were treated equally by law, resulting in an incentive for notifiers to increase volume rather than quality. The DSA aims to change this. Partly building upon industry convention,²¹ but also on the literature,²² this new regime shows how badly the original system structured its incentives.

To improve the situation, the DSA creates a new tier of notifiers—the so-called 'trusted flaggers'. The underlying logic is that repeated actors whose work is known for its quality can be trusted more and given privileges in content moderation procedures, such as priority of review. Such privileges then act as an incentive for other frequent actors to improve their quality of notification to attain such status. The more trusted flaggers the ecosystem has (provided that there is sufficient quality control in getting the status),²³ the fewer mistakes the providers make and the fewer complaints necessary to correct their mistakes. In the end, not only victims but also content creators and their audiences benefit.

The Member States should encourage civil societies throughout the EU to create enough skilled and well-resourced trusted flaggers locally. Unlike other parts of the DSA, the task here lies heavily with the local civil societies, as German organisations are unlikely to police hate speech in Slovak or Danish. This societal infrastructure, which the DSA only incentivises and envisions, needs to be built in each Member State

¹⁸ Commission, 'Tackling Illegal Content Online: Towards an Enhanced Responsibility of Online Platforms' (Communication) COM(2017) 555 final.

¹⁹ Commission Recommendation (EU) 2018/334 on measures to effectively tackle illegal content online [2018] OJ L63/50.

²⁰ It is a common practice by the best-known online platforms to create a privileged reporting channel for users or organisations that are particularly active in reporting violations with an extraordinarily high accuracy rate. These programmes vary from commercial users (rights holders, usually both for copyright and trademarks) to public policy objectives, such as hotlines or market surveillance authorities. Encouragements of such practices were already reflected in several codes of conduct, European Commission, 'The EU Code of Conduct on Countering Illegal Hate Speech Online' <https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combating-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en> accessed 6 September 2023; European Commission, 'Memorandum of Understanding on the Sale of Counterfeit Goods on the Internet' <https://single-market-economy.ec.europa.eu/industry/strategy/intellectual-property/enforcement-intellectual-property-rights/memorandum-understanding-sale-counterfeit-goods-internet_en> accessed 6 September 2023.

²¹ Naomi Appelman and Paddy Leerssen, 'On "Trusted" Flaggers' [2022] Yale-Wikimedia Initiative on Intermediaries & Information <https://law.yale.edu/sites/default/files/area/center/isp/documents/trustedflaggers_ispessayseries_2022.pdf> accessed 29 August 2023.

²² Fiala and Husovec (n 17).

²³ However, Rec 61 DSA establishes that '[t]o avoid diminishing the added value of such mechanism, the overall number of trusted flaggers awarded in accordance with this Regulation should be limited'.

for each area of content moderation. The situation is thus similar to the case of out-of-court dispute settlement bodies, which often have to originate from the same Member State where the issue they help to resolve arises.

Trusted flaggers are entities awarded special status by national Digital Service Coordinators (DSCs). Their notifications must be ‘given priority and are processed and decided upon without undue delay’ (Article 22(1)). However, Recital 61 emphasises that this only applies when ‘acting within their designated area of expertise’.

It is expected that Article 22’s reference to ‘necessary technical and organisational measures’ will lead to standardisation in the area of interfaces through which trusted flaggers can submit their notification in bulk and automatically from their internal systems.²⁴ While Article 22 only applies to illegal content, nothing stops providers from relying on the existing certifications in the context of terms of service violations or awarding other flaggers the same status as other entities that do not meet the criteria under Article 22.

The status is awarded only to entities with expertise and competence in a specific area of content moderation, are independent of providers, and have a track record of carrying out their activities ‘diligently, accurately and objectively’ (Article 22(2)). Trusted flaggers must publish annual reports concerning notifications they have submitted with numbers according to the identity of providers, type of illegal content, and actions taken by the respective providers. The database of trusted flaggers is maintained by the European Commission (Article 22(5)).

While under the Commission proposal, individual entities (such as rightsholders) could not be awarded this status, the final text allows any entity to become a trusted flagger even if it does not represent collective interests. Since trusted flaggers must be entities independent of any platform, the reports must explain the procedures in place to ensure their independence. It is unclear why Article 22(3) limits independence to the providers of platforms and does not include other stakeholders (Article 22(2)). The DSA’s goal is generally to make sure that the trusted flagger represents the collective interests of some stakeholders, which is why Recital 61 encourages ‘industry associations representing their members’ interests’ to apply for the status of trusted flaggers ‘without prejudice to the right of private entities or individuals to enter into bilateral agreements with the providers of online platforms’. The same recital also clarifies that even authorities, such as enforcement authorities, Europol, or semi-public bodies, can equally gain the status.

Entities awarded the status of trusted flagger can be stripped of that status by the same DSCs. The responsible DSC can act upon complaints by the affected platforms, or on its own initiative. Following an investigation, during which the entity is confronted with the allegations, the DSCs can decide to revoke the awarded status. If the procedure was initiated due to a complaint from a provider, the status can also be suspended during the revocation procedure (Article 22(6)). The typical reason for revocation is

²⁴ Art 44 of the DSA also includes a call for developing voluntary standards for the ‘electronic submission of notices by trusted flaggers under Article 22, including through application programming interfaces’.

a violation of the elements of trust: objectivity, diligence, and accuracy of notifications or internal appeals. Trusted flaggers are in a special position here. Their trusted status can be suspended with much lower thresholds of mistakes, given that they should be known for diligent, objective, and accurate notifications or complaints. Finally, the European Commission is empowered to issue guidance further detailing the conditions for the award, revocation, and suspension of trusted flagger status in case, over time, there is divergence in the interpretation by the different DSCs (Article 22(8)).

11.2 Step 1: Notice Handling (Article 16)

Regulating content moderation starts with anticipating how providers receive external notices. The procedure dealing with notifications is now closely regulated under the DSA.

It was evident from its Impact Assessment that, for the European Commission, a basic obligation to put in place ‘notice and action’ mechanisms was essential to improve the status quo for several reasons: to harmonise a very fragmented legal framework, to transform into the binding form the rules included in the 2018 Recommendation,²⁵ and to ensure that users could easily flag manifestly illegal content. The Commission was clearly conscious of the compliance costs of such an obligation. It is expected that ‘the introduction of the standard, minimum requirements for notices, procedures, and conditions, as well as reporting templates, should further decrease the expected costs for small companies, supporting them in tackling illegal content and increasing, in turn, the legal certainty.’²⁶

To be clear, the DSA does *not* regulate notice-receiving mechanisms for hosting service providers seeking to find violations of *terms and conditions*. Article 16 applies only to notification of illegal content. The reason for this is simple. The DSA makes a conscious choice not to legitimise and incentivise public enforcement of private rules, ie the removal of content contractually restricted by the providers despite its lawful nature (eg nudity). This policy choice aligns with the rest of the DSA, which intends to keep separate channels for public enforcement of ‘public rules’, such as orders by authorities or notifications by others, and private enforcement of ‘private rules’. In the latter case, the DSA nevertheless aims at least to correct the negative impact such private enforcement can have on users by subjecting them to the same process.

As explained above, *mere conduit* and *caching* services are not the traditional players in content moderation. Hence, Article 16 (and Article 17)²⁷ does not apply to them. This is also due to the fact that under the liability exemptions protecting such

²⁵ Commission Recommendation (EU) 2018/334 on measures to effectively tackle illegal content online [2018] OJ L63/50.

²⁶ Commission, “Impact Assessment” (Commission Staff Working Document) Accompanying the Document “Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (DSA) and Amending Directive 2000/31/EC” SWD(2020) 348 final, para 200.

²⁷ Discussed fully below in section 11.3.

categories, there is no ‘knowledge standard’ following which providers could be held liable if they had actual knowledge of the illegality of the content they transmit or temporarily store. Article 16 is closely linked to Article 6 (the hosting liability exemption), as explained in Chapter 7. Thus, internet access providers, open WiFi providers, domain name authorities, messaging apps, videotelephony tools, web browsers, VPN services, and content delivery networks remain outside those rules. These services only have the universal obligation to conduct content moderation fairly under Article 14 if they decide to engage in content moderation. Article 15 prescribes some level of transparency, but again, only if they choose to moderate.²⁸ The fairness required by Article 14 for other providers cannot be equated with the elaborate set of procedural rules prescribed for hosting services by Article 16, although undeniably they give some indication, and can be followed by such providers voluntarily.

Hosting services are thus the core target of Article 16. The relevant services include social networks, various content-sharing services (pictures, text, or video), auction sites, marketplaces, user-edited encyclopaedias, and discussion forums. However, even among hosting services, there exist some less traditional, infrastructure-like services that only moderate content on occasion, such as web hosting,²⁹ cloud computing services, map services, or app stores.³⁰ Nonetheless, all these hosting services are subject to the basic due diligence obligations concerning notice submission and handling under Articles 16–17. For hosting services that are *not* online platforms, such as web hosting and cloud services, or which do not qualify as medium-sized or bigger firms (Chapter 9), Articles 16–17 (and also 18) remain the only obligations they are subject to in the area of content moderation.

Despite these limitations, Article 16 sets out an important framework under which all providers of *hosting* services are subject to an elaborate notice and action choreography, which was subject to fierce discussions during negotiations.³¹ As explained by Roche Laguna, ‘while the Council’s stance seemed quite similar to the Commission’s proposal and they did not propose strong variations, the European Parliament represented both traditionally-confronted positions: on the one hand, a fierce defence of freedom of expression and information online, hence limiting notices’ effect to the bare minimum; on the other hand, an impulse to expand the effect of such notices, including so-called “stay-down” effects, and facilitating the submission of notices, following demands of some industries.’³² In the end, the result is very close to the Commission’s original proposal.

²⁸ See the separate chapter on transparency, ch 16 of this book.

²⁹ eg AWS suspending web hosting for Parler, John Paczkowski and Ryan Mac, ‘Amazon is Booting Parler Off of its Web Hosting Service’ *BuzzFeed News* (10 January 2021) <<https://www.buzzfeednews.com/article/johnpaczkowski/amazon-parler-aws>> accessed 4 September 2023.

³⁰ Sarah Perez and Brian Heater, ‘Apple Suspends Parler from App Store’ *TechCrunch* (10 January 2021) <<https://techcrunch.com/2021/01/09/apple-suspend-parler-from-app-store/>> accessed 4 September 2023.

³¹ *Interview with Irene Roche Laguna*, Deputy Head of Unit for Coordination and Regulatory Compliance, European Commission (2021–23).

³² *ibid.*

11.2.1 The mechanism

Providers of hosting services are uniquely placed to provide the mechanism required for this notice and action choreography. As Recital 50 explains, they play a critical role in tackling illegal content online as they store the information provided by and at the request of the recipients of the service and typically give other recipients access thereto, sometimes on a large scale.³³

Under Article 16(1) DSA, they are obliged to ‘put mechanisms in place to allow any individual or entity to notify them of the presence on their service of specific items of information’ that they consider illegal content. The illegality depends on the national or EU law (Article 3(h)). Those mechanisms shall be ‘easy to access, user-friendly, and allow for the submission of notices exclusively by electronic means’ (Article 16(1)). Thus, as mentioned above, the DSA prescribes that providers must allow for notifications to be received by electronic means.³⁴ The DSA, in other parts, imposes an obligation on recipients of the service to send any communications electronically (Article 12(1)). As such, both sides of the notice and action mechanism are effectively required to utilise electronic communication. In practice, the hosting providers are likely to use a range of options, including regular email submission, electronic forms, or more sophisticated application interfaces for repeated notifiers. The DSA foresees a role for standardisation in this space (Article 44) to ensure that this obligation is affordable for the smallest hosting service providers or those services that only offer hosting as an ancillary service.

The obligation contained in Article 16 refers primarily to the establishment of a submission ‘mechanism’ that shall ‘facilitate the submission of sufficiently precise and adequately substantiated notices’ (Article 16(2)). Compliance with this Article will be met when the mechanism is in place under the conditions established, in particular allowing the submission of sufficiently precise and adequately substantiated notices, a standard derived from the Court of Justice of the European Unions (CJEU) case law.³⁵ Such mechanisms should also be ‘clearly identifiable, located close to the information in question and at least as easy to find and use as notification mechanisms for content that violates the terms and conditions of the hosting service provider.’³⁶ If such a system is not in place, it would not allow notifiers to provide the necessary information (eg making the submission of notices difficult or hiding the mechanism).³⁷ Such providers

³³ DSA, Rec 50.

³⁴ Saulius Kaleda, Paul-John Loewenthal, and Folkert Wilman, *Digital Services Act: Commentary* (forthcoming, OUP 2024) § 16 (regarding the knowledge standard).

³⁵ *L’Oréal SA and others v eBay International AG and others* ECLI:EU:C:2011:474.

³⁶ DSA, Rec 50.

³⁷ This was the main problem identified in the first round of enforcement of German NetzDG, or Germany’s Network Enforcement Law. In July 2019, the authority imposed a fine on Facebook of €2 million based on its flawed transparency report for the first half of 2018 and on its reporting form being ‘too hidden’ for its users, see German Federal Office of Justice, ‘Federal Office of Justice Issues Fine against Facebook’ (3 July 2019) <https://web.archive.org/web/20221219105930/https://www.bundesjustizamt.de/DE/ServiceGSB/Presse/Pressemitteilungen/2019/20190702_1.html> accessed 19 December 2022; also Patrick Zurth, ‘The German NetzDG as Role Model or Cautionary Tale? – Implications for the Debate on Social Media Liability’ (2021) 31 *Fordham Intellectual Property, Media and Entertainment Law Journal* 1084.

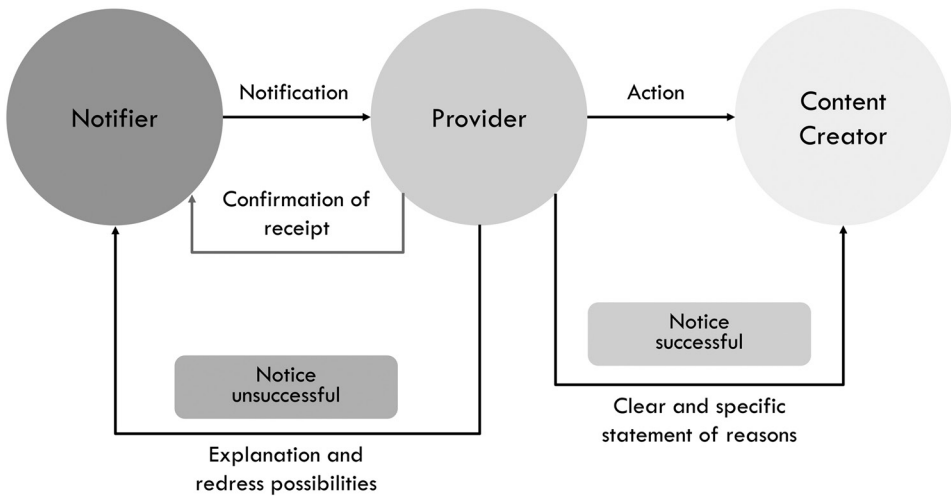


Figure 11.2 Notice and takedown choreography

could be liable for violations of the DSA’s due diligence obligations, despite the fact that they will retain their liability exemptions for the hosted content.

The language thus builds upon the elements required to confer actual knowledge of third-party illegal content upon hosting providers. The concept’s goal is two-fold: to allow notifiers to identify what is illegal and to allow them to explain reasons, including providing additional evidence, if necessary. The ‘mechanisms’ that would preclude providing evidence or constrain the explanation to avoid receiving effective knowledge are incompatible with Article 16. Figure 11.2 illustrates the procedure.

11.2.2 The ‘notice’

Article 16(2) DSA spells out that the notification mechanism shall be such ‘to enable and to facilitate the submission of notices³⁸ containing all of’ the following four basic elements: identification of the notified information, explanation of why it is illegal, notifier’s name and contact details, and a good faith statement.

11.2.2.1 Identification of the illegal content

One of the most contentious parts of notification requirements concerns the identification of the information. The DSA requires that the notification includes ‘a clear indication of the exact electronic location of that information, such as the exact URL or URLs, and, where necessary, additional information enabling the identification of the illegal content adapted to the type of content and the specific type of hosting service’

³⁸ The obligation is not to have complete notices but to establish a system that enables gathering all these elements.

(Article 16(2)(b)). The provision thus identifies URLs as the primary method of reference in a notification while not insisting on them as the only way. This is sensible given that some hosting services might not allow for identification by a URL, for instance, when accessing content via an app.

Each notification should therefore include any means that identifies the illegal information in question. If the content is dynamic and without a URL, it could be a screenshot complemented by instructions (eg accounts or pages) on where to find it. The notification mechanism could also extract the location automatically from the content the user is reporting. Finally, if the notification concerns the behaviour of an individual (eg repeated spamming) or groups (eg harassment or war propaganda) rather than a specific piece of content,³⁹ the identification would primarily concern the actors, and then examples of their behaviour.

In any event, since any follow-up search efforts slow down the assessment by platforms and increase the cost of compliance, notifiers shall employ reasonable means to prepare the instructions concerning the location of information. The responsibility here also lies with the providers who should make it easier to pinpoint specific information for the notification. After all, Article 16(2) requires that platforms design their service to facilitate such notification. If they fail to do so, they might be expected to sort through notifications that are more difficult to locate. On the other hand, if providers offer a simple and accessible notification interface to locate the information, there is no reason why they should accept hard-to-process forms like screenshots with ambiguous written instructions. This is also emphasised by the reference to ‘adaptation’ to each service.

In any event, what is clear is that the notice mechanism is envisioned to identify specific pieces of illegal content and not to receive generic instructions, such as those concerning all works of a given author or all posts by a relevant user. The provision does not allow for the so-called notice-and-stay-down mechanisms to prevent the reappearance of the same content. The location of a piece of content refers to the existing piece of content and not to future ones. It is possible, however, to notify multiple specific items of allegedly illegal content through a single notice.⁴⁰

11.2.2.2 Explanation of why the content is considered illegal

Notices can only trigger actual knowledge of the illegality of the content ‘where they allow a diligent provider of hosting services to identify the illegality of the relevant activity or information without a detailed legal examination’ (Article 16(3)).

In order to do so, Article 16(2)(a) requires that the notifier provides ‘a sufficiently substantiated explanation of the reasons why the individual or entity alleges the information in question to be illegal content’. The level of explanation will differ between

³⁹ See examples provided by Douek (n 13) 540; Camille François, ‘Actors, Behaviors, Content: A Disinformation ABC’ [2019] Working paper of Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression <https://www.ivir.nl/publicaties/download/ABC_Framework_2019_Sept_2019.pdf> accessed 29 August 2023.

⁴⁰ DSA, Rec 50.

various types of unlawful content. Content that is, per se, illegal will probably require little explanation. Context-sensitive content will require addressing the obvious reasons why the content is not justified. For instance, a notification claiming a violation of copyright must explain that the picture is protected, who owns its copyright, and why the use is not justified by exceptions or an existing licence. Only with this information can the provider make a proper decision. Similarly, in the context of allegedly defamatory content of a factual nature, the notifier must explain why the facts are incorrect and the content therefore illegal. If the evidence is necessary to substantiate these claims, the notifier should be allowed to upload it.

11.2.2.3 Notifiers' identification

While the DSA requires the self-identification of *notifiers* as a general rule (Article 16(2)(c)), this does not necessarily imply the self-identification of *victims*. In cases of certain sexual or child-related sexual offences,⁴¹ the notifier does not have to identify themselves. Moreover, since the DSA allows victims to be represented by various organisations, they do not have to file in their own name, even in the context of other unlawful content (Article 86). In addition, many organisations can file notifications without consulting or knowing the victim because the ability to file notifications is *not* preconditioned upon any right of action. Only the notification of illegal content whose assessment is context-dependent and usually requires additional evidence (eg the truth defence in the context of defamation) might be indirectly constrained since the notification cannot succeed without such evidence. In contrast, content that is per se illegal, such as child abuse material or terrorist content, can be notified by anyone. This means that the self-identification of the victim is not required in many other cases, not just those explicitly exempted.

11.2.2.4 Statement of good faith

Each notification shall be accompanied by 'a statement confirming the bona fide belief of the individual or entity submitting the notice that the information and allegations contained therein are accurate and complete' (Article 16(2)(d)). This requirement is presumably inspired by the US Digital Millennium Copyright Act (DMCA).⁴² The providers themselves might use the statements when they decide to act against the notifiers, for instance, to collect damages for the cost of compensation paid to content creators for wrongful takedowns or restrictions. The statement might also be used by content creators, other users, or their organisations when they seek redress for wrongful restrictions.

⁴¹ Art 16(2) DSA refers to arts 3–7 of Directive 2011/93/EU, which covers the following offences: sexual abuse, sexual exploitation, child pornography, solicitation of children for sexual purposes, incitement, aiding and abetting, and attempt, see European Parliament and Council Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography [2011] OJ L335/1, arts 3–7.

⁴² DMCA (1998), 17 USC § 512(c)(3)(A)(v).

11.2.3 What is illegal content?

The definition of illegal content was debated in negotiations until the very end. ‘Illegal content’ is defined as ‘any information that, in itself or in relation to an activity, including the sale of products or the provision of services, is not in compliance with Union law or the law of any Member State which is in compliance with Union law, irrespective of the precise subject matter or nature of that law’.⁴³ The notion of illegality thus covers the illegality of content or activity related to content. The former covers typical scenarios of terrorist content, hate speech, and copyright infringements, while the latter covers grooming, stalking or spam. Even situations where content creators sell goods or offer services without a license should fall under illegal content because the resulting information is not compliant with consumer law.

The DSA, through the definition of ‘illegal content’, de facto opens the doors to the applicability of the EU Charter to all digital content disputes. By extension, the CJEU is competent in deciding whether a national law violates the EU Charter (and, most likely, the European Convention on Human Rights). As a result, the CJEU determines the outer limits of what is ‘legitimately’ illegal content on the national level. In this special area, it thus gains a role similar to the European Court of Human Rights, which has always been in charge of the human rights review of all national rules on content. The DSA places the CJEU in the same position through a piece of secondary EU law. Therefore, for instance, any national rule prohibiting the depiction of homosexual relationships or prescribing disclaimers can be reviewed for its compatibility with the EU Charter. If it is legitimate, it must be enforced through the DSA’s mechanisms. If it violates the EU Charter, it may not be. While in theory, this is clear, in practice, it will be arduous to find a legal route through which the courts, and eventually the CJEU, can review such rules (Chapter 3).

The DSA does *not* create any explicit mechanism through which such considerations can enter the application of the law by the DSCs, providers, users, or out-of-court dispute settlement (ODS) bodies. Thus, for instance, providers assessing notices or the ODS bodies hearing appeals do not have an explicit mandate to scrutinise the underlying law from the perspective of its validity. After all, creating such a mechanism in the context of delegated enforcement by private parties is not easy. The main resolution would seem to be to presume the lawfulness of such national rules and challenge them *ex post* through national judicial systems.

In most cases the content will be ‘legitimately illegal’ in one Member State but not necessarily in another. Consider examples of prohibitions of the promotion of abortion services, religious blasphemy, different shades of laws about defamation, rules on disinformation, advertising of sugary drinks, or depiction of cruel behaviour on animals, etc. The DSA, as the E-Commerce Directive (ECD) before it, does not explicitly limit the geographical implementation of content moderation decisions.⁴⁴ However, the

⁴³ Rec 12 DSA informs the broad interpretation that should be made on what can constitute ‘illegal content’.

⁴⁴ Case C-18/18 *Eva Glawischnig-Piesczek v Facebook Ireland Limited* ECLI:EU:C:2019:821.

constitutional requirement of strict targeting of the measures, reiterated by the CJEU case law⁴⁵ and the DSA itself (Recital 51), means that the over-implementation of local restrictions can be problematic. Over-implementation often diminishes the rights of other users ‘who are using the provider’s services in order to lawfully access information.’⁴⁶ The situation is, however, complicated by the fact that service providers have a right to conduct their business as they see fit, thereby they are in principle allowed to set their own house rules that can contractually broaden the scope of unacceptable content (eg to prohibit nudity).

The legal complexity that arises in a global environment is likely to incentivise the removal of content based on the terms and conditions.⁴⁷ A similar situation applies if the basis for enforcement is local orders, for which the DSA also provides specific requirements on their geographic scope.⁴⁸

11.2.4 The ‘action’

Articles 16(1) and (2) do not *oblige* hosting service providers to act upon notices. The notice may or may not give rise to actual knowledge or awareness for the purposes of Article 6, depending on whether they allow a diligent hosting service provider to identify the illegality of the relevant activity or information without a detailed legal examination. If the notice does give rise to actual knowledge, the hosting service provider will lose the protection conferred by the liability exemption. However, its liability (in case it fails to act) will be judged on the basis of the national or European law establishing positive liability, not based on the DSA.

During negotiations, it was discussed whether creating an *obligation to remove* content was necessary or appropriate (as is the case under much more narrow German law),⁴⁹ but the question was deliberately decided in the negative.⁵⁰ It was feared that doing so would incentivise the over-removal of lawful content, as providers would err on the side of caution and immediately remove the content in cases of doubt to avoid infringing such an obligation.⁵¹ Moreover, the DSA is a horizontal measure, and thus

⁴⁵ Case C-401/19 *Republic of Poland v European Parliament and Council of the European Union* ECLI:EU:C:2022:297.

⁴⁶ *ibid* para 56.

⁴⁷ Ben Wagner reports that the average level of content deleted by online platforms is 10.9% and, within this, 4.33% was deleted for reasons of legal compliance, while 95.67% owing to terms of service violations: Ben Wagner, ‘Digital Election Observation: Regulatory Challenges around Legal Online Content’ (2020) 91(4) *The Political Quarterly* 739.

⁴⁸ Ch 8.

⁴⁹ Germany’s Network Enforcement Law, *Netzwerkdurchsetzungsgesetz* (NetzDG) v 01.09.2017 (BGBl. I S 3352), requires networks to remove or disable access to *manifestly illegal content* to be removed or blocked within 24 hours. Content which is *non-manifestly illegal* can be removed or blocked within seven days. A similar law (Avia law) was passed in France, but it was declared unconstitutional by the French Constitutional Court due to its interference with freedom of expression, *Conseil Constitutionnel*, 18 Juin 2020, *Décision* n° 2020-801 DC.

⁵⁰ *Interview with Irene Roche Laguna* (n 31).

⁵¹ Whether the Member States are allowed, after the adoption of the DSA, to impose such obligation in national law, is discussed in ch 17 of this book.

creating such an obligation could have a draconic effect in some areas where the loss of the exemption should not immediately lead to liability. It would also change Article 16's ethos to more of a content-regulating rule.

After receiving the notice, the provider shall issue a *confirmation of receipt* to the notifier if its contact details were provided with the notice (Article 16(4)). Once the provider decides on the action to be taken, the notifier shall be updated 'without undue delay' about the outcome, including the redress possibilities that the notifier has (Article 16(5)).

The DSA has two requirements for the provider's decisions:

- Each assessment of a notification on the basis of the fact that the content is *illegal*⁵² shall be 'timely, diligent, non-arbitrary and objective' (Article 16(6)).
- Each decision leading to a relevant content restriction must be accompanied by a 'clear and specific statement of reasons' (Article 17(1)); this requirement applies to decisions based on illegality and/or terms and conditions.

There is no time specification of what 'timely' means. Given the broad scope of the obligation (all hosting service providers), it was left open as to which service provider would be expected to act. All these questions are merely informed by Recital 51, which clarifies that, to be aligned with the fundamental rights guaranteed under the Charter of all parties concerned:

... any action taken by a provider of hosting services pursuant to receiving a notice should be strictly targeted, in the sense that it should serve to remove or disable access to the specific items of information considered to constitute illegal content, without unduly affecting the freedom of expression and of information of recipients of the service. Notices should therefore, as a general rule, be directed to the providers of hosting services that can reasonably be expected to have the technical and operational ability to act against such specific items. The providers of hosting services who receive a notice for which they cannot, for technical or operational reasons, remove the specific item of information should inform the person or entity who submitted the notice.

Failing that, the provider's interference with the freedom of information of those users would be unjustified in the light of the objective pursued.

This recital covers two important and interrelated issues. Firstly, any action must be interpreted to be limited geographically to what is strictly necessary: if the content is illegal in one Member State, global removal is not strictly targeted. Secondly, if a hosting service provider cannot act with the necessary level of granularity against a particular

⁵² If the decision is taken on the basis of the provider's terms and conditions, Art 14(4) still requires providers to 'act in a diligent, objective and proportionate manner in applying and enforcing the restrictions', but it does not require the action to be 'timely'.

item to achieve strict targeting because it can only act at a higher level up in the infrastructure (as it could be the case, for instance, for web hosting services or cloud infrastructure services), it is not expected to ‘have the technical and operational ability to act against’ a specific item. This results in an ‘unserved notice’, which should not lead to a loss of the liability exemption. In that case, the provider must inform the notifier about the situation. This is what has been called the ‘subsidiarity principle’, whereby an action should be as close to the content as possible given the circumstances, and technical and operational ability to act.

Another special case concerns decentralised versions of content moderation on services, which split their content moderation between centralised (operated by the provider’s legal team) and decentralised forms (driven by the community or left to operators of add-on services). The DSA presupposes moderation is mostly centralised by providers’ employees or contractors. However, some services, such as Reddit or Wikipedia, are known to split their content moderation.

The DSA’s rules apply only to those channels of content moderation that the provider instructs. Thus, if a community moderates its content independently without significant involvement of the provider, it remains outside of the remit of the DSA rules. For this reason, an independent community might not need to issue a statement of reasons. That being said, notifications or orders received based on the DSA’s recognised channels (orders or notifications), must be resolved in compliance with the DSA rules. This means that the DSA effectively pushes community content moderation to areas where the content is found *proactively*, ie without an external notification or order, such as following the community’s monitoring efforts.

On the other hand, if the community is only an extension of the provider and lacks any real independence from it, the actions of volunteers can be attributable to the provider and thus remain governed by the DSA. The key test for this lies in the words ‘undertaken by providers of intermediary services’ (Article 3(t)).

11.2.5 Relationship with liability exemptions

While the observance of Article 16 is clearly related to standards that govern liability exemptions, the relationship between compliance with conditions for liability exemptions on the one hand and due diligence obligations on the other is more complex and fundamental.

For instance, the provider might comply with due diligence obligations and process a notification in a procedurally sound manner but still make the wrong decision substantively. In such cases, there is no violation of the DSA due diligence obligations, but there might be liability for underlying content. Alternatively, the provider acts upon a notification and avoids any liability for the users’ content; it might do so in a way that is procedurally in violation of the DSA due diligence obligations (eg by failing to provide a confirmation to the notifier or giving advance notice prior to suspension). Therefore, the due diligence obligations, even those in the context of Article 16, based

on interrelated standards, are best seen as a separate layer of obligations with their own goals and enforcement mechanisms (Chapter 9).

While Article 16 does not contradict the case law of the CJEU on the hosting liability exemption, neither does it modify such case law in any way. A failure of providers to meet obligations imposed by Article 16 does not trigger any automatic consequences in the context of the liability exemption envisaged by Article 6 of the DSA.

Functionally, the most important consequence of the notice is that, if it is *valid*, it might trigger the acquisition of the provider's actual knowledge or awareness about the illegality of content (Article 16(3)). This strips the provider of the liability exemption—but only for that notified piece of content: the knowledge is limited only to what is specifically notified and does not extend to other information. That being said, if the provider uncovers other illegal information while examining the notice, it shall also act on that. In practice, however, it might be difficult to obtain evidence on the extent of the provider's knowledge and subsequent omission in this case (Chapter 7.4).

The Commission's proposal for the DSA initially intended to introduce an implied presumption of knowledge.⁵³ It suggested that just by 'ticking all the boxes' on the prescribed content of the notice, such notice would automatically trigger actual knowledge. This was not in line with the CJEU case law. In the final version, the text has been revised. A complete notice (containing all elements under Article 16(2)) will *not* automatically trigger actual knowledge. The inverse is also true. Even a notice missing the identity of the notice provider or a good faith statement could still trigger actual knowledge.⁵⁴ However, the notifier omitting such information would fall short of the DSA's requirements, which could be taken into account when considering what damages they are owed.⁵⁵

Article 16(3) DSA stipulates what a notice requires to give rise to actual knowledge or awareness for the purposes of Article 6 in respect of a specific item of information: it must 'allow a diligent provider of hosting services to identify the illegality of the relevant activity or information without a detailed legal examination'. This provision codifies the standard of manifest illegality developed by the CJEU during the legislative process (Chapter 7.4). It was heavily debated during negotiations, raising the questions

⁵³ The proposed art 14(3) stated that 'notices that include the elements referred to in paragraph 2 shall be considered to give rise to actual knowledge or awareness for the purposes of Article 5 in respect of the specific item of information concerned'; Commission, 'Proposal For A Regulation of the European Parliament and of the Council on a Single Market for Digital Services (DSA) and Amending Directive 2000/31/EC' COM(2020) 825 final, art 14(3).

⁵⁴ Kaleda, Loewenthal, and Wilman (n 34) § 16.

⁵⁵ In liability systems worldwide, it is an established principle that if victims contribute to their own damage by failing to exercise due care, the person who is otherwise liable will face less or no liability. This principle of comparative negligence was famously formulated by Lord Ellenborough in 1809 who said that, 'One person being in fault will not dispense with another's using ordinary care for himself'. (*Butterfield v Forrester* (1809) 11 East 60 at 61, 103 ER 926 at 927). See more generally, Martin Turck, 'Contribution Between Tortfeasors in American and German Law - A Comparative Study' (1966) 41 *Tulane Law Review* 1; Ernest Turk, 'Comparative Negligence on the March' (1950) 28 *Chicago-Kent Law Review* 189; Giuseppe Dari-Mattiacci and Eva S Hendriks, 'Relative Fault and Efficient Negligence: Comparative Negligence Explained' (2013) 9(1) *Review of Law & Economics* 1. Also, art 8.1.1 of the Principles of European Tort Law (PETL): 'Liability can be excluded or reduced to such extent as is considered just having regard to the victim's contributory fault and to any other matters which would be relevant to establish or reduce liability of the victim if he were the tortfeasor', taken from the European Group on Tort Law, 'Principles of European Tort Law (PETL)' <<http://www.egtl.org/PETLEnglish.html>> accessed 4 September 2023.

of: what precisely is ‘manifestly illegal’, and why should actual knowledge be limited to ‘manifestly illegal content’?

As explained in Chapter 7.4, the CJEU in *YouTube and Cyando* established that a notice ‘must contain sufficient information to enable the operator of that platform to satisfy itself, without a detailed legal examination, that that communication is illegal and that removing that content is compatible with freedom of expression.’⁵⁶ This was subsequently confirmed in *Poland* judgment. In the Council, several Member States insisted⁵⁷ on explicitly adopting this high threshold for notices after the CJEU published the landmark *Poland* judgment,⁵⁸ reiterating *YouTube and Cyando*. As a result, Recital 53 now reads as follows:

Where a notice contains sufficient information to enable a diligent provider of hosting services to identify, *without a detailed legal examination, that it is clear that the content is illegal*, the notice should be considered to give rise to actual knowledge or awareness of illegality.⁵⁹

Consequently, the provider is not expected to act expeditiously if the underlying notification relates to content whose illegal nature is not clear despite the notification. This is particularly relevant in cases of defamatory content whose illegality might be difficult to establish (eg it is not clear if a review of a restaurant is true or false based on what parties to the dispute claim).

A special situation concerns compliance with what I have termed ‘illegitimate’ national content rules, ie when a provision of national law violates the EU Charter, but it forms a basis for an order or notification. The DSA provides a hosting liability exemption if providers act upon manifestly illegal content they became aware of. If non-compliance with the illegitimate national rule is evident, providers are expected to act if they wish to preserve the liability exemption—although they only need to act locally. However, since they are only required to act under the illegitimate national rules and not under the DSA, they might also decide to take the legal risk and not comply with such requests.

In such cases, whenever the Member State, or an individual in that Member State, tries to enforce the rule against the provider in courts or through the authorities, the provider can invoke the defence of the rule’s non-compliance with the EU Charter. If successful, the liability exemption would be preserved because the content was never ‘illegal’ according to the DSA’s definition (Article 3(h)). The same would be true for potential violations of due diligence obligations that rest on the ‘illegality’ of content.

While Article 6 DSA (similarly to Article 14 ECD) conditions the liability exemption to the hosting provider on acting ‘expeditiously’ upon obtaining actual knowledge or awareness, Article 16(6) requires hosting providers to take their decision in respect

⁵⁶ Joined Cases C-682/18 and C-683/18 *Frank Peterson v Google LLC and others and Elsevier Inc v Cyando AG* ECLI:EU:C:2021:503, para 116.

⁵⁷ *Interview with Irene Roche Laguna* (n 31).

⁵⁸ *Poland* (n 45) paras 53, 91.

⁵⁹ DSA, Rec 53 (emphasis mine).

of a notice in a ‘timely’ manner. Despite some calls to define what expeditiously or timely means⁶⁰ and thereby establish specific timeframes, the DSA leaves the notion undefined on purpose.

Pre-DSA, some countries had experimented with explicit timeframes.⁶¹ The two notable examples are Germany and France.⁶² The French law, known as Avia law, was declared unconstitutional by France’s Conseil Constitutionnel, which called for extreme caution against timeframes that were too tight.⁶³ Post-DSA, experimentation with explicit timeframes is no longer possible due to pre-emption (Chapter 17).

As a result, whether the action was taken ‘expeditiously’ (condition of the liability exemption) or ‘timely’ (a requirement for compliance with Article 16 DSA) will need to be assessed on a case-by-case basis.⁶⁴ The Member States are not allowed to prescribe specific time limits in their national legislation due to the DSA’s pre-emption that requires ad hoc balancing. Only the EU legislature can specify the period, as it did in the Terrorist Content Regulation (TCR) (Chapter 18). In this context, it is remarkable that the creative sector, for instance, which would naturally be interested in expeditious action against copyright infringements, openly argued against the introduction of specific time limits for the take down of illegal content as ‘any indication of specific time limits would be short-sighted and make the DSA obsolete very quickly in light of the continuous and rapid technological developments.’⁶⁵

11.3 Step 2: Statement of Reasons (Article 17)

An important added-value of the DSA is its ability to extend and improve on existing rules that apply in sector-specific contexts (like the platform-to-business relationships (PTBR))⁶⁶ or industry practices based on the US DMCA’s ‘counter-notices’ for copyright notices.⁶⁷ Article 17(1) is an example of such added-value and has plays a crucial

⁶⁰ Several amendments in the European Parliament that did not make it to the final report called for a 24-hour deadline, or even ‘30 minutes where the illegal content pertains to the broadcast of a live sports or entertainment event’, European Parliament, ‘IMCO Report on the proposal for a regulation of the European Parliament and of the Council on a Single Market for Digital Services (DSA) and amending Directive 2000/31/EC’ Report A9-0356/2021, Opinion of the Committee on Legal Affairs, 419, amendment 111 (new Art 5(1)(a). In the EU Council, Germany attempted to reproduce its national law NetzDG into the DSA, thereby including a 24-hour deadline for removal, Presidency of the Council of the European Union, ‘Digital Services Act: Consolidated Comments on Chapter 3 and Respective Recitals’ (2021) Document WK 5155/2021 REV 2, 140.

⁶¹ Ch 17 on the DSA’s relationship with national laws.

⁶² Ch 17 for detailed debate.

⁶³ The law imposed on certain operators of online platforms, under penalty of criminal sanction, an obligation to remove or make inaccessible within 24 hours illegal content because of its manifestly illegal nature, Conseil Constitutionnel, 18 Juin 2020, Décision n° 2020-801 DC, para 18.

⁶⁴ Folkert Wilman, *The Responsibility of Online Intermediaries for Illegal User Content in the EU and the US* (Edward Elgar Publishing 2020) para 2.74.

⁶⁵ International Federation of the Phonographic Industry (IFPI) and others, ‘DSA: A Missed Opportunity and a Step Backwards’ (2021) para 2 <https://www.ifpi.org/wp-content/uploads/2021/10/Creative-sector-in-Europe-A-letter-on-the-DSA_October-2021.pdf> accessed 4 September 2023.

⁶⁶ Art 4 P2BR already establishes that ‘where a provider of online intermediation services decides to restrict or suspend the provision of its online intermediation services to a given business user in relation to individual goods or services offered by that business user, it shall provide the business user concerned, prior to or at the time of the restriction or suspension taking effect, with a statement of reasons for that decision on a durable medium’.

⁶⁷ DMCA (1998) 17 USC § 512(g).

role in the DSA because it defines the due process obligations applicable to the crux of the entire choreography: the content moderation decision itself. The scope is broad because it applies to restrictions based on *illegality* or is deemed *incompatible with terms and conditions*. This leaves out only actions by providers that do not qualify as individual restrictions, such as demotions due to the prominence given to paid content.

11.3.1 Scope of individual explanations

Article 17(1) requires all hosting service providers to provide a ‘clear and specific’ statement of reasons to any affected recipients of the service whose information has been made subject to any of the following restrictions:

- (a) any restrictions on the visibility of specific items of information provided by the recipient of the service, including removal of content, disabling access to content, or demoting content;
- (b) suspension, termination or other restriction of monetary payments;
- (c) suspension or termination of the provision of the service in whole or in part;
- (d) suspension or termination of the recipient’s accounts.

The scope of Article 17 is narrower than the definition of content moderation in Article 3(t). To recall, the DSA’s definition of content moderation covers any measure aiming, in particular, to detect, identify, and address illegal content or information incompatible with their terms and conditions. What Article 17(1) does is spell out what these measures can represent: those relating to a) visibility of content, b) its monetisation, and c) suspension or d) termination of service or account. The table below, inspired by Eric Goldman’s taxonomy of remedies⁶⁸ illustrates how various typical remedies in content moderation are likely to be classified from the perspective of Article 17 DSA (see Table 11.1).

The Commission’s original proposal had been limited to decisions ‘to remove or disable access to specific items of information,’⁶⁹ but this was eventually revised to the current iteration with its arguably far wider scope. This broad scope is likely to cause difficulties in determining what precisely falls under each of the classifications, but the most problematic tensions will likely revolve around what constitutes visibility restrictions under Article 17(1)(a), as almost anything could be described as such.

Consider when a platform changes its recommender algorithm to start recommending more happy content. Such decision clearly affects visibility of unhappy content. However, the platform does not need to have a working definition of what is unhappy content. The optimisation can be based on various imprecise proxies that

⁶⁸ Eric Goldman, ‘Content Moderation Remedies’ (2021) 28(1) Michigan Technology Law Review 1.

⁶⁹ Commission, ‘COM(2020) 825 Final’ (n 53) art 15(1). Both the Council and the European Parliament agreed that this was too restrictive and extended the obligation to other kinds of content moderation decisions.

Table 11.1 Types of content restrictions.

Content visibility restrictions (Art 17(1)(a))	Monetisation restrictions (Art 17(1)(b))	Service restrictions (Art 17(1)(c))	Account restrictions (Art 17(1)(d))	Content moderation outside Article 17
Removing content	Forfeiting earnings	Blocking access to a service	Blocking accounts	Shaming
Suspending content	Suspending access to earnings	Suspending rights on a service	Suspending accounts	Community service
De-ranking content	Disabling income on some content	Reducing speed on a service	Erasing accounts	Attach context or warning
Redacting content	Reducing earnings	Limits put on notifications	Blacklisting registration	Apology
Shadow banning or Blacklisting	Fines	Limits on internal complaints		General changes to recommender systems

only correlate with happy content. The question then is whether such redesign of the recommender system must be individually explained to everyone affected. It certainly must be disclosed by online platforms if it constitutes one of the main parameters for such recommendations (Article 27). The DSA does not have an elegant answer, but the solution likely resides in the words ‘any restrictions of the visibility of *specific* items of information.’⁷⁰ If a platform redesigns its recommender system that targets specific items of information, an individual explanation is in order, even if the item is only part of a class (eg importing a blacklist, or defining a category of ‘unhappy content’ for delisting). However, if the changes do not target specific items of information, only general disclosure under transparency obligations is owed to the public (Articles 15(1)(e) and 27).

Similarly, labelling arguably is not a visibility restriction unless the original content is simultaneously restricted (eg labelling and subsequently blurring an image of violent content before showing it to users, or labelling coupled with de-ranking). The usage of the Commission’s database of the statement of reasons suggests that at least some companies probably couple labelling with other visibility restrictions, such as de-ranking.⁷¹ In case when labelling is applied by users, but de-ranking by providers, the statement of reasons still should be provided to affected users.

In the coming years, Article 17(1)(a) will likely cause significant difficulties in interpretation, and regulators and judges will need to flesh out the distinction. Applying Article 17(1)(a) too broadly can seriously strain platform development and design, while using it too restrictively can undermine the goal of the legislature—to ensure the

⁷⁰ Emphasis mine.

⁷¹ See <https://transparency.dsa.ec.europa.eu/statement-search> (upon closer look, all such notifications only come from Facebook).

explainability of decisions. Without such judicial or legislative clarification, the costs of uncertainty in the interim can be fairly large since this obligation applies to all hosting services, including micro businesses. The Commission's efforts to implement a database for these decisions made by online platforms (Article 24(5)) might be able to give some limited guidance to companies.

Furthermore, Article 17(4) provides that the statements of reasons shall be 'clear and easily comprehensible and as precise and specific as reasonably possible under the given circumstances'. These statements must reasonably allow the recipient of the service concerned to effectively exercise the redress possibilities that the DSA foresees—internal or external appeals or general judicial redress. Nothing in the provision prohibits the statement of reasons to be issued by an automated system. In fact, it is expected that the bigger the platform, the more likely it is that it will automate the process. Yet, even with this qualification, Article 17(1)(a) can still prove to be somewhat burdensome in practice if it is not meaningfully curtailed by soft law.

11.3.2 Exceptions

The DSA introduces three *exceptions* to the obligation to issue a statement of reasons.

The first exception concerns situations 'where the information is deceptive high-volume commercial content' (Article 17(2)). The exception clearly targets spam bots or computational propaganda that relies on automation (Recital 55). However, it is rather narrow in its definition because if the content is deceptive and high-volume but not commercial, such as war propaganda, the exception usually will not apply.

The second exception concerns decisions made based on orders from national authorities (Article 9).⁷² This makes sense, as Article 9(5) already obliges providers of intermediary services to inform the recipient of the service, including a statement of reasons 'explaining why the information is illegal content, by reference to one or more specific [legal bases]' (Article 9(2)). Such orders can delay or limit these explanations. As explained in Chapter 8, the use of Article 9 is not mandatory for the national authorities of the Member States. However, if national authorities comply with Article 9 when issuing the orders to providers, Article 17 does not apply. Thus, whenever the providers comply with requests of authorities, they must issue a statement of reasons, either based on Article 9(2) or 17. The benefit of using Article 9(2) for national authorities, if they comply with its safeguards, is that the provision gives them more flexible mechanisms which can be adopted by national law compared to the strong pre-emptive effect of Article 17.

The final third exception is a situation where the electronic contact information of the affected recipient of the service is unavailable (Article 17(2)). This was usually

⁷² In some areas, like the TCR, there are specific rules on this.

when the content creator who uploaded the content did not have to register or the registration ceased to exist.

11.3.3 Who is owed what explanations?

The statement of reasons shall be given only to ‘any affected recipients’ (Articles 17(1)–(2)). Due to the broad notion of a recipient (Article 3(b)), the obligation extends to affected content creators and, theoretically, to those who are ‘using’ the service.

Consider a situation of registered users of a video-sharing service who can no longer view the video. The DSA certainly was not written with them in mind; however, they qualify as recipients of the service, and depending on the context, they can be ‘affected’ by the imposed visibility restriction. If their details are known to the provider, this would suggest that the provider must also provide another statement of reasons to them (eg by keeping the link to a video as a tombstone with an explanation of why the content was removed or, if applicable, interlinking with the EU Commission’s centralised database according to Article 24(5)). This is a possible, albeit somewhat unintended, reading of Article 17. On the other hand, an *a contrario* reading of Article 32, whereby providers of online marketplaces need to inform buyers when a product or service happens to be illegal, could suggest that Article 17, despite its broad language, was intended to cover *only* content creators and notifiers who are affected.

The legal obligation under Article 17 also clears any doubts about the legitimacy of processing personal data that the statement of reasons might entail. For instance, if the search engines, with respect to their links, were to be considered hosting services, they would have an obligation under Article 17(1) DSA to issue a statement of reasons to the affected websites (eg news publishers) whose content they are delisting under the GDPR’s right to be forgotten.⁷³ A similar requirement already applies to search engines delisting or de-ranking ‘corporate websites’ under the Platform to Business Regulation (P2BR).⁷⁴ The DSA and P2BR respectively create legal bases for the processing of personal data in such statements of reasons.

Finally, if the notice fails to lead to a relevant content restriction, the *notifier* should equally receive notice of such an important development because of Article 16(5). This information must allow the notifier to exercise redress against the decision. The DSA does not explicitly equate it with the framework of the statement of reasons and an unsuccessful notifier cannot be ‘affected’ by visibility or other restrictions. However,

⁷³ Consequently, this would mean that the data protection law has to recognise such notifications under the legal basis of ‘legal requirement’ under art 17 of the GDPR.

⁷⁴ Art 5(4) P2BR: ‘Where a provider of an online search engine has altered the ranking order in a specific case or delisted a particular website following a third party notification, the provider shall offer the possibility for the corporate website user to inspect the contents of the notification.’ It must be noted, however, that the existence of this obligation in the context of data protection seems to be disputed by some DPAs without much explanation. The Swedish Administrative Court of Appeal in Gothenburg in November 2021 ruled that art 5(4) P2BR does not require a search engine to notify webmasters in the right to be forgotten context, see Swedish Administrative Court of Appeal, *Google LLC* [2021] Case No 2232-21.

Table 11.2 Statement of reasons requirements.

When required	Minimum contents of the provider's statement of reasons
Always	Specification of the type of restriction: visibility-restriction, account-restriction, monetisation-restriction or service-restriction
Always	'[T]he facts and circumstances relied on in taking the decision', such as whether it resulted from a notification or own-initiative investigations
Always	'[C]lear and user-friendly information on the redress possibilities' available to the recipient of the service (internal or external appeals mechanisms)
If necessary	The identity of the notifier
If relevant	The duration of the restriction
If relevant	The geographical scope of the restriction
If relevant	Information on the use of automated means
Always	Either: a reference to the legal ground relied on and explanations as to why the information is considered to be illegal content on that ground
	Or: a reference to the contractual ground relied on and explanations as to why the information is considered to be incompatible with that ground

Articles 16(5), 20(5), and 21(1), respectively, expect that the next steps of each party are informed by the possibilities for redress, and the appeal rights in each case do not differ. Thus, given that appeal is only possible if the grounds are known to the affected party, arguably, Article 16(5) should be interpreted in line with Article 17.

With regards to *what* information should be included in the statement of reasons, Article 17(3) specifies the minimum contents as follows (see Table 11.2).

11.3.4 Disclosure of the identity of the notifier

During negotiations, it was strongly debated whether the service provider should disclose the identity of the notice provider to the content provider.⁷⁵ On the one hand, such a measure could discourage rogue or abusive notices for fear of legal consequences. On the other hand, such measures could precisely discourage the exercise of the right to report illegal content for fear of retaliation (eg women reporting online harassment). Furthermore, given that Article 16 does not oblige notice providers to disclose their identity, the service provider may not even have such information. The resulting text of Article 17 is a compromise between these two concerns.

Article 17(3)(b) limits the obligation to disclose the identity of the notifier to the affected content provider only when it is 'strictly necessary'. This also follows from Recital 54, which states that 'where this information is necessary to identify the illegality of the content, such as in cases of infringements of intellectual property rights'. The rationale is thus to disclose the identity of the notifier (who does not have to be the same person

⁷⁵ Interview with Irene Roche Laguna (n 31).

as a victim) only if it is *functionally necessary* for the content providers to be able to defend themselves, for instance, by challenging the illegal nature of the content. Article 17 also provides a legal basis for the necessary processing of personal data, as required under the GDPR.

For instance, to defend herself against a claim of trademark infringement, the content provider needs to know who claims to own what rights as some legal defences depend on it; to defend herself against a claim of defamation, the content provider will need to know whose reputation is claimed to be affected. On the other hand, to assess a notification about child sexual abuse images, it is often irrelevant who reported it. It is therefore the applicable law regulating illegality that determines whether the disclosure of identity is functionally required or not. If a defence to illegality can be made in the abstract without knowing the identity of the notifier (eg the picture is not sexually explicit), disclosure is not strictly necessary.

The lack of disclosure in the context of the decision, however, does not prejudice the potential recourse that the content provider might have against the service provider to disclose the identity of the notifier.⁷⁶ Such disclosure is usually based on the national law, although in some areas, such as intellectual property law, it may be harmonised in the EU.⁷⁷

11.3.5 Notification of suspected crimes (Article 18)

Article 18 provides that all hosting providers who become aware of information ‘giving rise to a suspicion’ that some criminal offences took place must notify the law enforcement or judicial authorities of the ‘Member State(s) concerned’. If the concerned Member State is unclear, they must inform either the authorities of their Member State of establishment or the Member State of their legal representative, Europol, or both. If the providers inform only one of these entities, their obligation under Article 18 should also be fulfilled.

Hosting providers may learn about suspected relevant crimes when carrying out their risk mitigation strategies or voluntary investigations, but most typically, such information arises in the context of their content moderation processes. Consequently, this means that providers, in addition to its standard assessment, must now also include a flagging procedure within their content moderation process for notices that raise the suspicion of criminal offences. Where they suspect a relevant crime was or is likely to be committed, they must notify authorities. Moreover, they must assess the information, such as video or text, to determine which state is concerned. This is particularly important if the crime is only attempted or ongoing. However, some crimes, such as the distribution of terrorist content, can be equally time-sensitive even after they are complete. The DSA provides a number of factors that can be used by hosting

⁷⁶ Ch 8.

⁷⁷ Martin Husovec, *Injunctions against Intermediaries in the European Union: Accountable but Not Liable?* (CUP 2017).

providers to determine which authorities to notify: (a) the state where the crime was or is likely to be committed, (b) the place where the offender or (c) victim likely resides or is located.

Along with a notification, they must retain and transmit all relevant information at their disposal concerning the suspected crime. The DSA does not specify what information could be relevant. Recital 56, however, mentions that this includes ‘where relevant, the content in question and, if available, the time when the content was published, including the designated time zone, an explanation of its suspicion and the information necessary to locate and identify the relevant recipient of the service.’ Providers are effectively under obligation to retain moderated content in many circumstances for reinstatement purposes. Article 18 equally implicitly requires the retention of the suspected moderated content.

The interesting question is whether Article 18 compels the providers to always notify authorities about the identity of the suspected criminal and victim. Recital 56 speaks of the identity of the recipient of the service, which is a term that could cover both a victim and a suspected perpetrator. However, in some countries, the disclosure of identity can require some legal processes to be followed, such as the issuance of orders by competent authorities. The proactive provision of information by Article 18 seems to circumvent these processes where they exist, as it gives law enforcement information about identity without the authorities starting any process on their own. The DSA says little about this concern. Recital 56 only explains the following:

This Regulation does not provide the legal basis for profiling of recipients of the services with a view to the possible identification of criminal offences by providers of hosting services. Providers of hosting services should also respect other applicable rules of Union or national law for the protection of the rights and freedoms of individuals when informing law enforcement authorities.

It is unclear how companies will implement this provision, particularly when potential crimes are of different kinds. The legislation in the Member States can substantially differ not only for in what is labelled as a crime, but also in what procedural processes to follow.

The relevant crimes that trigger this obligation are criminal offences ‘involving a threat to the life or safety’ of persons, regardless of whether imminent or already committed. Recital 56 details that this includes offences specified in the Directives on combating human trafficking,⁷⁸ on combating the sexual abuse and sexual exploitation of children and child pornography,⁷⁹ or on combating terrorism.⁸⁰ These include:

⁷⁸ European Parliament and Council Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA [2011] OJ L101/1.

⁷⁹ European Parliament and Council Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography [2011] OJ L335/1.

⁸⁰ European Parliament and Council Directive (EU) 2017/541 on combating terrorism [2017] OJ L88/6.

- Directing or assisting a terrorist group.
- Public provocation to commit a terrorist offence.
- Recruitment and providing or receiving training for terrorism.
- Organising or otherwise facilitating travelling for the purpose of terrorism.
- Terrorist financing.
- Offences concerning sexual abuse, such as engaging in sexual activities with a child.
- Offences concerning sexual exploitation, such as recruiting or forcing a child to participate in prostitution or pornographic performances.
- Offences concerning child pornography, such as acquisition, possession, dissemination, transmission, or knowingly obtaining access to child pornography.
- Solicitation of children for sexual purposes.
- Offences concerning trafficking in human beings, such as recruitment, transportation, transfer, harbouring, exploitation or reception of persons.

The national law can specify other relevant crimes if they meet the threshold of ‘involving a threat to the life or safety’ of persons. The Commission’s proposal to limit the relevant crimes only to ‘serious’ criminal offences was opposed by the European Council.⁸¹ The final version thus refrains from using the term.

The other relevant crimes that potentially come under Article 18 are incitement to violence,⁸² stalking of protected persons, such as journalists, or crimes of kidnapping, hostage-taking, murder, or war crimes generally. The category is thus potentially vast and almost unworkable. Given the ever-changing landscape of such crimes on the national level and the number of Member States, it might be in the best interest of victims for law enforcement authorities, along with Europol, to try to standardise what qualifies as the relevant types of crimes in different countries and try to prioritise them. Otherwise, the providers might simply over-burden the authorities by the sheer volume of notifications. The authorities often have limited resources to act. Practically, it makes the most sense to notify about upcoming threats where authorities can avert harm to victims or where speedy action allows authorities to preserve and act upon the evidence. Notification about past crimes is only as helpful as the capabilities of local law enforcement authorities to process them and potentially prosecute the offenders.

11.4 Step 3: Internal Appeals (Article 20)

One of the DSA’s main objectives is to establish a safe, predictable, and trusted online environment in which the fundamental rights of users are effectively protected. This

⁸¹ General Secretariat of the Council, ‘Note on the Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (DSA) and amending Directive 2000/31/EC - General approach’ (2021) Document 13203/21, 41 (Amendment 42a)

⁸² Council Framework Decision 2008/913/JHA on combating certain forms and expressions of racism and xenophobia by means of criminal law [2008] OJ L328/55.

entails empowering users through Article 20 (and Article 21)⁸³ to contest certain decisions of online platform providers concerning the illegality of content or its incompatibility with the terms and conditions that negatively affect them.⁸⁴

In the case of users as notifiers, if the notice were unsuccessful, ie if the notifier is dissatisfied with the provider's decision, it can avail itself of the internal and external appeals envisioned by the DSA (Articles 20–21). As explained above, notifiers will receive, under Article 16, all the necessary information regarding the follow-up given to their notice by the provider, including possibilities for redress.

Similarly, users as content creators can avail themselves of the same appeal procedures under Articles 20–21 where restrictions were imposed by the provider against the content creator's content, perhaps because a notice was successful.

Such agency granted to users is much needed for medium and larger platforms, which are often the most used. This might explain why the obligations under Articles 20–21 apply exclusively to them and do not bind hosting services, which are not online platforms, or small or micro firms. Once these DSA processes become part of general expectations, smaller companies might adapt these mechanisms voluntarily to keep up with the rest of the industry.⁸⁵

11.4.1 Appeal scenarios

Given the myriad of paths to redress for both content creators and notifiers, it is useful to delineate five paths to redress in the content moderation process:

- The content creator's content is restricted on the provider's initiative.
- The content creator's content is restricted due to an order.
- The notifier is fully successful with its notice.
- The notifier is entirely unsuccessful with its notice.
- The notifier is partly unsuccessful with its notice.

Information about redress possibilities accompanies all these decisions (Articles 16(5), 17(3)(f), and 9(5)). However, the redress available is not always the same. Following the DSA, there are generally three possible types of redress, which are not mutually exclusive nor mutually dependent:

- internal appeals, or so-called complaint handling system (Article 20);
- external appeals, or so-called ODS (Article 21); and
- judicial redress, in accordance with the laws of the Member State concerned (Recital 59).

⁸³ Discussed fully below in s 11.5.

⁸⁴ DSA, Rec 58.

⁸⁵ However, even where they decide to use them voluntarily, they are not subject to advanced due obligations about how to operate them and cannot be fined for breach of those obligations.

Table 11.3 Content moderation steps.

Outcome Procedural step		Content creator's content is restricted on provider's own initiative or orders	Notifier is fully successful	Notifier is fully unsuccessful	Notifier is partly unsuccessful
All hosting providers	Level 2: Statement of reasons	Yes, provided to the content creator (Art 17; 9(5))		Explanation for the decision in feedback received (Art 16(5))	Provided to content creator (Art 17(3)(f)) and notifier (Art 16(5)) respectively
Only mid-size and bigger online platforms	Level 3: Internal appeals	Provided to the content creator under Art 20 (except for orders under Art 9(2))		Provided to the notifier (Art 20)	Both the notifier and content creator can make use of internal appeals simultaneously
	Level 4: External appeals (ODS)	Obligatory to submit to ODS initiated by content creator under Art 21 (except for orders under Art 9(2))		Obligatory to submit to ODS initiated by the notifier (Art 21)	Both the notifier and content creator can make use of ODS simultaneously
All providers	Level 5: Judicial redress	Always available under national law			

The DSA regulates the first two but does not establish the availability of judicial redress for individuals (Chapter 19). However, notifiers and content creators might, however, still have a cause of action against providers, including those who do not have to offer redress mechanisms (see Table 11.3).

11.4.1.1 The content creator's content is restricted on the provider's own initiative

In the case where the content creator's content is restricted following the provider's investigation, they must receive a statement of reasons (Article 17), which includes information on the redress possibilities (Article 17(3)(f)). As there is no notifier within the meaning of Article 16, any internal and external appeals procedures filed by the affected content creator proceed without the presence of any notifier.

11.4.1.2 The content creator's content is restricted due to an order

If the provider adopts a relevant content restriction based on an *order* issued by the authorities and providers issue a statement of reasons under Article 17, the usual appeals procedure under Article 20 is available. However, this will not be the case if the authority decides to rely on Article 9(2).⁸⁶ If Article 9 is used, an explanation is still

⁸⁶ Note, however, that only the Member State authorities can rely on art 9; authorities of the non-Member States cannot.

given, but only based on Article 9(5). On the basis of Article 20(2), the affected content creator cannot use internal appeals against decisions based on Article 9 orders and must instead challenge the order itself. While the DSA does not discuss this option, an argument can be made for the availability of internal appeals, as follows: Although Article 20(2) intentionally omits Article 9 orders, such decisions are not excluded from the scope of Article 20(1). Thus, the matter remains somewhat open. On the one hand, it is understandable that the legislature did not want to offer the ability to make appeals in response to well-drafted legal orders according to Article 9, as these are issued by authorities that are the right forum for any contestation. On the other hand, the providers could be over-implementing such orders on their own initiative, a decision that the authorities cannot reverse and thus deserving of an internal appeal avenue. Accordingly, the possible middle-ground is to allow such internal appeals only after the authorities at stake clarify the proper scope of their orders or modify their orders to accommodate the complainant. After such clarifications by authorities, the decision of the provider is arguably no longer based on Article 9 orders.⁸⁷ This does not seem drastic given that other orders than those complying with Article 9 continue to be reviewable under Article 20. For them, Article 17 applies without any changes because there is no carve-out similar to Article 17(5).

The situation is even more complex for external appeals. Although Article 21(1) references Article 20(1) for the reviewable subject matter, it does not even implicitly limit it by the types of explanations given along with the decision (as does Article 20(2)). The question thus is whether Article 9 orders could be reviewed before the ODS bodies when they cannot be reviewed in internal appeals. This, in my view, seems internally inconsistent. In any case, the ODS bodies cannot review the order itself. While the same is true for orders not based on Article 9, there the authority is not bound to explain the redress possibilities against the decision itself. Thus, in my view, the argument seems stronger that Article 21 equally cannot be used to review the decisions of platforms that implement Article 9 orders.

11.4.1.3 Notifier is successful

In the case where the notice is successful, the content creator's content is restricted. The notifier is informed about the decision (Article 16(5)), and the affected content creator receives the statement of reasons (Article 17), which includes information on the redress possibilities (Article 17(3)(f)). If the platform qualifies as a medium or larger online platform, the provided material must include information about internal and external appeals; otherwise, it need only mention judicial redress but can mention any other voluntary systems, if available. In this scenario where the notifier is fully successful, the affected content creator can avail herself of these additional options to contest decisions.

⁸⁷ The question remains on how to measure time in such cases.

11.4.1.4 Notifier is unsuccessful

If the notice is unsuccessful, the notifier can also avail itself of the internal and external appeals, as confirmed by Articles 20(1) and 21(1). While the unsuccessful notifier is not issued with the statement of reasons according to Article 17, the feedback it receives on the decision on the basis of Article 16 should include sufficient explanation which will facilitate any subsequent use of internal and external appeals. As explained above, Article 16(5) only speaks of ‘providing information on the possibilities of redress’ and does not mention any provision of reasons for the decision; one can easily imagine that without a relevant explanation of reasons for refusal, appeals could hardly be properly used. For this reason, I have argued above that Article 16(5) should have an equivalent meaning to Article 17. Given the sanction mechanism implicit in Article 21, online platforms will likely be incentivised financially to better explain their decisions to discourage the notifiers from pursuing external appeals.

11.4.1.5 Notifier is partly unsuccessful

In the case where the notice is only partly successful (eg only part of the content is taken down), both the notifier and the affected content creator can use the internal and external appeals simultaneously. The DSA does not foresee this situation explicitly, but it is likely that if two actions are pending in parallel, the providers could merge them.⁸⁸

11.4.2 Scope and outcomes

Each relevant decision can be reviewed within six months following the day the recipient of the service, including the notifier, was informed about the relevant decision (Article 20(2)). The appeal must be handled electronically and proceed at no direct cost to the complainant (Article 20(1)). It can concern the relevant content restrictions based on illegality, or incompatibility with the terms and conditions of the provider (Article 20(1)). The relevant content restrictions following Article 20(1) are the same as those indicated in Article 17 (visibility, account, monetisation, and service restrictions). As a result, the internal appeals do not, for instance, cover decisions about disclosure of information about users or other typical remedies, such as labelling, attachment of warnings, or other contextual information.

Internal appeal systems must be ‘easy to access, user-friendly, and enable and facilitate the submission of sufficiently precise and adequately substantiated complaints’ (Article 20(3)). The internal reviews must be undertaken ‘in a timely, non-discriminatory, diligent and non-arbitrary manner’ (Article 20(4)). The DSA specifies that internal appeals should allow full reviewability, ie reversal of any possible decision that was initially made, including initial inaction or application of a disproportionate remedy. If the provider finds that it made an error in its initial assessment, it shall ‘reverse its

⁸⁸ The problem, however, is that either side can file an internal complaint within six months, and an ADR review without time limitation. Thus, two review requests do not have to meet in time.

decision ... without undue delay' (Article 20(4)). Such 'reversibility' implies that the providers may only disable disputed content at the start and can only remove it following the expiration of the period for internal appeals. During this period, they have a retention obligation to assure 'reversibility'.

The internal review by a provider shall result in a 'reasoned decision' (Article 20(5)) accompanied by information about further available remedies, including the ODS appeal and judicial remedies. The DSA does not further specify the content for such a reasoned decision; however, the content required for the statement of reasons is likely applicable by analogy. Unlike the initial content restriction decisions and the related statements of reasons, the 'reasoned decisions' issued by providers following the internal appeal process must be overseen by humans (Article 20(6)). Thus, the expected minimum requirement is a proper response to complainants' objections. The DSA also requires that the human experts overseeing internal appeals are 'appropriately qualified' (Article 20(6)). It is possible that future codes of conduct will try to specify what qualifications and conditions for decision-making can be expected of persons handling such internal appeals (Chapter 20).

The DSA addresses how to resolve conflicts between multiple internal or external appeals, or internal and external appeals. Article 21(2) only provides that an online platform may refuse to engage 'when the dispute concerning the same information and the same grounds of alleged illegality or incompatibility of the content has already been resolved.' Therefore, in the case of multiple internal appeals, it is up to a provider to organise its own systems. The more serious question concerns the conflict between external appeals decisions, as the different ODS bodies can issue these. However, since online platforms are not effectively bound by these decisions and only face pressure to observe them in general, these exceptional circumstances should be easily resolvable by implementing the decision the provider finds more convincing. Internal appeals can be initiated even when a statement of reasons was not issued.⁸⁹

11.5 Step 4: External Appeals (Article 21)

The DSA considers private rulemaking that affects third-party content a potential source of significant private power over society and the market. Because digital services providers come in different shapes and sizes, the DSA only gradually constrains such power. All providers must disclose their rules (Article 14(1)), and those who store content (hosting providers) must explain their individual content moderation decisions (Article 17). Mid-sized companies that distribute the content publicly as their main functionality (online platforms) must also allow internal appeals and engage in external dispute resolution (Articles 20–21). These tiered procedural rules constrain the private power of companies when exercising their discretion and commercial freedom.

⁸⁹ This is also confirmed by art 20(2) DSA.

Any firm with a superior bargaining position that unilaterally sets rules for its business partners and consumers cannot remain impartial when interpreting such rules, especially if it is affected by the outcomes of such disputes. The temptation to bend the rules to the desired outcomes is too high. Any hidden changes affect the legal certainty. And without legal certainty, business partners and consumers build their livelihoods and lives on top of unstable fundamentals. The carpet can be pulled from under them without advance notice. The DSA does not cement the rules—it would be foolish to do so—but it tries to bring some *predictability* to the inevitable changes.

Since the companies behind the platforms handle internal appeals of content disputes and are thus not entirely independent, the DSA supplements the system by external review of decisions through the ODS (Article 21). The ODS systems have been known in the digital ecosystem for years. Domain name disputes, for instance, have been decided by swift and efficient alternative dispute resolution (ADR) systems since 1999.⁹⁰ They help domain name authorities tackle the problem of abusive registration on a global scale. Similarly, there are ADR systems in consumer law, such as in the aviation industry, in which airlines submit their disputes to impartial decision-making concerning the compensation for delayed or cancelled flights.⁹¹

The ODS bodies are not courts, not even ‘de facto’ courts. The DSA’s system is probably better described as a system of second opinions that providers cannot easily ignore and must pay for if they lose.

Article 21 DSA has a three-fold goal. First, it provides a *credible remedy* to the affected individuals who can complain to an independent party and have their cases quickly reviewed by an expert who issues a second opinion. Second, because successful applicants are reimbursed by providers, the ODS creates a *financial incentive for providers to make fewer mistakes* in their own internal review. Third, because the ODS bodies are independent of providers, they provide for a credible separation of decision-making powers from the profit-orientated leadership of companies.⁹²

The first two goals were proposed and empirically tested in the academic literature by Fiala and I before it became part of Article 21 DSA.⁹³ The papers’ idea was that the rational bias toward over-blocking documented during the past two decades could be

⁹⁰ All ICANN-accredited domain name registrars must follow the Uniform Domain-Name Dispute-Resolution Policy (UDRP), which was adopted by Internet Corporation for Assigned Names and Numbers (ICANN) in 1999. See ICANN, ‘Uniform Domain-Name Dispute-Resolution Policy’ (ICANN, 24 October 1999) <<https://www.icann.org/resources/pages/help/dndr/udrp-en>> accessed 4 September 2023.

⁹¹ See eg Centre for Effective Dispute Resolution (CEDR), ‘CEDR Aviation Adjudication Scheme Rules’ <<https://www.cedr.com/wp-content/uploads/2021/10/Aviation-Adjudication-Rules-Nov-2020-v2.pdf>> accessed 29 August 2023. For further background on the EU law in general, Pietro Ortolani, ‘The Digital Services Act, Content Moderation and Dispute Resolution’ <<https://papers.ssrn.com/abstract=4356598>> accessed 4 September 2023. Some examples of similar ADR bodies are France’s FEVAD, Signal Conso and ReclameICI, Spain’s OCU, Portugal’s electronic consumer complaints book, Luxembourg’s Médiateur de la consommation, Belgium’s French-speaking Test Achat and Dutch-speaking Test Aankoop, Germany’s Reklamation24, Italy’s Altroconsumo, UK’s PissedConsumer.com, Austria’s Ombudsstelle, the EU ODR platform, and the European Consumer Centres, etc.

⁹² Douek argued for separation within companies, Douek (n 13) 587 (‘platforms should be required to put a wall between those concerned with the enforcement of content moderation rules ... and those whose jobs is measured against other metrics, such as product growth and political lobbying’).

⁹³ Fiala and Husovec (n 17).

mitigated by giving the affected parties the ability to correct the mistakes by an outsider, thereby inflicting small costs onto providers for their initial mistakes. If many individuals use their newly gained rights and try to improve their situation, the cost for the provider becomes significant. Thus, in turn, they will work to change the flawed internal processes that give rise to the ODS disputes in the first place. The ultimate goal of the ODS is thus better internal content moderation with fewer mistakes.

11.5.1 Who can file an external appeal and when?

Every ‘recipient’ of the platform service addressed by the relevant content restrictions (visibility, account, monetisation, and service) can file an external appeal. This includes content creators, notifiers of the content, and potentially affected readers. They are entitled to file an external appeal even if they failed to initiate an internal appeal or did initiate it, but it is still pending (Article 21(1)). Naturally, they can equally file an external appeal if the internal appeal process has been finalised. The DSA does not place any time limit for initiating such an ODS procedure.

Unless states decide to subsidise some ODS bodies, the majority will be run as fee-charging projects. Thus, the existence of fees will impose an informal structure: free internal appeals are relied upon first, and fee-based external appeals are relied upon next.

Platforms must inform their users about the ODS in their statement of reasons and internal appeal decisions. According to Article 21(1), they should even facilitate access to such bodies on their own interface. Ideally, the providers would provide a simple link through which affected parties can refer their case to one of the ODS bodies whose systems are interconnected with those of providers. This is particularly important given that the DSA also requires providers to be forthcoming with various kinds of specialist independent non-profit organisations of users (Article 86(1)).

The choice of an ODS body is with the complainant. However, the ODS bodies must be experts in a particular area of dispute resolution for which they have received certification. Thus, while the choice is with the complainant, it is constrained by the availability of expert bodies in the area of the dispute. The certification in one EU state is valid across the EU.

In terms of geography, the DSA does not limit the relief to European citizens or inhabitants (Articles 3(b) and 21(1)). Thus, a successful Nigerian YouTuber with a following in the EU can use the ODS system vis-à-vis decisions of online platforms regulated in the EU (Article 3(e)). The DSA does not provide a hard limit on which EU non-residents can use the ODS system, and benefit from its compensation scheme. The CJEU will need to clarify to what extent ‘an EU connection’ is even a relevant criterion for individuals invoking the DSA rights in some cases. It is likely that the providers might protest the unrestrained use of the ODS bodies for non-EU individuals because it increases their costs. Therefore, the DSCs and ODS bodies should think about how they inform the non-EU complainants about the compensation of fees and costs.

Table 11.4 List of VLOPs/VLOSEs.

Type of service	Digital Service	COO	Company
Social media	YouTube	Ireland	Alphabet
	Facebook	Ireland	Meta
	Instagram	Ireland	Meta
	TikTok	Ireland	Bytedance
	LinkedIn	Ireland	Microsoft
	Snapchat	Netherlands	Snap
	Pinterest	Ireland	Pinterest
	X/Twitter	Ireland	Twitter
App stores	Google App Store	Ireland	Alphabet
	Apple App Store	Ireland	Apple
Marketplaces	Amazon Marketplace	Luxembourg	Amazon
	AliExpress	Netherlands	Alibaba
	Booking.com	Netherlands	Booking.com
	Temu	Ireland	Whaleco Technology
	Shein	Ireland	Infinite Styles
	Zalando	Germany	Zalando
Adult sites	Pornhub	Cyprus	Aylo Freesites
	Stripchat	Cyprus	Technius
	Xvideos	Czechia	Webgroup Czech republic
Price comparison	Google Shopping	Ireland	Alphabet
Maps	Google Maps	Ireland	Alphabet
Encyclopaedia	Wikipedia	n/a	Wikimedia
Search	Google	Ireland	Alphabet
	Bing	Ireland	Microsoft

11.5.2 What decisions are subject to ODS appeals?

ODS shall be available for all *relevant* decisions by *online platforms*.

All online platforms are obliged to submit to the ODS (Article 21 DSA). Online platforms are services that store and distribute content to the public and are operated by at least mid-sized companies (ie 50 employees or €10 million turnover).⁹⁴

In practice, most disputes will concern VLOPs (see Table 11.4).

⁹⁴ Ch 9.

Other non-VLOP platforms that are subject to ODS if they meet the mid-size company criterion are, for instance: BeReal, Reddit, Telegram (groups), Viber (groups), Airbnb, Apple Books, Vinted, Allegro, Cdiscount, Leboncoin, Roblox, eBay, Tripadvisor, Trustpilot, Gutfrege, Heureka, Skyscanner, PornHub, OnlyFans, Spotify Podcasts, DailyMotion, Github, Discord, and Tumblr.

Very large search engines (VLOSEs) are not explicitly subject to ODS; however, their situation can be complicated by the fact that various features of search engines can constitute platforms. Thus, disputes revolving around the right to be forgotten or copyright infringements could, in theory, be subject to Article 21 DSA, but the interpretation is far from being settled (Chapter 7). The Commission's database suggests that search companies so far do not issue statements of reasons in delisting or other cases.

The disputes can concern businesses or consumers. The relevant decisions are defined very broadly as 'decisions taken by the provider of the online platform on the grounds that the information provided by the recipients constitutes illegal content or is incompatible with its terms and conditions:

- (a) decisions whether or not to remove or disable access to or restrict the visibility of the information;
- (b) decisions whether or not to suspend or terminate the provision of the service, in whole or in part, to the recipients;
- (c) decisions whether or not to suspend or terminate the recipients' account;
- (d) decisions whether or not to suspend, terminate or otherwise restrict the ability to monetise information provided by the recipients.⁹⁵

Although the relevant decisions are widely construed, some are nevertheless not subject to Article 21 DSA. For instance, typical disputes between consumers and marketplaces about the quality of performance, such as services, goods, or their delivery, are not subject to external appeals. In contrast, the typical disputes between traders and marketplaces, in contrast, are more likely to be subject to them. Removal of their offerings, deduction of penalties, hiding of offers, or suspension of accounts can all qualify.

Only moderation that is conducted by the provider itself is relevant to services like Wikipedia that rely on substantial community content moderation. Unless the community is specifically instructed by the provider, community decisions are unlikely to be attributable to the provider (see section 11.2.4).

11.5.3 Who counts as an ODS expert?

In the ODS certification process, the national DSCs must assess the expertise of the candidate bodies. According to Article 21(3)(b): 'it has the necessary expertise in relation to the issues arising in one or more particular areas of illegal content, or in relation

⁹⁵ DSA, art 20(1)

to the application and enforcement of terms and conditions of one or more types of online platform, allowing the body to contribute effectively to the settlement of a dispute.' In addition, Article 21(3)(e): 'it is capable of settling disputes in a swift, efficient and cost-effective manner and in at least one of the official languages of the institutions of the Union.' Thus, the expertise concerns three main areas: language, illegal content, and terms and conditions.

The ODS bodies will inevitably delimit their expertise into sub-areas because no single body can engage experts with track records covering all the areas of law or platforms.

The two main types of ODS bodies are likely: (1) *area-specific ODS bodies* that focus on specific types of illegal content, such as hate speech, child abuse material, or copyright infringements; (2) *platform-specific ODS bodies*, such as Facebook-related, Twitter-related, etc. In addition, the ODS bodies might further narrow their expertise through the language of the disputes (eg Slovak, Finish, etc). In theory, the ODS bodies could limit their expertise further. However, they risk having the fee compensations challenged by the platforms whenever their expertise would be slightly overstepped. This is because they benefit from the fee mechanism only within the scope of their certification.

In the certification process, the national DSCs will mostly look into the composition of the experts engaged by the ODS candidate bodies. An ODS body that claims to specialise in hate speech must be able to demonstrate that its experts have a track record of assessing such subject matter. The DSA does not require legal expertise. However, given that the key activity will consist of resolving interpretation disputes, some subject matter expertise might be needed, even though legal education might not be necessary. Thus, experts working at NGOs who previously notified hate speech on specific platforms could probably submit their work experience as relevant. National DSCs should, however, be careful whom they assess as 'experts'.

Part of the expertise assessment could be how the ODS bodies screen and train their experts, including how they onboard new experts who join their ranks to keep the quality stable. Because it would not be practical for the DSCs to reapprove certification every time the expert composition at the ODS bodies significantly changes, one of the ways how to assess expertise would be to ask the ODS bodies to come up with their *own criteria* that describe their present and future experts. This will force the ODS bodies to think hard about how they define their expertise and provide the DSC bodies with a simple checklist of criteria on which they can potentially reassess or withdraw the certification.

11.5.4 What content rules apply in the ODS procedure?

The ODS body cannot have its own substantive rules for disputes. With every dispute, it must defer to the policies of a particular online platform. Therefore, the ODS bodies do not take away the rulemaking power of the platforms. Thus, in a dispute concerning hate speech, the contractual policy of a particular platform, along with state rules on hate

speech, is determinative. The same applies to remedies. If an account suspension dispute concerns copyright infringement, the first source of law is the contractual arrangement between the platform and its users. Thus, if the policy contractually constrains some legal practices, that is the starting point. If policy only reiterates some legal concepts from the legal system, such as parody, copyright norms can be applied to determine the meaning.

The applicable content rules are one of the difficult issues that the industry will need to resolve in the coming years. Without a doubt, the dynamics under the ODS might change the drafting strategies of platform providers, who have thus far preferred to draft their own special policies. Post-DSA, they might decide to create industry-wide templates on specific issues to cut down on costs. In the absence of such templates, the ODS bodies must follow the idiosyncrasy of each platform.

One of the open questions of the ODS procedure is how much power it gives the experts to declare some contractual arrangements *inapplicable* due to their conflict with the underlying legal rules. For instance, if the EU consumer law considers some arrangements illegal, should an expert ignore them or consider them relevant but refuse to apply them?

As explained in Chapter 12, the review under Article 14(4) arguably allows the ODS bodies to set aside invalid provisions which conflict with the underlying principles of fairness. However, the same argument does not apply to national laws stipulating illegality. The constitutionality review of legislation, even if *inter partes*, is reserved to the judiciary. The experts can always signal their views as obiter dictum, but their legitimacy is rather weak to take on the role of arbiters of the constitutionality of national law—even if such decisions are not legally binding.

11.5.5 Is the ODS procedure binding?

The ODS decisions are not contractually or otherwise legally binding for its parties (Article 21(2)). Instead of an arbitration model, the DSA opted for a non-binding mediation structure.⁹⁶ Providers must ‘engage, in good faith, with the selected certified out-of-court dispute settlement body with a view to resolve the dispute’ (Article 21(2)). Only if an identical dispute to the one at stake ‘has already been resolved’, can they refuse to ‘engage’ with an ODS body. An identical dispute concerns the same information and the same grounds of illegality or incompatibility of content (Article 21(2)). The ODS procedures do not affect judicial or other legal remedies that the eligible parties might have at their disposal (Article 21(1), third sentence).

In my view, the effect of ODS decisions is best described as ‘systemically but not individually binding’. This means that parties can always disregard the individual outcomes but cannot systematically ignore the mechanism without an explanation.

⁹⁶ While the Commission proposal established that online platforms ‘shall be bound by the decision taken by the body’, several Member States (in particular Finland) raised concerns as regards the constitutionality, under their respective legal systems, of a binding system, as it would be interpreted as impeding access to a judge, Commission, ‘COM(2020) 825 Final’ (n 53), art 18(1); Presidency of the Council of the European Union (n 60) 185, 191.

Systematic ignorance of the ODS decisions, which cannot be justified, can lead to a violation of Article 21 of the DSA. Such providers cannot be said to ‘engage in good faith’.⁹⁷ The DSA does not specify the cases in which non-compliance is justified; however, potential examples could be in my view jurisdiction overreach, abuse of the procedure or pending objections to the certification. These are objective reasons. But even if platforms disregard the decisions, they must pay for the procedure if they lose.

While it is true that nothing stops platforms from ignoring the ODS decisions in individual cases, if such instances pile up, they can violate the DSA. For VLOPs, such refusals would be scrutinised very closely in their annual risk assessments, not to mention the impact that refusals can have on public relations and political dimensions. While a refusal to implement an ODS decision can be an important check on possible overreach by the ODS bodies or the failure of DSCs to properly certify the ODS bodies, if platforms have no justification and still refuse to engage, they risk violating Article 21(2) of the DSA.

Nevertheless, the force of the ‘systemically but not individually binding’ effect should not be overstated. Unlike in other areas (eg aviation), the substantive rules are not imposed by the legislature solely. Under the DSA, providers still formulate the terms and conditions of their service. Thus, they largely set the rules of the game, within the boundaries of what is made possible by the otherwise applicable legal system. Even if the decisions were binding, providers could have simply changed the underlying rules at their will. Subject to the applicable legal system, the platforms retain the monopoly on formulating the underlying rules for their services; however, they share the power to interpret their own rules with the ODS experts (and courts).

In other words, providers still hold a pen on their terms and conditions, but going forward, they will cease to have a final word on interpreting their words in more cases.

Judicial or administrative authorities can always arrive at their own interpretation. However, the costs, formality, and speed of such state procedures in many EU countries are unlikely to attract the same amount and type of disputes. This is very similar to how domain name disputes progress in many countries. Domain name ADR decisions are rarely challenged in courts.⁹⁸ Most often, only complex cases go to courts, while ADRs resolve simpler cases. It is even common for ADR bodies to have a special clause in their own procedural rules, which provides that they would suspend self-execution of the ODS decision by a domain name authority in anticipation of an application to the court within a particular time limit.⁹⁹

⁹⁷ Some colleagues argue that good faith efforts only extend to participation but not to outcomes (Saulius Kaleda, Paul-John Loewenthal, and Folkert Wilman, *Digital Services Act: Commentary* (forthcoming, OUP 2024) § 21). I personally find it to be a too narrow reading which undermines the effectiveness of the mechanism. The provision speaks of ‘engag[ing], in good faith, with the selected certified out-of-court dispute settlement body with a view to *resolving the dispute*’. Thus, it appears to me that the scope is broader.

⁹⁸ Annette Kur, ‘UDRP: A Study by the Max-Planck-Institute for Foreign and International Patent, Copyright and Competition Law’ (Max Planck Institute 2002) <https://www.zar.kit.edu/DATA/projekte/udrp_705937a.pdf> accessed 29 August 2023.

⁹⁹ Even in such a system, the period thus stipulated is obviously not binding upon the court. However, it gives a chance to the unsuccessful party to prevent the implementation of an ODS decision.

11.5.6 What qualifies as an ODS body?

The ODS bodies utilised for the purposes of the DSA must be certified by the national DSCs. Each ODS body that fulfils the criteria is issued a certification for a maximum of five years. The certification decision is an administrative decision which should be subject to judicial review on a national level.¹⁰⁰ In the certification process, the ODS body must demonstrate the following:

- a) Its impartiality and independence, including from providers, their users, and notifiers;
- b) Necessary expertise in the subject matter area, such as area of illegal content, terms and conditions of specific services or platforms;
- c) Its members' pay is not linked to the outcome of procedures;
- d) It operates an electronic platform which can handle the disputes;
- e) It is capable of settling disputes in a 'swift, efficient and cost-effective manner' and in at least one of the official languages of the institutions of the EU; and
- f) It adopted 'clear and fair rules of procedure that are easily and publicly accessible'.

Each certification decision specifies the expertise and language(s) of the ODS body. On an annual basis, the ODS bodies report to their DSCs. They must report on their functioning; in particular, the report should at least cover the number of cases, their outcomes, length, and any encountered difficulties. National DSCs can request additional information. The DSCs then use this information to compile bi-annual reports about the functioning of the ODS ecosystem, identifying best practices, and making recommendations for improving the system further (Article 21(4)). The list of eligible ODS bodies will be aggregated and published by the European Commission (Article 21(8)).

Since the ODS bodies must be 'independent' from providers and their users (including content creators and notifiers), the existing ODS forums, such as Meta's Oversight Board, are unlikely to qualify unless they restructure their operations.¹⁰¹ This is because the organisation behind it receives funding from the provider, and some of its members are appointed by it.¹⁰² In contrast, the dispute settlement systems operated by World Intellectual Property Organisation (WIPO), or even many other national bodies designated to operate domain name' dispute systems, are unlikely to have the same problem. These systems are not funded by the domain name authorities

¹⁰⁰ See ECtHR's case law on the issue of the right to a fair trial under art 6 ECHR, *Ramos Nunes de Carvalho e Sá v Portugal* App nos 55391/13, 57728/13, and 74041/13 (ECtHR, 6 November 2018), paras 177–81.

¹⁰¹ For the same view, Aleksandra Kuczerawy, 'Social Media Councils under the DSA: A Path to Individual Error Correction at Scale?' in Matthias C Kettemann and Wolfgang Schulz (eds), *Platform://Democracy: Perspectives on Platform Power, Public Values and the Potential of Social Media Councils* (Leibniz Institut für Medienforschung | Hans-Bredow-Institut (HBI) 2023) <<https://doi.org/10.21241/ssoar.86524>> accessed 4 September 2023.

¹⁰² Oversight Board, 'Governance' <<https://www.oversightboard.com/governance/#governance>> accessed 4 September 2023.

but by complainants. The funding thus does not come from any providers or notifiers. At the time of writing, the WIPO Arbitration and Mediation Centre is preparing its copyright-focused system that it plans to certify in one of the Member States.

11.5.7 Who pays for ODS?

The innovative component of Article 21 is its payment structure. The payment structure of each ODS depends on who sets it up. Only two types of fees are possible: (a) nominal fee or (b) no fee (Article 21(5)). The fee structure must be known upfront. For-profit ODS bodies will likely require a nominal fee paid by the complainant (ie the content creator or notifier). State-funded ODS bodies might require very low nominal fees or offer the ODS at no cost to the complainants. The DSA envisages fees paid by complainants (content creators or notifiers) and providers.

The fees charged shall be reasonable and cannot exceed ‘the costs incurred by the body’. This reference arguably means nothing else other than that the fee must reflect the costs of running the ODS. The original Commission’s proposal was clearer in this respect when it elaborated that ‘[t]he fees charged by the body for the dispute settlement shall be reasonable and shall in any event not exceed the costs thereof’.¹⁰³

Typically, each ODS has two main costs: (1) operational costs of running the digital tools and educating the pool of its experts and (2) costs of experts who decide its individual cases. In domain name ADR bodies, operational costs usually account for one-third of the costs and expert costs are the other two-thirds.

Since the fee structure determines the financial independence of the body and the potential bias of its experts, it should be reviewed as part of the certification process.

In theory, there are four potential fee structures: (a) the complainant pays a nominal fee, (b) the state pays for the entire system, (c) the complainant and provider pay two fees, and (d) only the provider pays a fee. Unlike the first and second options, the last option—provider pays fees for mere participation and no one else pays fees—is likely to undermine the independence of ODS bodies in many cases created by commercial actors. Consider a case where an ODS body charges 0 euros to start a complaint and 200 euros for mere platform participation. Fee shifting (Article 21(5)) in case of success is rendered useless because the punishment for a wrong decision is irrelevant. Such an ODS body would have an incentive to hear many disputes to attract consumers even if it cannot help them. Many fee structures in the third category with very low or merely symbolic nominal fees are likely to have similar problems. While the word ‘nominal’ clearly favours affordability for users, and indicates that the fee should be below the cost of the system, the complainants’ nominal fee should still remain as incentive for better decisions. Without additional safeguards, the fee structures with only provider participation fees or extremely low user fees are inherently prone to abuse. The regulators

¹⁰³ Commission, ‘COM(2020) 825 Final’ (n 53) 54.

should thus review them carefully and undertake stronger monitoring. A fee structure that makes it irrelevant whether the provider wins or loses goes against the logic of fee shifting and compensation in cases of abuse (Article 21(5)).

The fees charged have an important function.¹⁰⁴ Since the fee paid to the ODS must be reimbursed in case of the complainant's success ('in favour of'),¹⁰⁵ this is a small punishment for the provider for its original mistake. At the same time, the risk of losing the fee paid when the complainant is not successful also discourages and filters abusive or meritless appeals since only success is rewarded by reimbursement. The compensation structure partly de-risks the dispute resolution for complainants by making sure that even if the provider prevails, the complainant will not be obliged to reimburse it for its costs; the only exception being an instance of the abusive complainant who 'manifestly acted in bad faith' (Article 21(5)). Such bad actors might be obliged to pay fees and other related reasonable expenses of *providers*.

Any ODS body preparing its fee structure must consider: a) its costs, and b) the demand for its ODS services at distinct price points. The main cost for any ODS body is the labour of experts who prepare their decisions. To improve cost efficiencies, the ODS body can assist experts with technology, and flexible rules that do not require elaborate explanations. However, if stretched too far, both practices can cost the ODS body its certification. At the same time, the higher the fees, the fewer disputes the ODS body is likely to attract because they must convince the future complainant that their services are worth it. As a result, the ODS bodies will need to navigate the trade-offs by tailoring their offerings. One way to do so would be to employ a tiered fee structure that charges according to the type of complainant and effectively cross-subsidises more lucrative disputes (eg e-commerce trader account terminations).

Ultimately, any optimisation of the ODS operations must successfully juggle not only real costs and legally acceptable fee structures but also acceptance of decisions by providers and regulators who certify them. The ODS bodies that tilt too much in one direction can lose their acceptance by providers and thus become less interesting for the complainants who seek to correct the mistakes. If all providers refuse to make decisions with proper justification, they can lose not only interested complainants but also certification.

On the other hand, the state-run free-of-charge ODS system runs a risk of being overwhelmed by complaints that have little prospect of winning, as their complainants do not face the risk of losing the fee. At the same time, such a system can be an important way to incentivise complaints by individuals who have no means or whose complaints have low value to the complainants but have high social significance. In any case, the DSA also provides other ways to support the same goal. By bearing their fees, the state can support similar ODS cases through specialist non-profit independent organisations (Article 86) or trusted flaggers (Article 22). In my view, this approach is preferable because it allows better targeting of support.

¹⁰⁴ For background, Fiala and Husovec (n 17).

¹⁰⁵ DSA, art 21(5).

Apart from the fee itself, Article 21(5) also foresees reimbursement of ‘any other reasonable expenses that [the complainants] have paid’ in case of the complainant’s success. Some have interpreted this to mean that providers will be obliged to pay the full cost of legal representation.¹⁰⁶ In my view, such a reading is not very convincing.

Firstly, unlike in the pre-litigation phase, the ODS does not require legal assistance. The point of the ODS is to get an *expert view*. The fact that the complainant obtained expensive legal assistance cannot mean that such expense is necessary or reasonable, given the merits of the case. Second, given that the DSA places clear limits on fees that an ODS body can charge, it would be inconsistent to allow costs that exceed the fees by several multiples to be reimbursed along with the fee. Any reasonable costs incurred by complainants must be reasonable given the forum (ODS), its costs and legal weight, and the complexity of the case. If the fee costs several hundred euros, the reasonable costs can hardly cost thousands. Thirdly, such ‘reasonable costs’ are not meant to provide a back door to damages caused by the original content moderation decision. Damages must be sought through judicial routes or negotiated settlements. This is again consistent with how similar systems operate in areas such as domain names.

The ODS bodies have no foreseen role in estimating ‘reasonable costs’. This leaves the system with several options: (1) the ODS bodies take over the entire task of cost clearance (fees and reasonable costs), (2) the ODS bodies entirely leave it to the parties to collect compensation from each other, or (3) the ODS bodies only clear the fees but not reasonable compensation. Unless the DSCs express a strong preference, it will be up to the ODS bodies to decide in which configuration they want to operate.

As mentioned, the complainants typically bear the fees charged by the ODS bodies, which are nominal and subject to possible reimbursement. However, an ODS body that does not get any assurances or deposits from the platform risks being unable to collect reimbursements of fees and costs. If an ODS body leaves it to its complainants to collect such monies, this can undermine the attractiveness of the ODS as a service. Successful complainants who were not reimbursed could complain to the DSCs, but their position remains weaker than that of ODS bodies that aggregate many disputes.

It is therefore preferable that the ODS bodies assume the role of complex reimbursement clearance. Without specific agreements with platforms, they could request the platforms to put money corresponding to a nominal fee and capped reimbursement of reasonable costs into an escrow. Thus, as the procedure starts, ODS bodies would have complainants’ and platforms’ contributions secured and only release the funds to the party depending on the success of the dispute. If the platform refused to put the money into escrow, the ODS body would still hear the disputes but warn the complainant about the situation.

In my view, the best outcome would be if the ODS body assumes the full role of fee reimbursement but caps the reasonable costs at the percentage of the original fee

¹⁰⁶ Daniel Holznagel, ‘A Self-Regulatory Race to the Bottom through Out-of-Court Dispute Settlement in the Digital Services Act’ (*Verfassungsblog*, März 2022) <<https://verfassungsblog.de/a-self-regulatory-race-to-the-bottom-through-art-18-digital-services-act/>> accessed 4 September 2023. In my view, such interpretation could easily stumble upon constitutional limits and is thus less likely to be favoured by the courts.

(eg 50%). This allows the ODS bodies to better adjust the expectations of the complainants because they know how much they can get reimbursed in the event of success. If the winning party thinks it is owed more, it can always try to seek such an amount bilaterally. The ODS bodies could specify in their rules under which conditions they recognise such reasonable costs (eg engagement of an expert, evidence, or other expenses).

The question remains about resolving cases where providers are unwilling to put the money into an escrow. The dilemma is as follows. If platforms lose the cases, they ought to pay to complainants. If the ODS bodies leave it to the platform-complainant relationship, the issue remains that this can undermine confidence in the system. If ODS bodies absorb the loss and try to collect money from the platforms, they assume additional risks and can potentially undermine their own independence.

Lastly, the DSA does not specify how the fee reimbursement rules apply when success is only partial. Since Article 21 employs the phrase ‘in favour of’, the fee reimbursement should take place regardless of the amount of success. However, ‘reasonable expenses’ could be arguably adjusted for the scope of success.

11.5.8 What is a fair ODS procedure?

While the exact fashioning of the procedure is in the hands of the ODS bodies, it must comply with the DSA and other applicable laws. Article 21(3)(f) states that: ‘the out-of-court dispute settlement that it offers takes place in accordance with clear and fair rules of procedure that are easily and publicly accessible, and that comply with applicable law, including this Article.’ Thus, the overarching criterion for procedural rules is that of fairness. There are very few explicit rules that the ODS bodies must follow.

Their decisions must be made available to the parties within a reasonable period not exceeding 90 days after receiving the complaint. Only exceptionally, in very difficult cases, can the period be extended to 180 days (Article 21(4)). The process takes place entirely online. The ODS bodies can flexibly design other questions. Thus, the DSCs will need to assess the fairness of the proposed procedural rules holistically. Such rules clearly need to be part of the application for certification.

The DSA does not even specify who shall be invited to participate in such disputes. It is clear that the platform and the complainant must be part of the procedure. However, how about content creators whose account the notifier is contesting or a notifier whose notification content creator is contesting? The DSA does not require their presence. One can argue that it is in the platform’s best interest to engage such parties because providers are in danger of losing the case and having to pay. That said, including such parties can also be very difficult for the ODS bodies logistically. The simplest way to approach this would be for the ODS bodies to generally proceed without further parties but incentivise the platforms to collect such views and/or open up the process to such parties to comment on the submitted disputes.

However, the ODS bodies are likely to view any additional procedural turns as a costly exercise. The DSA does not even ban secrecy; thus, the ODS bodies can easily opt for secret, or semi-secret decision-making that is cheaper to operate. This, per se, is not a problem as long as the ODS bodies retain some level of accountability for how they decide the disputes (eg through high-level summaries and collection of detailed statistics that the DSCs will need). Some level of secrecy can be an enhancing feature for certain disputes, but it can also be counterproductive for other complainants, especially if they lose and are bound by strict non-disclosure rules. Preferably, the complainants should always have a choice if they want to have their procedure subject to secrecy or not.

11.5.9 What can an ODS body decide?

The ODS body can only decide to *undo* the platform's decision. It cannot award damages or order some other specific performance. While nothing stops ODS bodies from making recommendations, these have little legal consequences for the providers. Such recommendations can have, however, some legal value for regulators (eg to assess their compliance with Article 14). The findings of the ODS bodies thus can also feed into the annual risk assessment. They can also file complaints before the DSCs if they observe some problematic behaviour.

If the ODS bodies take over the task of cost clearance, they can make decisions about the fee and reasonable cost compensation. They could also make decisions about the presence of bad-faith actors. If the money is put into escrow by all the parties, cost clearance is made much more efficient. Thus, the clearance model of the ODS could be beneficial even to online platforms because they can easily enforce cost reimbursement against bad actors who try to abuse the ODS process.

11.5.10 What if an ODS body becomes a rogue?

The certification process should ensure that the ODS bodies have sufficient expertise and independence. However, the DSCs should be aware that the ODS bodies could try to abuse the system. For instance, one can imagine the possible emergence of ODS bodies that are ideologically biased and only hire experts who decide in a particular direction and then market themselves as such (eg right-wing or left-wing friendly ODS bodies) or ODS bodies who encourage their experts to decide against providers, attract complainants, and collect their reimbursements.

The DSA places several safeguards in place to prevent this. The system of checking balances relies upon the ODS bodies, platforms, and DSCs that constantly look over each other's shoulders to work.

First, the DSCs are tasked to continuously review the independence of the ODS bodies and their internal fee and payment structure. They can revoke the certification

at any point, following their own investigation or complaints of third parties (Article 21(7)). Second, the DSCs should receive a steady stream of reports, including how the cases are handled, so any bias can be detected relatively early, especially when the DSC benchmarks results against those of the other ODS bodies. Third, the providers obliged to 'engage in good faith' with the ODS bodies might refuse to implement their decisions with the argument that the decisions are not impartial until a DSC decides about the pending investigation of an ODS body.

While the DSA leaves providers with no room for withholding the reimbursement of fees, if an ODS body loses its certification, it might arguably equally lose its due fees. The DSA does not deal with this situation. The reimbursement owing in case of loss of certification might depend on the date from which the certification is lost. The DSCs could, in theory, backdate their decisions to the point when the evidence of abuse exists to prevent rogue ODS bodies from reaping any benefit. Alternatively, it could fine the rogue ODS body and distribute the fines as compensation to the affected parties.

The DSA does not address the question of liability for damages under national law. However, if an ODS body runs a system in accordance with its rules and certification, it clearly cannot be liable to the providers or other actors for its functioning. However, if an ODS body loses such certification due to abuses of the process, the potential liability is probably not pre-empted by the DSA.

11.6 Conclusion

Articles 16–21 only focus on procedural fairness. Their goal is to impose minimum standards of due process on companies that annually handle billions of decisions about Europeans. The discussion has shown that while the DSA is marked by some imprecisions and potentially ambiguous language, the general direction of travel is very sensible. Obviously, whether and how the system will eventually work is an empirical question that I can hardly properly evaluate before the framework is used. One of the critical issues will be to educate and convince individuals to use their newly gained rights.

Fair Content Rules

12.1 Introduction	249	12.3.4 Rules vs design	262
12.2 General Explainability of Content Moderation (Article 14(1))	249	12.3.5 Impact on non-platform services	263
12.3 Fairness of Content Rules (Article 14(4))	253	12.4 Safeguards Against Abuse by Users and Notifiers (Article 23)	265
12.3.1 Three views on proportionality	255	12.4.1 Prior warning	265
12.3.2 Contractual consequences	259	12.4.2 Scope and conditions	267
12.3.3 Precision vs administrability of rules	260	12.5 Conclusions	268

12.1 Introduction

The previous chapter focused on procedural rules. But the Digital Services Act (DSA) also contains several provisions that shape the substantive content rules that providers can set for their users—Articles 14 and 23. Article 14(1) obliges companies to publicly state and explain their content restrictions. Article 14(4) makes their enforcement subject to fundamental rights scrutiny. Article 23 prescribes the minimum rules for users who misuse their system. This chapter will tease out the implications of these provisions, and how they interact with the rest of the DSA. My overarching argument is that these provisions embody the fairness principle that applies to three basic dimensions of content moderation: how rules are drafted, explained, and enforced.

12.2 General Explainability of Content Moderation (Article 14(1))

In the early days of now-large social media platforms such as Facebook or Twitter, these providers would have a few standards to moderate their users' content. The main ethos in the early 2000s was often organised around the principle—'if it makes you feel bad in your gut, then go ahead and take it down.'¹ Over the years, with the size of companies

¹ Kate Klonick, 'The New Governors: The People, Rules, and Processes Governing Online Speech' (2018) 131 Harvard Law Review 1598, 1631, quoting one of the early content moderators at Facebook but her work also documents other social media. For the history of Twitter, Emillie de Keulenaar, João C Magalhães, and Bharath Ganesh, 'Modulating Moderation: A History of Objectionability in Twitter Moderation Practices' (2023) 73(3) Journal of Communication 273.

and their user base, the size of the rule book grew more complicated and detailed. Not all of the rules were made public. Companies would routinely keep additional details of their policies internally. For instance, Yoel Roth, a former Twitter employee, describes how Twitter used to have a three-insult rule on top of its official policy on abusive behaviour.² When Facebook's internal guidelines for content moderators leaked in 2012, many commented on the absurdity of the long and detailed rules.³ Radiolab most vividly documented Facebook's journey when trying to refine its policy about the depiction of female nipples, explaining the problems companies face on daily basis.⁴ The current community guidelines of Facebook are almost 19,000 words long.⁵ In contrast, the DSA is around 64,000 words.

The DSA tries to bring some order to these practices. According to Article 14:

- (1) Providers of intermediary services shall include *information on any restrictions* that they impose in relation to the use of their service in respect of information provided by the recipients of the service, *in their terms and conditions*. That information shall include information on any policies, procedures, measures and tools used for the purpose of content moderation, including algorithmic decision-making, and human review, as well as the rules of procedure of their internal complaint handling system. *It shall be set out in clear, plain, intelligible, user-friendly and unambiguous language, and shall be publicly available in an easily accessible and machine-readable format.*
- (2) Providers of intermediary services shall inform the recipients of the service of any significant change to the terms and conditions.⁶

All providers of intermediary services, therefore, must *codify*⁷ their content moderation rules and *notify* any significant changes. These requirements represent a change in how policies concerning certain decisions, such as mere visibility restrictions, are explained. For instance, as illustrated by Leerssen,⁸ secret moderation techniques such as shadow-banning (eg hiding one's content) or shadow privileges (eg granting immunity),⁹ are generally incompatible with the DSA.¹⁰ While in theory, Article 14(1)

² Yoel Roth, 'Content Moderation's Legalism Problem' (*Lawfare*, 24 July 2023) <<https://www.lawfaremedia.org/article/content-moderation-s-legalism-problem>> accessed 3 September 2023.

³ Tarleton Gillespie, 'The Dirty Job of Keeping Facebook Clean' (*Social Media Collective*, 22 February 2012) <<https://socialmediacollective.org/2012/02/22/the-dirty-job-of-keeping-facebook-clean/>> accessed 3 September 2023.

⁴ Radiolab podcast, 'Post No Evil' (*Radiolab*, 17 August 2018) <<https://www.radiolab.org/podcast/post-no-evil>> accessed 3 September 2023.

⁵ Meta, 'Policies | Transparency Centre' <<https://transparency.fb.com/en-gb/policies/>> accessed 3 September 2023.

⁶ Emphasis mine.

⁷ Paddy Leerssen, 'An End to Shadow Banning? Transparency Rights in the Digital Services Act between Content Moderation and Curation' (2023) 48 *Computer Law & Security Review* 105790.

⁸ *ibid.*

⁹ Jeff Horwitz, 'Facebook Says Its Rules Apply to All Company Documents Reveal a Secret Elite That's Exempt' *The Wall Street Journal* (New York, 13 September 2021) <<https://www.wsj.com/articles/facebook-files-xcheck-zuckerberg-elite-rules-11631541353>> accessed 3 September 2023.

¹⁰ Also Franz Hofmann and Benjamin Raue (eds), *Digital Services Act: Gesetz über digitale Dienste* (1. Auflage, Nomos 2023) 250.

only requires the disclosure of their existence and underlying rules, the subsequent individual statement of reasons issued under Article 17(1) makes it impossible to keep their application secret from the specific affected users. The codification and notification principles are meant to assure that the public can infer what restrictions apply to their content and behaviour on a particular service upfront.

Article 14(1) does not prescribe how specific the rules must be. For instance, it is unclear whether the disclosure about the harassment policy must state all the tiny details. In general, if a rule is applied, it must be disclosed. However, the wording of ‘information on any restriction’ provides some leeway for providers to be less specific about their security-sensitive rules, such as spam filters. Moreover, Article 14(1) applies also to restrictions that are not based on explicit rules (eg weights given to information to evaluate attractiveness). What Article 14(1) clearly bans is withholding information about the *existence* of some types of restrictions. Arguably, given the rule is one of general explainability of restrictions, the standard should be somewhat lower than under individual explainability according to Article 17(1).

The standard is defined as ‘clear, plain, intelligible, user friendly and unambiguous language’ (Article 14(1)). Where the service is directed at minors, the language must be further adjusted for the audience (Article 14(3)). Consider the following two rules:

Everyone is protected from: Repeated contact which is: Unwanted, or Sexually harassing, or Directed at a large number of individuals with no prior solicitation.

People can’t bother you again and again, be mean, or message lots of others without permission. It’s about feeling safe.

The first rule is an official rule applied by Facebook.¹¹ The second is ChatGPT’s brief version for a 10-year-old. Undeniably, for a lawyer, they express slightly different boundaries. At the same time, they seem to encapsulate the same goal well: avoidance of harassment. Since the DSA insists on ‘plain’ language even for adults, it can only be as ‘unambiguous’ as the language itself. In my view, the DSA hardly prescribes detailed lists of factors or full disclosure of content moderation manuals under Article 14(1). The key quality that they must satisfy is *reasonable predictability*.

This standard was first employed under Recital 15 of the Platform to Business Regulation (P2BR), a pioneering piece of EU legislation in this space of platform fairness and transparency, albeit only targeted at protecting businesses. It gives further context to Article 3(1) of the P2BR, which prescribes that terms and conditions must be drafted in ‘plain and intelligible language’. As explained by Recital 15 of the P2BR:

Terms and conditions should not be considered to have been drafted in plain and intelligible language where they are vague, unspecific or lack detail on important

¹¹ Meta, ‘Bullying and Harassment | Transparency Centre’ <<https://transparency.fb.com/en-gb/policies/community-standards/bullying-harassment/>> accessed 3 September 2023.

commercial issues and thus fail to give business users a reasonable degree of predictability on the most important aspects of the contractual relationship.

Although the DSA does not have a comparable recital, its ultimate goal is establishing a ‘safe, *predictable* and trusted online environment’ (Article 1(1) DSA). While the obligation under the P2BR aims to prevent ‘unfair behaviour to the detriment of business users’ (Recital 18 P2BR), under the DSA, Article 14(1) extends this logic to any other recipient of the service, including consumers. Furthermore, the benchmark for reasonability under the DSA is an average user.¹² Thus, the concept might be different when applied to business users and when applied to consumers.

The DSA also does not reiterate Recital 15 P2BR’s detail about ‘most important aspects’. However, realistically, it is impossible to disclose everything in a way that would be still intelligible. Thus, providers can keep most of it internal, provided they do not withhold significant details. If the existence of rules is disclosed in their key features, which make the rights and obligations in the relationship sufficiently foreseeable, compliance with Article 14(1) is likely.¹³

In contrast, a rule saying ‘we block everything that is caught by our hate speech filters’, is unlikely to meet the threshold. From such a description, an average user is unable to infer what must be done to avoid being blocked. For the same reason, companies cannot simply incorporate ‘catch-all clauses’, such as ‘we reserve a right to block your content when we think it does not fit our services’, or ‘when we are faced with regulatory risks’. Such clauses would not be predictable, as they are not organised around anything that the user can understand and comply with.

Article 14(1) can be arguably analogised to the ‘prescribed by the law’ requirement found in European human rights case law. In the Strasbourg jurisprudence, each restriction of rights must be based on rules that are sufficiently foreseeable for their addressees. Such foreseeability can differ by area; however, the rules should be ‘sufficiently clear in its terms to give individuals an adequate indication as to the circumstances in which and the conditions on which [providers] are empowered to resort to any such measures.’¹⁴ The standard applied to platforms can naturally be more relaxed than the one applied to state actors; however, the logic remains similar.

Any restriction of content—the rule and its sanction—needs a legal basis either in the legal norm that stipulates illegality, or a contractually agreed provision. If a legal basis is missing, the restriction is arbitrary and will violate Article 14(1) due to lack

¹² This point is made by Hofmann and Raue (n 10) 260.

¹³ Ofcom, the UK regulator, recently undertook a study of video-sharing platforms concerning the ease of reading their terms and conditions, Ofcom, ‘Many Adults Would Struggle to Understand Video-Sharing Platforms’ Rules - Kids Have Even Less Chance’ (9 August 2023) <<https://www.ofcom.org.uk/news-centre/2023/video-sharing-platforms-rules-kids>> accessed 3 September 2023; for an archive of the policies, ‘An Archive of Social Media Platforms’ Content Moderation and Legal Policies’ (*Platform Governance Archive*) <<https://www.platformgovernancearchive.org/>> accessed 3 September 2023.

¹⁴ *Roman Zakharov v Russia* App No 47143/06 (ECtHR, 4 December 2015), para 229; the original cites public authorities instead of providers.

of disclosure and potentially Article 14(4) because it baselessly restricts the rights of others. What is disclosed *ex ante*, influences what is justified *ex post*.¹⁵

12.3 Fairness of Content Rules (Article 14(4))

When Donald Trump was permanently banned by social media following the insurrection in Capitol Hill,¹⁶ the then-German-chancellor, Angela Merkel, criticised the decision as ‘problematic.’¹⁷ Thierry Breton, European Commissioner for the Internal Market and a political face of the DSA was even more explicit in his criticism by stating that: ‘the fact that a CEO can pull the plug on POTUS’s loudspeaker without any checks and balances is perplexing’.¹⁸

So, does the DSA take away the power of social media and other digital providers to do the same again? Yes and no. The DSA’s content moderation due diligence obligations discussed in Chapter 11 demand the implementation of extensive due process obligations. Donald Trump would have had many remedies that he could invoke, such as internal and external appeals. These remedies represent the most obvious checks and balances on platforms’ power. At the same time, they do not directly dictate whose accounts can and cannot be terminated and for how long. The power to formulate rules stays with platforms. Articles 14(4) and 23 are two key exceptions to this rule of contractual freedom.

According to Article 14(4):

Providers of intermediary services shall act in *a diligent, objective and proportionate manner in applying and enforcing the restrictions* referred to in paragraph 1, with due regard to the rights and legitimate interests of all parties involved, including the fundamental rights of the recipients of the service, such as the freedom of expression, freedom and pluralism of the media, and other fundamental rights and freedoms as enshrined in the Charter.¹⁹

The European Commission initially conceived the provision as an umbrella ‘fundamental rights by design’ provision.²⁰ The European Parliament then tried to give it

¹⁵ A similar point is made by Hofmann and Raue (n 10) 250.

¹⁶ Ben Collins and Brandy Zadrozny, ‘Twitter Permanently Suspends President Donald Trump’ *BBC News* (London, 8 January 2021) <<https://www.nbcnews.com/tech/tech-news/twitter-permanently-bans-president-donald-trump-n1253588>>.

¹⁷ Pierre-Paul Bermingham, ‘Merkel Among EU Leaders Questioning Twitter’s Trump Ban’ *Politico* (Arlington County, 11 January 2021) <<https://www.politico.eu/article/angela-merkel-european-leaders-question-twitter-donald-trump-ban/>> accessed 3 September 2023.

¹⁸ Thierry Breton, ‘Thierry Breton: Capitol Hill — the 9/11 Moment of Social Media’ *Politico* (Arlington County, 10 January 2021) <<https://www.politico.eu/article/thierry-breton-social-media-capitol-hill-riot/>> accessed 3 September 2023.

¹⁹ Emphasis mine.

²⁰ *Interview with Irene Roche Laguna*, Deputy Head of Unit for Coordination and Regulatory Compliance, European Commission (2021–23).

further explicit framing as a fairness rule.²¹ While this proposal of the Parliament was not adopted, in Recital 45, the DSA states that:

Whilst the freedom of contract of providers of intermediary services should in principle be respected, it is appropriate to set certain rules on the content, application and enforcement of the terms and conditions of those providers in the interests of transparency, the protection of recipients of the service and *the avoidance of unfair or arbitrary outcomes*.

Fairness is also mentioned in Recital 58, where the DSA states that providers must ensure ‘swift, non-discriminatory, non-arbitrary and fair outcomes’ in the context of internal appeals. This suggests that the overarching criterion remains fairness to users and others.

Regardless of labels, Article 14(4) is first and foremost a provision that should positively influence the interpretation of other provisions of the DSA as an ever-present North Star. The provision applies to illegal content and contractual breaches alike and to all services envisaged by the DSA. It, therefore, acts as a sort of general clause against unfair treatment by providers. Thus, even if a provider does not violate one of the explicit requirements of the DSA, it could still be in breach of its general fairness requirement in Article 14(4).

Thus, from a fundamental rights perspective, Article 14(4) invites an indirect effect of fundamental rights.²² From the regulatory perspective, it is a catch-all clause for all services regulated by the DSA, even if only lightly. And finally, from civil society’s perspective, it is an anchor for arguments that content moderation decisions of companies should not be solely guided by profit.

Technically, Article 14(4) only provides that ‘providers of intermediary services shall act in a diligent, objective and proportionate manner in *applying and enforcing the restrictions*’.²³ Thus, the provision does not mention the drafting of the rules, only their application and enforcement. However, an interpretation that excludes drafting is unlikely to be convincing.²⁴ Firstly, Recital 47 which accompanies the article clearly anticipates broader use, explaining that ‘[w]hen *designing*, applying and enforcing those restrictions, providers of intermediary services should act in a non-arbitrary and non-discriminatory manner and take into account the rights and legitimate interests of the recipients of the service, including fundamental rights as enshrined in the Charter’. Similar references can be found elsewhere in the DSA (eg in Recital 51, which speaks

²¹ It proposed changing the language to ‘use fair, non-discriminatory and transparent’; see European Parliament, ‘Amendments adopted by the European Parliament on 20 January 2022 on the proposal for a regulation of the European Parliament and of the Council on a Single Market for Digital Services (DSA) and amending Directive 2000/31/EC (COM(2020)0825 — C9-0418/2020 — 2020/0361(COD))’ [2022] OJ C336/48, amendment 513.

²² João Pedro Quintais, Naomi Appelman, and Ronan Ó Fathaigh, ‘Using Terms and Conditions to Apply Fundamental Rights to Content Moderation’ (2023) 24(5) German Law Journal 881, 910. Also ch 3.

²³ Emphasis mine.

²⁴ The same conclusion is drawn by Quintais, Appelman, and Ó Fathaigh (n 22) 894 (‘the obligation applies not just to the application and enforcement of restrictions, but also to its design’); Hofmann and Raue (n 10) 253.

of ‘any action taken by a provider of hosting services pursuant to receiving a notice should be strictly targeted’).

Second, Article 20 foresees internal appeals explicitly expands the review to the questions of whether ‘the complainant’s conduct does not warrant the measure taken.’²⁵ Finally, if a rule imposing a restriction is disproportionate, no sanction imposed on its basis can be proportionate. Thus, limiting reviews only to enforcement and application must clearly affect the provider’s design and drafting of the underlying content rules.

Under Article 14(4), content moderation restrictions must also meet the following standards: diligence, objectivity, and proportionality. Recital 47, however, refers to these requirements as non-arbitrariness and non-discrimination. Additionally, it is mentioned in Article 20(4) that the internal appeals must be non-discriminatory, diligent, and non-arbitrary. The DSA certainly mentions many noble concepts one can think of. Arguably, objectivity and non-arbitrariness are the same standard. It means that every restriction needs a previously disclosed legal basis. Thus, retroactive restrictions or punishments without crime are unlikely to comply with Article 14(4). Non-discrimination is self-explanatory. In the DSA’s context of private bureaucracies, the key notion that it will push for is reasonable consistency.

Diligence likely overlaps largely with good faith, although both terms are used next to each other in other parts of the DSA such as Article 7. In fact, the DSA uses the word ‘diligent’ or ‘diligently’ as standard 20 times across the text.²⁶ Yet, little can be said about its self-standing meaning. Even though the standard of a ‘diligent economic operator’ has been known to existing case law on the E-Commerce Directive,²⁷ its meaning has never been defined beyond some indications that this should be a business that acts in good faith and with an appropriate level of care to attend the affairs of others. Until the Court clarifies the concept, the concept’s added value will be questioned.

12.3.1 Three views on proportionality

The most nebulous of all, however, is proportionality. Proportionality, of course, is the key component of the human rights system.²⁸ The way proportionality is conceptualised in Article 14(4) will determine its level of prescriptiveness. Three basic views can be already anticipated: the rights-maximalist view, the fairness view, and the pro-business view.

The rights-maximalist view will argue that all decisions of providers which are subject to the provision shall be made subject to the same standards as those applicable

²⁵ Art 20(4) DSA.

²⁶ This excludes references to due diligence obligations.

²⁷ Chs 6–7.

²⁸ Kai Möller, ‘Proportionality’, *The Global Model of Constitutional Rights* (OUP 2012); Jacco Bomhoff, ‘Proportionality in Comparative Law’ [2022] LSE Legal Studies Working Paper No 03/2022, forthcoming as an entry on ‘Proportionality’ in the Elgar Encyclopedia of Comparative Law (2nd edition), Jan Smits, Catherine Valcke, Jaakko Husa, and Madalena Narciso (eds) <<https://papers.ssrn.com/abstract=4063283>> accessed 3 September 2023.

to the state. As a result, they would adopt a very prescriptive reading of the provision, which allows Article 14(4) to actively intervene in content moderation policies and their design. The pro-business view, on the other hand, will likely argue that the provision hardly amounts to any binding legal standards, and has a mostly declaratory character. Thus, Article 14(4) should be construed more as interpretation guidance than a real filter of acceptable policies. Finally, the middle ground between the two, the fairness view, which I find most convincing, would argue that Article 14(4) does not submit non-state entities to legal standards applicable to state actors. Instead, in respecting contractual freedom, the provision allows a range of fair outcomes that are acceptable and only outlaws those that grossly disregard any fairness to others, including their fundamental rights.

The adoption of a particular reading has practical consequences. Consider the following two policies:

- (1) A micro-blogging site decides to create a list of VIPs whose content is not moderated at all (regardless of illegality or contractual nature). VIPs are all top elected officials in countries of the UN.
- (2) A micro-blogging site decides to launch a new product. For €5 a month, users can say whatever they want on the service, as long it is legal in their country. Usual contractual restrictions, such as those on disinformation, nudity, and vulgar content will not apply to them.

The first policy tries to exempt some persons from the moderation of illegality. Such policy will likely be seen as against Article 14(4) in both the rights-maximalist and fairness views. For both, the provision tries to do an illegitimate thing—ie to exempt some individuals from the rules adopted by the parliament. From the pro-business view, Article 14(4) might be considered superfluous. The proponents of the view would probably argue that such a policy is unlikely to be adopted because the company risks losing the liability exemption.

In contrast, the second policy is likely to split the view differently. The rights-maximalist view is likely to see the practice as problematic because it discriminates between groups of individuals and grants broader rights to some at the expense of others. The fairness view, in the absence of additional circumstances, is likely to accept the outcome, with the argument that everyone can opt into the class if they pay the fee. However, with some additional context (eg if the provider at stake is a very large online platform (VLOP)), the assessment might change to become more prescriptive. Finally, the pro-business view would see this as non-problematic and guaranteed by the freedom to conduct business.

The key difference between the rights-maximalist and fairness views is in the intensity of the legal review. The fairness view only intervenes to moderate gross disproportionality, such as retroactivity, punishment without rules, or other extreme unfairness, while the right-maximalist view is willing to intervene whenever the balance of rights is not exactly right. Let me illustrate it with another example:

Meta's Oversight Board overturned Facebook's decision to remove content in which a user posted a quote incorrectly attributed to Joseph Goebbels, Minister of Propaganda in Nazi Germany.²⁹ Facebook removed the content since it considered it to have breached the Community Standard on Dangerous Individuals and Organizations as it evoked a dangerous individual without explicitly distancing himself. According to Facebook's publicly published rules as reproduced in the case decision, Facebook will remove any content that supports or praises 'groups, leaders or individuals involved in these activities.' However, internally, their policy was said to read, 'Facebook *treats* all content that supposedly quotes a designated dangerous individual *as an expression of praise or support* for that individual *unless the user provides additional context to make their intent explicit*.'³⁰ The Board, after reviewing the context of the user's account, concluded that the user did not intend to praise or support the Nazi party, and that comment sought to draw comparisons between the presidency of Donald Trump and the Nazi regime.³¹ The Board considered that the policies lack clarity, including a failure to explain key terms.

From the DSA's perspective, one can debate its compliance with Article 14(1). It is likely that the internal rules should have been disclosed upfront to inform users of the additional, but crucial, detail. For Article 14(4), the result depends on one's reading. From a fairness view, the provision is unlikely to be violated by a rule that states that whoever quotes a dangerous individual and does not explicitly distance himself or herself, will be removed. The policy might be imprecise, but its rule is foreseeable and defensible. From a rights-maximalist view, the policy, even if compliant with Article 14(1), could still be problematic because it suppresses some legal speech as a result of an overly cautious policy against extremists.

Finally, consider Donald Trump's example. His Facebook account was blocked 'indefinitely and for at least the next two weeks until the peaceful transition of power is complete.'³² While Meta's Oversight Board agreed that Facebook's policies had been violated, it found, however, that the remedy had been arbitrarily applied and that 'it was not appropriate for Facebook to impose an indefinite suspension.'³³ From the rights-maximalist view, Article 14(4) could be read as prohibiting any indefinite bans due to their undifferentiated character. From the fairness view, Article 14(4) would step in only if the ban was grossly disproportionate to the actions; eg if the violations that triggered the indefinite ban were only minor. Thus, the two readings give different deference to the providers.

²⁹ Oversight Board, 'Nazi Quote – Case Decision 2020-005-FB-UA' (2020) <<https://www.oversightboard.com/decision/FB-2RDRCVQ#>> accessed 3 September 2023.

³⁰ Emphasis mine.

³¹ Oversight Board, 'Nazi Quote – Case Decision 2020-005-FB-UA' (n 29).

³² Oversight Board, 'The Oversight Board Upholds Former President Trump's Suspension and Finds That Facebook Failed to Impose Proper Penalty' (May 2021) <<https://www.oversightboard.com/news/226612455899839-oversight-board-upholds-former-president-trump-s-suspension-finds-facebook-failed-to-impose-proper-penalty/>> accessed 3 September 2023.

³³ Oversight Board, 'Former President Trump's Suspension - Case Decision 2021-001-FB-FBR' (2021) <<https://www.oversightboard.com/decision/FB-691QAMHJ>> accessed 3 September 2023.

At the time of writing, it is unclear how the Court will develop Article 14(4). I find the fairness view more convincing because it reflects the ability of providers to set their own rules. If the providers were fully assimilated into the test for state actors, many sensible contractual policies, such as those on disinformation, can become illegal under Article 14(4). The goal of the provision should be to give breathing space for experimentation by providers, especially in light of their obligations to mitigate the risks if they are very large. If this option is closed off by very strict interpretation, many interventions that could mitigate risks might become impossible. This is not to say that Article 14(4) might *require* platforms to outlaw what is not illegal. Rather, it simply might *allow* them to do so if they see fit. The fairness view only imposes constraints on the margins of such experimentation.

To conclude, in my view, Article 14(4) constrains private power by outlawing extremely (grossly) unfair uses of that power but does not step in every single time the balance reached would have been slightly off-kilter if placed in the context of state actors. Such understanding of Article 14(4) is still a bold step because it moves beyond sector-specific attempts to rebalance the various power asymmetries.

This limited approach to the review of content moderation rules has been already adopted before the DSA by the courts in some of the Member States.³⁴ Several additional arguments can be made in its favour. The DSA's starting point is the providers' freedom of contract (Recital 45).³⁵ Any rules proclaimed to be disproportionate come on top of other applicable mandatory rules that rely on more than simple proportionality tests, such as the Unfair Contract Terms Directive, the Unfair Commercial Practices Directive, or the P2BR. The sectorial contractual rules include special requirements as to what sanctions are acceptable for what type of user conduct breaches the contract. For instance, the P2BR prescribes a 30-day waiting period for the termination of accounts, although with some exceptions, including legally prescribed actions.³⁶ If Article 14(4) receives a very prescriptive meaning, these other rules can be easily displaced.

³⁴ For instance, the German courts held that the dominant social network has broad leeway on how to design its rules, but it must respect some basic procedural rights, interpret rules in light of fundamental rights, and avoid arbitrariness of its decisions (German Federal Supreme Court, BGH v 29.07.2021—III ZR 179/20 and III ZR 192/20). For discussion, Mauritz Hennemann and Amelie Heldt, 'Prozedurale Vermessung: Das Kuratieren Kommunikativer Räume Durch Soziale Netzwerke Zugleich Besprechung von BGH, Urteile vom 29.7.2021—III ZR 179/20 und III ZR 192/20' (2021) 65 ZUM 981; Matthias C Kettemann and Torben Klaus, 'Regulating Online Speech: Ze German Way' (*Lawfare*, 20 September 2021) <<https://www.lawfaremedia.org/article/regulating-online-speech-ze-german-way>> accessed 3 September 2023. Italian and Dutch courts adopted a similar approach in *Forza Nuova v Facebook Ireland NTD*, Case No 64894/2019 [2020], *Facebook v CasaPound*, Case No 80961/19 [2020] and *Rechtbank Noord-Holland, Van Haga/LinkedIn*, Case No ECLI:NL:RBNHO:2021:8539. For comparative work, Berdien van der Donk, 'Digital bouncers. A European roadmap to navigate online access rights and moderation issues' (PhD thesis, University of Copenhagen 2023).

³⁵ Rec 45 DSA states that '[w]hilst the freedom of contract of providers of intermediary services should in principle be respected, it is appropriate to set certain rules on the content, application and enforcement of the terms and conditions of those providers in the interests of transparency, the protection of recipients of the service and the avoidance of unfair or arbitrary outcomes.'

³⁶ Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services [2019] OJ L186/57 (P2BR), Art 4(2).

12.3.2 Contractual consequences

Unlike the P2BR, the DSA does not address the question of legal consequences within contractual relationships if Articles 14(1) or (4) are violated. In contrast, the business-oriented P2BR and the consumer-oriented Unfair Contract Terms Directive, both state the result is invalidity of such clauses.³⁷ The mechanism under P2BR is explained succinctly in Recital 20 P2BR as follows:

In order to protect business users and to provide legal certainty for both sides, non-compliant terms and conditions should be null and void, that is, deemed to have never existed, with effects *erga omnes* and *ex tunc*. This should however only concern the specific provisions of the terms and conditions which are not compliant. The remaining provisions should remain valid and enforceable, in as far as they can be severed from the non-compliant provisions. Sudden changes to existing terms and conditions may significantly disrupt business users' operations. In order to limit such negative effects on business users, and to discourage such behaviour, changes made in contravention of the obligation to provide a set notice period should therefore be null and void, that is, deemed to have never existed, with effects *erga omnes* and *ex tunc*.

In my view, the effectiveness of the DSA requires that a violation of Article 14 leads to the same consequences.³⁸ Otherwise, the EU rules would create a curious split between regimes, where the affected parties would have to argue the parallel applicability of the business-oriented P2BR and the consumer-oriented Unfair Contract Terms Directive to give them protection against terms deemed illegal under the DSA. Thus, Article 3(3) P2BR should apply by analogy to violations of Article 14(4) DSA.

In practical terms, this means that an illegal clause (eg 'we block everything that is caught by our hate speech filters') is null and void, and not considered to exist from the very start. This has key consequences for content moderation sanctions, as rules that are not properly stipulated, are always arbitrary. Similarly, sanctions that are excessive given the underlying rule (eg 'we reserve a right to block your account for any violation of these terms, regardless of severity'), are then equally without legal basis in the contract. Thus, if they cannot be based on illegality, they are arbitrary.

This has profound consequences for external appeals. Because the Out-of-Court Dispute Settlement (ODS) bodies are bound by the DSA, legislation, and rules drafted by providers, they must respect the norms as they find them. However, Articles 14(1) and (4) give them the rare ability to review the contents of such rule books. The main utility of this will come from the review of rules that order legal content. As argued in Chapter 11, the ODS bodies do not have the legitimacy or empowerment to question

³⁷ Unfair Contract Terms Directive, art 6; P2BR, art 3(3).

³⁸ Similar point is made by Hofmann and Raue (n 10) 253, 263.

the constitutionality of the legislature's rules. However, for clashes of private rules with legislation, such as Article 14, their position is much stronger. The ODS bodies could rule in favour of users on the grounds that a particular sanction was not validly incorporated into the contract or lacks sufficient predictability to be enforced against users. While providers might reject following this, if such conclusions are drawn by several bodies, the indication is strong that they violate the DSA, including their obligations under Article 21 DSA. Moreover, users can invoke their right for the put back of their content (Article 20(4)) before the courts.

12.3.3 Precision vs administrability of rules

The DSA is likely to facilitate the standardisation of content moderation processes and thereby the increased outsourcing of the tools that feed into systems used by providers. However, such standardisation represented by key standards and procedures of the DSA is likely also to impact how providers draft their rules in the first place.

For providers, the key trade-off is between *precision* and *administrability*. By precision, I mean the ability of providers to target only the intended situations by expressed rules. By administrability, I mean the organisational, human, and technological cost of adjudicating the rules, including facing and paying for the respective internal and external appeals.

Usually, the more precise the rules are, the more costly their administrability due to their complexity; vice versa, the less precise the rules, the cheaper their administrability due to their simplicity. This trade-off has been debated for years in the literature, often as a difference between standards and rules.³⁹ Administrability is a term borrowed from antitrust literature interested in the trade-offs of flexible standards and bright-line rules.⁴⁰ In the context of rule setting by providers, administrability highlights that the complexity of rules increases their cost of administration not only because of the difficulty in establishing meaning⁴¹ but also due to the regulatory compliance costs triggered by more complex rules.

If the cost of administrability is not offset by benefits gained by the precision of rules, the providers are likely to revert to simpler, and thus more administrable rules.

Each content rule that the provider adopts must conform to the following legal metrics imposed by the DSA, which increase its cost of administrability:

³⁹ Colin S Diver, 'The Optimal Precision of Administrative Rules' (1983) 93(1) *The Yale Law Journal* 65, 71–79; Ronald M Dworkin, 'The Model of Rules' (1967) 35(1) *The University of Chicago Law Review* 14, 22–29; Louis Kaplow, 'A Model of the Optimal Complexity of Legal Rules' (1995) 11(1) *The Journal of Law, Economics, and Organization* 150, 152–58; Louis Kaplow, 'Rules Versus Standards: An Economic Analysis' (1992) 42 *Duke Law Journal* 557, 571–86; Eric Posner, 'Standards, Rules, and Social Norms' (1997) 21(1) *Harvard Journal of Law and Public Policy* 101, 107–16; Julia Black, *Rules and Regulators* (OUP 1997).

⁴⁰ Geoffrey A Manne and Joshua D Wright, 'Google and the Limits of Antitrust: The Case Against the Antitrust Case Against Google' [2010] *George Mason Law & Economics Research Paper* No 10-25 <<https://papers.ssrn.com/abstract=1577556>> accessed 3 September 2023.

⁴¹ The importance of information gathering has been highlighted by Kaplow (n 39) 152–58.

- a) general explainability (Article 14(1))
- b) individual explainability (Articles 17(1) and 20(5))
- c) non-arbitrariness and fairness (Articles 14(4), 16(6), and 20(4), Recital 45)⁴²

Consider two content moderation rules on social media:

- (1) Anyone who repeatedly contacts a stranger without his or her prior permission with the intention to start an intimate relationship shall be banned from the service for the period of one month.
- (2) Anyone who contacts another person more than 10 times in 10 days without reply shall be banned from the service for the period of one month.

Both rules are trying to tackle the same problem of harassment. The first rule is likely more precise because it includes numerous qualifiers, such as ‘stranger’, ‘intention’, ‘intimate relationship’, ‘prior permission’, etc. These qualifiers are, however, also a source of increased costs of administrability of the rules. In contrast, the second rule is probably very cheap to implement, as the context is fully provided by meta-data about the interaction of two users. It is likely less precise because it does not try to capture the essence of harassment. Instead, it places some easily quantifiable metrics that are easily explainable around the notion of harassment as signposts.

Naturally, not all situations have cheaper alternatives. Most illegality rules in the legal system are highly contextual, which in turn increases their administrability costs. The companies are therefore turning to their own terms and conditions to fine-tune the rules in ways that are more administrable. The situation becomes even more complicated when companies start resorting to machine-learning systems to predict what constitutes a breach of a rule from patterns. If providers are unable to spell out the underlying logic for what constitutes a rule that has been internalised by the system, they might have very useful technologies but are unable to use and comply with Articles 14(1) and 17(1).

The DSA keeps the possibilities open for companies to use various explanations, including visual ones.⁴³ Thus, explainability systems that rely on the graphical representation of what machines are doing (eg saliency heat-maps),⁴⁴ could be an permissible way of implementing Articles 14(1) or 17(1).⁴⁵

⁴² The DSA uses various terms: ‘shall act in a diligent, objective and proportionate’ (art 14(4)), ‘a timely, diligent, non-arbitrary and objective manner’ (art 16(6)), and ‘timely, non-discriminatory, diligent and non-arbitrary manner’ (art 20(4)). While the DSA expects non-arbitrariness and non-discrimination, the term ‘consistency’ is never mentioned by the DSA in the context of art 14. Despite this, it expresses the same maxim: ‘like cases should be treated alike’, ie similarly situated individuals should receive similar treatment. The hodgepodge of terms is a result of the legislative process that changes the Commission’s initially more consistent use of terms (Hofmann and Raue [n 10] 267). I consider the terms of non-arbitrariness and fairness to be the overarching concepts.

⁴³ DSA, Rec 45 (‘Providers of intermediary services may use graphical elements in their terms of service, such as icons or images, to illustrate the main elements of the information requirements set out in this Regulation’).

⁴⁴ Adrit Rao and Oliver Aalami, ‘Towards Improving the Visual Explainability of Artificial Intelligence in the Clinical Setting’ (2023) 1 BMC Digital Health 23.

⁴⁵ AI explainability is a large research field: for an overview, Feiyu Xu and others, ‘Explainable AI: A Brief Survey on History, Research Areas, Approaches and Challenges’ in Jie Tang and others (eds), *Natural Language Processing and Chinese Computing*, vol 11839 (Springer International Publishing 2019); Royal Society, *Explainable AI: The*

On the other hand, unless providers are very large online platforms (VLOPS) or very large online search engines (VLOSEs), the DSA does not tell companies how *precise* their rules must be. It requires minimum compliance with the three administrability metrics. Thus, if a provider prefers low-cost solutions and it does not mind angering users with imprecise rules, its strategy will likely comply with Article 14. If, on the other hand, a company prefers to be precise and does not mind higher costs, this can equally comply with the provision. The key challenge for the Digital Services Coordinators (DSCs) and European Commission will be to set acceptable boundaries for each of the three key metrics. The harder they push, the more likely it is that they will influence companies to formulate less precise rules. If they make administrability of open concepts too costly, they are likely to see providers retreating from overly precise rules and resorting to cheaper alternatives, whenever possible.

To illustrate the problem, consider the earlier mentioned inability of Facebook to consider the context when posts quoting Goebbels did not explicitly condemn him. While Facebook's rule might have been imprecise, in the absence of a cheap ability of the provider to infer context, the rule was much more administrable than one advanced by the Oversight Board. In my view, the above decision of the Facebook Oversight Board, while correct on merits, is *not* compelled by the DSA. The DSA arguably does not force providers to be surgically precise with respect to balancing. While the DSA requires providers to consider fundamental rights, I do not think that this prohibits them from adopting shortcuts in their policies that generate more consistent outcomes.

There is a trade-off between fairness, derived from consistency and precision.

12.3.4 Rules vs design

A difficult question that courts will have to grapple with in the coming years is what to do when rules are *not* the mechanism that regulates content moderation according to Article 14(1). The provision applies to 'any restrictions that [providers] impose in relation to the use of their service in respect of information provided by the recipients of the service'. This definition certainly includes all restrictions that trigger the statement of reasons in Article 17: content visibility restrictions, and monetisation, account, or service restrictions. What other activities remain to be covered?

Consider the example of content-ranking algorithms, such as newsfeeds. Such algorithms always lead to the restriction of *some* content because ranking is a zero-sum game, ie where some people gain increased visibility, they do so at the expense of others. Similarly, design decisions around networks, such as restrictions on who can share what with whom (eg number of words per post, or caps on reshares), equally limit *some* content. Are these design choices subject to Article 14, or not? If they are, they would need to be proportionate, even though it might sound absurd.

Arguably, the DSA cannot regulate the entire design of services through Article 14. All design choices of a service, such as limiting posts to 100 or 200 characters, can hardly be subject to a codification requirement in the terms of service and the principles of fairness. The Court will need to navigate the boundaries of the term carefully. An over-broad interpretation of Article 14 is likely to be not only counterproductive, but also unnecessary. This is because the DSA only leaves the general design of services partially out of its scope. On the contrary, it comes up with specific due diligence obligations concerning the design of recommender systems or user interfaces. Plus, the risk-management mechanism for VLOPs and VLOSEs covers the entire service design of the regulated services.

One type of restriction that is excluded from Article 14(1) and thus Article 14(4) are *community* decisions about content. If communities are independent of the providers, the providers cannot be said to ‘impose’ those rules. Such community-driven rules and decisions then escape the requirements of Article 14 and can be freely designed according to the desires of a community. As previously explained in Chapter 11, this is consistent with the view for procedural rights, which equally do not apply to the community content moderation rules.

During the DSA negotiations, the German media sector tried to ensure that content produced by legacy media would not be subject to content moderation by platforms.⁴⁶ Their argument was that editorial content does not have to be subjected to further checks. This proposal echoes one particular content fairness concern that has received a lot of attention in recent years in Europe amongst policy circles—that of *media pluralism*—the ability of individuals to find, read, engage with, and share publications representing different viewpoints. This proposal was strongly opposed by many, including professional journalists. At the time of writing, various attempts to specifically ‘upgrade’ the DSA for editorial media are being undertaken in some other legislative acts.⁴⁷ While Article 14 DSA invokes fundamental rights, and thus indirectly media pluralism, this can hardly be read as a hard requirement or even as a potential avenue to foster media diversity through content moderation rules. But for VLOPs and VLOSEs, the universal rules are complemented by much more explicit requirements in this area (Chapter 15).

12.3.5 Impact on non-platform services

Traditionally, in the sphere of hosting service providers, and in particular online platforms, we already see the main actors engaging in content moderation. Internet

⁴⁶ Luca Bertuzzi, ‘Media Exemption Ruled out in DSA Negotiations, but Could Return’ (www.euractiv.com, 24 November 2021) <<https://www.euractiv.com/section/digital-single-market/news/media-exception-ruled-out-in-dsa-negotiations-but-could-return/>> accessed 3 September 2023.

⁴⁷ Commission, ‘Proposal for a Regulation of the European Parliament and of the Council establishing a common framework for media services in the internal market (European Media Freedom Act) and amending Directive 2010/13/EU’ COM(2022) 457 final, art 17.

infrastructure services, such as top-level domain name registries, certificate authorities that issue digital certificates, virtual private networks, cloud infrastructure services, or content delivery networks,⁴⁸ as more ‘distant’ players, usually shied away from moderating content. The reason was simple. They are usually not expected to exercise any degree of control over the content by the liability exemptions.⁴⁹ But this is quickly changing.

Let me list some of the most recent examples: CloudFlare, a content delivery network, withdrew services to Kiwi farms and DailyStormer;⁵⁰ the CZ.NIC, a Czech domain authority, blocked disinformation sites in the country following the Russian invasion of Ukraine;⁵¹ Telegram, a messaging service, blocked conspiracy theorist Atilla Hildmann after receiving pressure from Google/Apple to do so;⁵² PayPal, a payment service, is working with Antidefamation League to investigate who not to service;⁵³ Zoom has blocked a San Francisco State University event featuring Palestinian activist Leila Khaled, who had taken part in two plane hijackings.⁵⁴

The DSA anticipates this shift to infrastructure to a limited extent. Article 14(4) applies to all intermediary services, including internet access providers, domain name registries, content delivery networks, and cloudless messaging or video-conferencing apps (Chapter 7.6). From the list above, it would not apply only to PayPal. While access providers are heavily constrained in their content moderation abilities by net neutrality laws,⁵⁵ and so might be financial institutions,⁵⁶ other providers are not subject

⁴⁸ DSA, Rec 28.

⁴⁹ Regarding communication network access providers, see *Tobias Mc Fadden v Sony Music Entertainment Germany GmbH* ECLI:EU:C:2016:170, Opinion of AG Szpunar, para 100; *Tobias Mc Fadden v Sony Music Entertainment Germany GmbH* ECLI:EU:C:2016:689, para 61ff.

⁵⁰ Matthew Prince, ‘Blocking Kiwifarms’ (*The Cloudflare Blog*, 3 September 2022) <<http://blog.cloudflare.com/kiwifarms-blocked/>> accessed 3 September 2023; Matthew Prince, ‘Why We Terminated Daily Stormer’ (*The Cloudflare Blog*, 16 August 2017) <<http://blog.cloudflare.com/why-we-terminated-daily-stormer/>> accessed 3 September 2023.

⁵¹ CZ.NIC Association, ‘CZ.NIC Blocked Websites Spreading Disinformation Concerning the Russian-Ukrainian Conflict’ (25 February 2022) <<https://www.nic.cz/page/4301/sdruzeni-cznic-zablokovalo-weby-sir-ici-dezinformace-spojene-s-rusko-ukrajinskym-konfliktem/>> accessed 3 September 2023.

⁵² Carla Reveland, ‘Dutzende Hildmann-Accounts weiter verfügbar’ *tagesschau.de* (12 April 2023) <<https://www.tagesschau.de/faktenfinder/telegram-ausweichkanale-hildmann-101.html>> accessed 4 September 2023.

⁵³ ADL, ‘PayPal Partners with ADL to Fight Extremism and Protect Marginalized Communities’ (26 July 2021) <<https://www.adl.org/resources/press-release/paypal-partners-adl-fight-extremism-and-protect-marginalized-communities>> accessed 3 September 2023.

⁵⁴ James Vincent, ‘Zoom Cancels Talk by Palestinian Hijacker Leila Khaled at San Francisco State University’ (*The Verge*, 24 September 2020) <<https://www.theverge.com/2020/9/24/21453935/zoom-facebook-youtubecancel-talk-leila-khaled-san-francisco-state-university>> accessed 3 September 2023. For the recent state of affairs, Moderated Content podcast, ‘Zoom Rethinks Its Approach to Content Moderation’ (*Stanford Law School Podcasts*, 1 February 2023) <<https://law.stanford.edu/podcasts/zoom-rethinks-its-approach-to-content-moderation/>> accessed 4 September 2023; ‘Acceptable Use Guidelines Enforcement’ (*Zoom*) <<https://explore.zoom.us/en/acceptable-use-guidelines-enforcement/>> accessed 4 September 2023.

⁵⁵ European Parliament and Council Regulation (EU) 2015/2120 laying down measures concerning open internet access [2015] OJ L310/1, art 3 (Open Internet Regulation).

⁵⁶ In a recent row about Nigel Farage and the closure of his bank account, the failure of the bank to uphold s 18 of the UK Payment Accounts Regulations 2015 became clear (Iain Withers, ‘UK Watchdog Steps into Row over “debanking” of Nigel Farage’ *Reuters* [19 July 2023] <<https://www.reuters.com/world/uk/farage-makes-fresh-allegations-against-uks-coutts-over-account-closures-2023-07-19/>> accessed 4 September 2023). The UK Regulations are the implementation of the EU-wide rules found in art 35(1) of European Parliament and Council (EU) 2015/2366 on payment services in the internal market [2015] OJ L337/35 (Payment Services (PSD2) Directive).

to similar obligations. Consider an example of a provider of a video-conferencing tool which might qualify as a mere conduit. While the DSA's liability exemptions do not expect such a provider to moderate, if it decides to cancel scheduled webcasts of events of its users, it will need to have pre-disclosed rules (Article 14(1)) and apply them non-arbitrarily (Article 14(4)). These obligations, unlike transparency rules (Article 15), will apply regardless of the size of the provider.

One of the key ways in which Article 14 can impact infrastructure services is by indirectly forcing companies to introduce procedural safeguards in their systems. The DSA limits internal and external appeals to online platforms. While infrastructure services do not have to moderate content in the absence of legal orders to do so, if they take the initiative, Article 14 might introduce obligations similar to Articles 17–20 by analogy. Thus, providers might be asked to explain their decisions individually and allow an internal review of their services. The DSA does speak to such situations; however, it is clear that the lowest version of fairness that these companies can provide their users with under Article 14(4) is procedural safeguards against abuse. Thus, if a video-conferencing system adopts an elaborate usage policy, it might not only need to satisfy Article 14 but also potentially offer individual explanations and some types of appeals.

12.4 Safeguards Against Abuse by Users and Notifiers (Article 23)

The only explicit rule in the DSA that prescribes specific content moderation rules is Article 23. The provision was designed as prescribing the *minimum* mandatory measures that platforms must undertake against abusers. Recital 64 makes clear that the obligation to suspend is 'without prejudice to the freedom by providers of online platforms to determine their terms and conditions and establish *stricter* measures in the case of manifestly illegal content related to serious crimes, such as child sexual abuse material'.⁵⁷ The DSA does *not* limit platforms which do not want to wait until the violation is repeated or becomes frequent.

Article 23 deals with two basic potential bad actors: a) recipients of the service, and b) notifiers. It anticipates their behaviour when filing the notices, using the service, or the provider's notice mechanism. The recipients of services are mostly users acting as content creators. However, the category can also include users who merely use the service, including NGOs which use the notice or appeal mechanisms.⁵⁸

12.4.1 Prior warning

According to Article 23(1), every suspension by providers based on manifest illegality must be 'for a reasonable period of time' and 'after having issued a prior warning'. The

⁵⁷ DSA, Rec 64 (emphasis mine).

⁵⁸ According to art 3(b) DSA, even such actors 'use' the service.

same applies to suspensions of services directed at notice submitters or anyone filing an internal complaint.

All these decisions are subject to Article 17 and thus must be accompanied by a statement of reasons. Unlike other provisions of DSA, Article 23 *mandates* that providers make these decisions in their rules to curb abuse. Since the decisions are mandated by the legislature, they must be proportionate. The EU legislature's requirement that they are subject to prior warning and a reasonable period, are its expressions of proportionality.

However, it could be argued that a similarly strong proportionality requirement does not apply to decisions that are at the *discretion* of the providers. Thus, if a provider adopts a stricter policy against abuse, its non-mandatory parts do not necessarily require prior warning. For such non-mandatory anti-abuse decisions, providers can formulate the sanctions much more flexibly. They can trigger them with lower thresholds, such as the existence of a mere suspicion of abuse by a group of actors who are likely to act in concert. Only the case law will show what boundaries the courts are willing to impose on the proportionality of the sanctions imposed by providers. If they adopt the fairness view, for which I have argued above, a range of acceptable responses remain at the providers' disposal.

Prior warnings are articulated as a common expectation for account suspensions under the DSA (Article 23) and business users' service suspensions, terminations, or restrictions under the P2BR.⁵⁹ Recital 22 P2BR explains the rationale as follows:

To minimise the negative impact of such decisions on business users, providers of online intermediation services should also allow an opportunity to clarify the facts that led to that decision in the framework of the internal complaint-handling process, which will help the business user, where this is possible, to re-establish compliance.

Thus, while prior warnings do not technically apply to all account suspensions one can think of, when designing the content moderation practices, the starting position should be that providers take the chance to 're-establish compliance', taking into consideration the provisions of Article 14 DSA.⁶⁰ If they want to deviate, and the DSA or specific regulation contains no explicit rules on this, they must be able to justify their failure to give a prior warning by reason of a special situation that does not allow such practice.

Typical situations where the providers might wish to dispense with prior warnings or move faster than usual, for instance, include anti-spam measures. Arguably, the DSA indicates that such situations must be treated differently. First, Article 17 allows providers to *not* issue a statement of reasons 'where the information is deceptive high-volume commercial content' (Article 17(2)). Thus, the high-volume commercial content that bombards the service, as long as it is deceptive, can be restricted without

⁵⁹ Art 4(1) P2BR.

⁶⁰ For a similar argument, Hofmann and Raue (n 10) 270, with reference to German practice.

issuing a statement of reasons for each individual piece of content. However, the provider might still be obliged to issue a statement of reasons for related service-level suspensions, for instance, when a high-volume users are individually restricted in their rights to post content or their account is terminated.⁶¹ That being said, those statements of reasons can be automated.

For anti-spam measures, there is a concern that the issuance of a statement of reasons might endanger the efficacy of the underlying detection tools and policies. This is a legitimate concern. However, even when the statement of reasons must be issued, which seems to be a minority of cases, the DSA does not entitle spammers to learn about all the intricacies of the underlying detection mechanisms. After all, copyright-infringers do not learn about how the filtering system operates from the statement of reasons either. They are entitled to the ‘facts and circumstances’ relied upon, clarification of the grounds for the termination, and an explanation ‘as to why’ and be offered information about the redress. Clearly, though, the explanations of ‘why’ and ‘facts and circumstances’ must be very careful to avoid teaching abusers how to circumvent the systems put in place to stop them.

Article 23, as already mentioned, also *mandates* that providers issue special suspensions to several groups of frequent violators: (a) recipients of the service, (b) notifiers, and (c) whoever uses the internal appeals system (Article 23(2)). The trusted flaggers can be stripped of their status by the DSCs (Article 22(6)).

12.4.2 Scope and conditions

Special suspensions for repeated violations are only mandated by DSA for *manifestly illegal* content or behaviour. Thus, a user who has a track record of vulgar expressions that are not manifestly illegal, even if still potentially illegal, does not have to be suspended if the same violations occur again. The decision to suspend in such cases is at the discretion of the provider (subject, again, to Article 14’s limitations). As explained earlier, according to the DSA, providers are free to decide how they treat individuals or entities who abuse their contractual obligations.⁶² Finally, even in the absence of the specific DSA rules, orders issued by courts or authorities can require a provider to take further anti-abuse measures on their services in specific cases. Since the DSA does not exhaustively regulate the question of prior warnings, national law (including constitutional law) may still have a role to play.

The thresholds triggering mandatory suspension are described as ‘frequently provid[ing] manifestly illegal content’ (Article 23(1)) and ‘frequently submit[ing]

⁶¹ One can also discuss whether such limitation on high-volume deceptive content applies vis-à-vis business users whose rights are regulated in the P2BR. Art 4(5) P2BR states that a statement of reasons does not have to be issued ‘where a provider of online intermediation services can demonstrate that the business user concerned has repeatedly infringed the applicable terms and conditions, resulting in termination of the provision of the whole of the online intermediation services in question.’

⁶² However, sector-specific regulations, such as P2BR, can have some concrete expectations in this regard, see ch 18.

notices or complaints that are manifestly unfounded’ (Article 23(2)). If the thresholds are met or after the first abuse, the provider comes under *an obligation* to issue a ‘prior warning’ informing of such policy and, if the compliance is not restored, temporarily suspend the provider for a ‘reasonable time’. If the provider fails to suspend services or specific privileges in such cases on these terms, it can violate its due diligence obligations, and be fined or sued for compliance.

The underlying idea is to create basic incentives for notifiers and content creators to examine what they submit as repeated egregious mistakes which can cost them a privilege to submit notifications, content, or complaints on the platform for a while. Thus, even if the notifiers are not trusted flaggers, the DSA introduces a mechanism that not only allows but *mandates* that providers ‘educate’ notifiers and content creators about the most egregious content mistakes—those relating to manifestly illegal content that should be recognisable even to a lay person. To protect against ‘convenient’ suspensions by platforms, Article 23(3) outlines several rules that should guide the mandated suspensions.

Firstly, each such suspension must be evaluated case-by-case, and thus cannot be delegated to machines. The human assessment must be timely, diligent, and objective. Secondly, the DSA prescribes the basic relevant framework for assessment: the absolute number of relevant mistakes in a given timeframe, their proportion to the overall number of relevant cases, the gravity of mistakes, and likely motivations for them. Thirdly, the benchmarks for the relevant circumstances shall be clearly stated in the terms and conditions, along with examples of cases where the provider triggered mandated suspensions. They must also specify the duration for which the temporary suspension applies.

Since Article 23 does not specify the ‘reasonable period of time’ for suspensions, providers have the freedom to design their mandated suspension policies for manifestly illegal content policies to a considerable extent. They have even broader discretion with respect to their policies concerning other types of content, or behaviour. While the DSA offers a minimalist framework for how to design some of these policies, many details are left to providers to determine. Article 23 thus acts mostly as a moderator of ‘disproportionate’ suspension policies. Thus, in cases like the suspension of former US President Donald Trump,⁶³ Article 23 offers only a basic indication of when to pull the trigger on the time-limited suspension.

12.5 Conclusions

Article 14 is a key piece of the DSA’s fairness architecture. From a fundamental rights perspective, it invites an indirect effect of fundamental rights. From a regulatory

⁶³ Ben Collins and Brandy Zadrozny, ‘Twitter Permanently Suspends President Donald Trump’ (*NBC News*, 9 January 2021) <<https://www.nbcnews.com/tech/tech-news/twitter-permanently-bans-president-donald-trump-n1253588>> accessed 4 September 2023.

perspective, it is a catch-all clause for all services. And from civil society's perspective, it is an expression of the rule that content moderation decisions of companies should not be solely guided by profit.

The provision is meant to assure that the public can infer what restrictions apply to their content and behaviour on a particular service upfront. As mentioned above, any restriction of content—rule and its sanction—needs a legal basis either in the legal norm that stipulates illegality, or a contractually agreed provision. What is disclosed *ex ante*, influences what is justified *ex post*.

Fairness is the overarching quality demanded by Article 14. The review foreseen by Article 14(4) allows the courts and ODS bodies to scrutinise individual terms. Rules that do not meet the criteria are not binding upon users. However, there is a trade-off between fairness derived from consistency and precision. It is impossible to maximise both equally. If the cost of administrability of rules is not offset by benefits gained by their precision, the providers are likely to revert to simpler and, thus, more easily administrable rules.

Risk-Based Approach to Digital Services

13.1 Regulatory Moment	270	13.4 Precautionary Principle and Rule of Law	279
13.2 A Risk-Based Approach	274		
13.3 The Regulator's Powers	276	13.5 The Bigger Cycle of Risk Mitigation	282

13.1 Regulatory Moment

Regulation is often a product of public confidence crises. For instance, European food safety laws were drafted in response to major incidents in the 1990s.¹ The Bovine Spongiform Encephalopathy (BSE) or Mad Cow Disease crisis, in particular, even led the then-president of the Commission, Jacques Santer, to promise institutional restructuring and legislative reform based on ‘sound science.’² Similarly, the regulation of banks has its origins in numerous financial crises. The European prudential requirements were introduced in the aftermath of the global financial crisis in 2007–08 to ensure that banks are better able to withstand liquidity shocks and absorb losses.³

The popular demand for digital regulation, too, was born out of a continuous stream of public confidence crises in the 2010s: hate speech, child abuse, grooming, terrorist content, election interference, disinformation, war propaganda, and the list goes on.⁴ The concerns related to digital services are best encapsulated in Frances Haugen’s revelations. The former data scientist at what was then Facebook leaked a wide array of internal documents in 2021, accusing Facebook of ‘putting profit over the public good.’⁵ She claimed that: ‘[t]he thing I saw at Facebook over and over again was there

¹ Patrick Van Zwanenberg and Erik Millstone, *BSE: Risk, Science, and Governance* (OUP 2005); Tim Lang, ‘Food, the Law and Public Health: Three Models of the Relationship’ (2006) 120 (Suppl 1) *Public Health* 30; see also European Parliament and the Council Regulation (EC) No 178/2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety [2002] OJ L31/1.

² Florence Bergeaud-Blackler and Maria Paola Ferretti, ‘More Politics, Stronger Consumers? A New Division of Responsibility for Food in the European Union’ (2006) 47 *Appetite* 134, 137.

³ European Parliament and Council Regulation (EU) No 575/2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 [2013] OJ L176/1; Sophie Harnay and Laurence Scialom, ‘The Influence of the Economic Approaches to Regulation on Banking Regulations: A Short History of Banking Regulations’ (2016) 40 *Cambridge Journal of Economics* 401.

⁴ The numerous challenges that shaped the European system have been detailed in chs 1, 4, and 17.

⁵ Kari Paul and Dan Milmo, ‘Facebook Putting Profit before Public Good, Says Whistleblower Frances Haugen’ *The Guardian* (4 October 2021) <<https://www.theguardian.com/technology/2021/oct/03/former-facebook-employee-frances-haugen-identifies-herself-as-whistleblower>> accessed 5 September 2023.

were conflicts of interest between what was good for the public and what was good for Facebook. And Facebook, over and over again, chose to optimise for its own interests, like making more money'.⁶

According to Julia Black and Andrew Murray, the period between 1995 and 2020 has been characterised by a lack of meaningful regulation over the digital environment.⁷ They observe that: '[e]ffective regulation of the online environment had been ceded through contractualism to a small number of key online platforms: platforms which act within their own spheres as private nation states'.⁸

The lack of top-down social control over digital services inevitably meant that the power has been appropriated by companies.⁹

For regulation of any kind, the most important consequence of this redistribution of power is described by Collingridge who posits that '[w]hen change is easy, the need for it cannot be foreseen; when the need for change is apparent, change has become expensive, difficult, and time-consuming'.¹⁰ Thus, any regulatory attempts by the state to regulate digital services 20 years after they have been widely adopted will only face increasing difficulty in exercising social control over the technology.¹¹

However, diagnosing the regulatory gap is easier than devising a useful regulatory approach.

Currently, our banks, food, drugs, environment, and many other areas are regulated through some form of a risk-based approach. Quite naturally, with the emergence of platforms and the risks they present, scholars started wondering whether the same approach could apply to digital services.¹²

In theory, the European Union (EU) legislature could have opted for the traditional command-and-control model of regulation where rules are ready-made and fully detailed upfront. However, relying on merely a top-down approach would have risked the rules becoming obsolete very quickly. Digital markets are characterised by large information asymmetries,¹³ rapid change, and global nature.¹⁴ The legislator moreover had

⁶ *ibid.*

⁷ Julia Black and Andrew Douglas Murray, 'Regulating AI and Machine Learning: Setting the Regulatory Agenda' (2019) 10(3) *European Journal of Law and Technology* 1, 5.

⁸ *ibid.*

⁹ Many scholars have anticipated this redistribution of powers in the absence of state intervention. See Henry Perritt, 'Cyberspace Self-Government: Town-Hall Democracy or Rediscovered Royalism?' (1997) 12 *Berkeley Technology Law Journal* 413; Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books 1999). See also ch 1.4 for a further discussion.

¹⁰ David Collingridge, *The Social Control of Technology* (St Martin's Press 1980) 11. See the discussion in ch 1.3.

¹¹ See ch 1.

¹² Carsten Ullrich, 'A Risk-Based Approach Towards Infringement Prevention on the Internet: Adopting the Anti-Money Laundering Framework to Online Platforms' (2018) 26(3) *International Journal of Law and Information Technology*, 226–51; Carsten Ulrich, *Unlawful Content Online: Towards a New Regulatory Framework for Online Platforms* (Nomos, 2021); Pieter Nooren, Nicolai van Gorp, Nico van Eijk, and Ronan Ó Fathaigh, 'Should We Regulate Digital Platforms? A New Framework for Evaluating Policy Options' (2018) 10 *Policy & Internet* 264–301; Lorna Woods and William Perrin, 'Online Harm Reduction—a Statutory Duty of Care and Regulator' (*Carnegie UK Trust* 2019) 7, 13 <<https://carnegieuktrust.org.uk/publications/online-harm-reduction-a-statutory-duty-of-care-and-regulator/>> accessed 10 August 2023.

¹³ Michèle Finck, 'Digital Co-Regulation: Designing a Supranational Legal Framework for the Platform Economy' (2018) 43(1) *European Law Review* 47, 51, 54.

¹⁴ See ch 1.

Table 13.1 DSA's elements according to regulatory approach

DSA's components	Goals	Regulatory approach
Risk management	Improved design	(1) few detailed rules for mid-sized platforms (2) supervised co-regulation for VLOP/VLOSEs
Content moderation	Procedural fairness	(1) detailed rules based on the size/function
Transparency	Explainability of decision-making and understanding of risks	(1) detailed rules for mid-sized companies (2) mandated data access for VLOP/VLOSEs

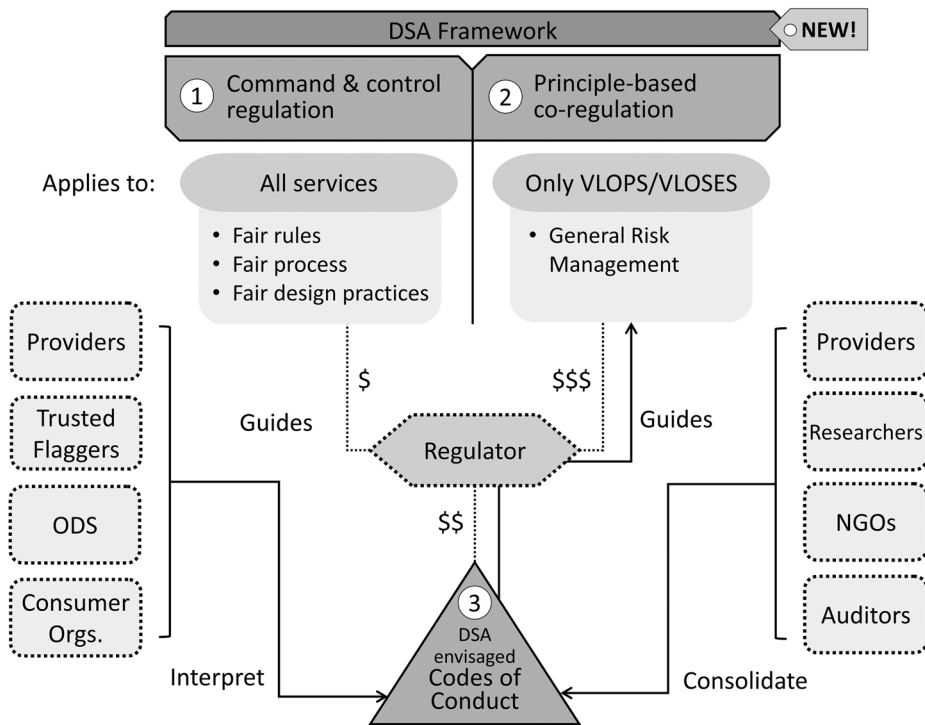
to balance the protective goals with overly broad rules that can erect extremely high barriers for competitors. Despite the limits of competition as a tool of regulation, its disciplining properties needed to be preserved for the digital ecosystem.¹⁵

Therefore, the EU legislature decided to embrace *several* regulatory approaches at once. In the areas where the risks seemed most fast-paced and open to new developments, traditional command-and-control regulation was substituted for the polycentric regulatory model with elements of co-regulation.¹⁶ In the areas where the problems seem to have crystallised across the industry, the EU legislature adopted detailed rules (see Table 13.1).

For the purposes of the latter, the Digital Services Act (DSA) defines Big Tech as very large online platforms or very large search engines (VLOPs/VLOSEs) that reach 45 million monthly active users and are designated as such by the European Commission (Chapter 9). VLOPs/VLOSEs are subject to 360-degree scrutiny of many types of risks through the annual regulatory dialogue with the European Commission. No corner of the service is spared. Many risks are relevant. The companies must conduct self-assessment, arrange audits, and engage with regulators, researchers, and other actors. These obligations are thus the opposite of prescriptive; they are very general and open-ended. They ask companies to think about the impact of their services on fundamental rights.

The marriage of businesses and the protection of human rights is not unique to digital services. Building upon the United Nations (UN) Ruggie Principles,¹⁷ the EU has recently proposed to tighten the due diligence obligations of companies when they operate their supply chains. Among other things, they must consider human rights abuses of their suppliers, such as forced labour, child labour, inadequate workplace

¹⁵ See ch 1.4.
¹⁶ Julia Black, 'Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a "Post-Regulatory" World' (2001) 54(1) *Current Legal Problems* 103; Finck (n 13) 58.
¹⁷ Office of the High Commissioner for Human Rights, 'Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework' (UN 2011) <https://www.ohchr.org/sites/default/files/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf> accessed 5 September 2023. In her 2012 PhD thesis, Emily Laidlaw suggested applying them to the gatekeepers; published as Emily B Laidlaw, *Regulating Speech in Cyberspace: Gatekeepers, Human Rights and Corporate Responsibility* (CUP 2015).



Number of \$ signs represents relative cost to regulator for meting out punishment for violation of each aspect of DSA

Figure 13.1 The DSA framework in one picture

health and safety, exploitation of workers, and environmental impacts, and establish processes to manage them.¹⁸

However, the unique characteristic of digital services regulation is, as explained by Balkin,¹⁹ that they are largely implemented with the *individual end-users* in mind since the risks at issue are often linked to expressive human behaviour. Although outwardly regulating companies, such regulation actually seeks to regulate private individuals using these global communication services. Regulation of digital services thus not only regulates the business; it regulates crowds. The stakes are, therefore, much higher. For this reason, without proper judicial oversight, the DSA's general risk management system can become a dangerous tool for regulators who claim to act in the public interest but do not bother to review evidence to confirm their hunches.

The graphic below tries to capture the essence of the DSA's regulatory approach, emphasising that the mode of enforcement differs for detailed prescriptive and risk management rules (see Figure 13.1). The prescriptive rules are cheaper and faster to enforce. In contrast, the general risk management provisions are expensive and slow

¹⁸ Commission, 'Proposal for a Directive of the European Parliament and of the Council on Corporate Sustainability Due Diligence and Amending Directive (EU) 2019/1937' COM(2022) 71 final.

¹⁹ Jack M Balkin, 'Free Speech is a Triangle' (2018) 118 Columbia Law Review 2011.

to enforce on their own. Similar to competition law, the lack of proper evidence will likely become an important limiting factor for the Commission's actions. In the absence of industry standards, it will be costly to substantiate baseline evidence to articulate what mitigation efforts are clearly suboptimal. In the event of judicial review, the Commission will lose if it cannot produce 'precise and consistent evidence' of both baseline and suboptimality of the behaviour of regulatees.²⁰ Given that the 'benefit of any doubt' must be given to the accused of regulatees, the evidence must be strong.²¹ From this perspective, the Codes of Conduct primarily help the Commission by making enforcement under Articles 34 and 35 somewhat cheaper and faster because they establish *prima facie* evidence of the industry's good standard of practices.

13.2 A Risk-Based Approach

As aptly summarised by Murray, '[e]volution rather than revolution is the key to effective regulatory intervention'.²² Even the DSA's detailed command-and-control rules are often codifications of prior industry practices. The mechanisms like trusted flaggers, appeals, transparency reports, or centralised databases of decisions already existed before the DSA, although they might have been more limited or only relied upon by some. From this perspective, the DSA is not exactly revolutionary. Even the general risk management tool foreseen for Big Tech is designed to favour incremental change rather than radical change. Risk mitigation improves year-by-year, as industry, society, and regulators gradually learn, rather than by large leaps.

The risk approach is therefore a good fit for the risks posed by the biggest digital services. If drafted as polycentric or symbiotic regulation,²³ it achieves a better concentration of knowledge naturally dispersed across society among many actors.²⁴ The outsourcing of solution-finding and agenda formulation broadens the ability of regulators to absorb important information. The exercise of drafting Codes of Conduct can potentially increase civil engagement and the transparency of public-private dealings that would otherwise remain opaque. Such forums potentially strengthen democratic deliberation in the EU.²⁵ And the regulatory relevance of these same Codes of Conduct increases the chances of their judicial review.

The DSA's idea to interweave co-regulation of Big Tech with typical top-down regulation of the industry as a whole is a strategic choice. It preserves the possibility for the regulators to invoke ready-made rules against other VLOPs unwilling to cooperate,

²⁰ Joined Cases T-67/00, T-68/00, T-71/00, and T-78/00 *JFE Engineering v Commission* ECLI:EU:T:2004:221, para 341; Koen Lenaerts, 'Some Thoughts on Evidence and Procedure in European Community Competition Law' (2006) 30(5) *Fordham International Law Journal* 1463.

²¹ Case 27/76 *United Brands v Commission* ECLI:EU:C:1978:22, para 265.

²² Andrew Murray, 'Symbiotic Regulation' (2008) 26(2) *John Marshall Journal of Information Technology & Privacy Law* 207, 225.

²³ Finck (n 13) 65; Murray (n 22) 224 ('A better approach is a control model that affords all participants in the regulatory matrix an opportunity to shape the evolutionary development of their environment.').

²⁴ Cass R Sunstein, *Infotopia: How Many Minds Produce Knowledge* (OUP 2006).

²⁵ Finck (n 13) 66.

even building the industry consensus (Chapter 20). In literature, such backup options have been recognised as key tools to motivate compliance under co-regulatory models.²⁶ In Chapter 15, I argue that the existence of prescriptive rules allows the regulators to practice a tit-for-tat enforcement strategy to motivate better compliance with more open-ended rules, such as general risk management.

Thus, adopting the risk-based approach and borrowing from the playbook of other industries are a good direction of travel.²⁷ In this sense, I agree with Woods and Perrin, the authors of the most comprehensive risk-based regulatory model for digital services, which inspired the UK Online Safety Act.²⁸ However, I disagree with their initial attempt to analogise risk management imposed on communication tools to physical safety rules, pollution, or similar problems.²⁹ As I will show, communication tools have many special features that demand a modified risk-based approach.

For a start, the respective subject matters are simply different in nature. The online vitriol that digital services regulation might seek to address is not the same as the disease-causing pathogens that food safety regulations aim to eliminate. The actions of internet actors, rather than unambiguous blights on the ecosystem, are the behaviour of real, living people. Digital services are communication tools at their core.³⁰ The ideas and expressions they transmit cannot be treated as pollution; their human authors cannot be analogised to disease-causing bacteria.

Communication is at the core of political liberties. It is the bedrock of our liberal democracies. The ideal level of ‘safety’, thus, cannot mean the same thing for communication as it does for food and chemicals. As noted by Graham Smith, speech is not a tripping hazard.³¹ People’s dignity and freedoms are deeply implicated when regulators are tasked to keep digital communications ‘safe’ by doing the balancing without any limitations other than proportionality. Safety is a good starting point, but as explained in Chapters 1 and 15, it must be continuously balanced with trustworthiness.

To be sure, the regulation of digital services can learn a lot from areas such as food safety if the right parallels are made. European food safety rules equally tackle a problem that is dynamic, global, opaque, and subject to complicated supply chains.³²

²⁶ *ibid* 59; Wolfgang Schulz and Thorsten Held, *Regulated Self-Regulation as a Form of Modern Government: An Analysis of Case Studies from Media and Telecommunications Law* (University of Luton Press 2004) 63, fn 15.

²⁷ Bridget Hutter, *The Attractions of Risk-Based Regulation: Accounting for the Emergence of Risk Ideas in Regulation* (Centre for Analysis of Risk and Regulation 2005) <https://web.actuaries.ie/sites/default/files/erm-resources/205_The_attractions_of_risk_based_regulation_accounting_for_the_emergence_of_risk_ideas_in_regulation.pdf> accessed 5 September 2023; Henry Rothstein and others, ‘The Risks of Risk-Based Regulation: Insights from the Environmental Policy Domain’ (2006) 32 *Environment International* 1056; Robert Baldwin and Julia Black, ‘Driving Priorities in Risk-Based Regulation: What’s the Problem?’ (2016) 43(4) *Journal of Law and Society* 565.

²⁸ Woods and Perrin (n 12). See the UK’s Online Safety Act 2023, <<https://www.legislation.gov.uk/ukpga/2023/50/enacted>> accessed 19 December 2023.

²⁹ This is visible also from the text of the proposed bill that omitted the definition of the notion of harm and empowered the regulator to do the full balancing, see <<https://carnegieuktrust.org.uk/publications/draft-online-harm-bill/>> (2019) accessed 19 December 2023.

³⁰ To understand how they profoundly changed social movements, see Zeynep Tufekci, *Twitter and Tear Gas: The Power and Fragility of Networked Protest* (Yale University Press 2017).

³¹ Graham Smith, ‘Speech is Not a Tripping Hazard—Response to the Online Harms White Paper’ (28 June 2019) <<https://www.cyberleagle.com/2019/06/speech-is-not-tripping-hazard-response.html>> accessed 10 August 2023.

³² Lang (n 1) 37.

Food products and digital services are both inseparable parts of our lives, culture, and identity. Constant innovation is key to business success in both areas³³ and businesses must always navigate the tension between profit and safety.

Food and digital products even face similar dilemmas: food businesses try to capture our eating habits, and technology firms our attention. Their profits increase the more people consume. Overconsuming each product can lead to obesity and loneliness, respectively, thus reducing the quality of life and affecting our well-being.³⁴ Overconsumption imposes externalities on the rest of society in the form of increased health care and other costs. As pointed out by Lang, '[u]nsafe food is quick to show results; malconsumption's illhealth effect may take decades and not be product-specific.'³⁵ Similarly, many challenges linked to digital services, such as health disinformation, radicalisation, or propaganda, can result from long-term consumption and are not necessarily product-specific.

Food policy also puts some of our online regulatory instincts in a different light. While very few would likely agree that obesity should be treated by rationing people's access to unhealthy food, in the digital realm, such proposals are constantly made about many types of 'unhealthy' information; while very few would likely agree that unhealthy food should be entirely banned from regular supermarkets because it is not 'safe', in the digital realm, the arguments about banning legal expression as 'unsafe' are not a rarity. While overt paternalism over people's affairs is easy to identify when we regulate food, it is much more hidden in discussions of digital content policy.

Thus, a risk-based approach may be a viable approach for digital services but it must account for the specifics of digital communications; namely, whenever it regulates the risks posed by digital communications, it regulates the people and crowds using such services, whether intentionally or not.

13.3 The Regulator's Powers

Francis Haugen, the Facebook whistle-blower, was very supportive of the DSA. During the legislative process, she argued that:

The right answer to this emergency is new rules and standards. The EU's Digital Services Act has huge potential. It does not try to 'delete' the problem with content

³³ Michael T Roberts, *Food Law in the United States* (CUP 2016) 3 (the history of food safety regulations is 'really history of discovering and inventions enabling regulatory responses to emerging safety problems').

³⁴ On the negative impact of overconsumption of digital products, see Amy Østertun Geirdal and others, 'Mental Health, Quality of Life, Wellbeing, Loneliness and Use of Social Media in a Time of Social Distancing During the COVID-19 Outbreak. A Cross-Country Comparative Study' (2021) 30(2) *Journal of Mental Health* (Abingdon, England) 148; Melissa G Hunt and others, 'No More FOMO: Limiting Social Media Decreases Loneliness and Depression' (2018) 37(10) *Journal of Social and Clinical Psychology* 751; Maartje Boer and others, 'Attention Deficit Hyperactivity Disorder-Symptoms, Social Media Use Intensity, and Social Media Use Problems in Adolescents: Investigating Directionality' (2020) 91(4) *Child Development* e853.

³⁵ Lang (n 1) 37.

regulations. It takes a content-neutral approach to address the systemic risks and harms of the overall business model.³⁶

As Chapter 15 explains, it is far from clear that the DSA firmly adopts a content-neutral approach as part of a risk-based approach. The breadth of the DSA's regulatory approach seems to be in the eye of the beholder. The DSA's true nature is partly hidden in a yet untested regime for general risk management.

Clarity will be increasingly demanded. Several days before the DSA went into full effect for the VLOPs and VLOSEs, an Irish journalist asked the Irish Media Minister about the reliance on the DSA to solve the problem of misinformation: 'Isn't it dangerous for democracy that powerful state institutions will get to decide what is and is not true?'³⁷ The Minister had no answers for the journalist.

The public needs proper answers to what the regulators will do under the DSA to dispel any doubts about the legitimacy of regulation. Without a clear stance, the confusion will only mount. Arguably, the Commission's rhetoric is somewhat confusing.

On the one hand, the Commission's Vice-President Jourová on the occasion of 2022 Václav Havel European Dialogues in Prague shortly before the DSA's adoption firmly argued that:³⁸

But we also see that digitalisation, the social media, has been massively used to spread and amplify disinformation. It is increasingly difficult to see who is saying what and why. Yet, new technologies should be tools for emancipation, not for manipulation. When I say this, some people argue, or rather shout: 'Jourová—you want to censor the Internet!' So, let me repeat: Freedom of speech is the most cherished value of democracy. I said many times: 'I don't want to see a Ministry of Truth'. To bring in Václav Havel again: 'Follow the man who seeks the truth; run from the man who has found it'. This is why our actions don't focus on assessing the content.

On the other hand, only a few months after the law was adopted, Commissioner Breton chastised companies in a series of letters asking them to 'spare no effort against disinformation'.³⁹ Moreover, around the same time, an independent study contracted by the European Commission looking at Russian disinformation in Europe concluded

³⁶ European Parliament Multimedia Centre, 'Public Hearing on Whistle-blower's Testimony on the Negative Impact of Big Tech Companies' Products on User: Opening Statement by Frances Haugen' (8 November 2021) <https://multimedia.europarl.europa.eu/video/public-hearing-on-whistle-blowers-testimony-on-the-negative-impact-of-big-tech-companies-products-on-user-frances-haugen-opening-statements_I213108> accessed 5 September 2023.

³⁷ Gript Media, 'Recording of Ireland's Media Minister Catherine Martin's Press Conference on 25 August 2023' (Twitter, 25 August 2023) Question by Ben Scallan about the EU's DSA <<https://twitter.com/griptmedia/status/1695108011767767114>> accessed 5 September 2023.

³⁸ European Commission, 'Speech by Vice-President Jourová on the Occasion of 2022 Václav Havel European Dialogues' (10 May 2022) <https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_22_2983> accessed 19 December 2023.

³⁹ Foo Yun Chee, 'EU's Breton tells TikTok CEO to "Spare No Effort" Against Disinformation' (6 November 2023) <<https://www.reuters.com/technology/eus-breton-tells-tiktok-ceo-ramp-up-efforts-against-disinformation-2023-11-06/>> accessed 19 December 2023.

that Big Tech did not do enough to counter Russian disinformation to satisfy the DSA's risk-based approach.⁴⁰ One of the arguments was that the sanctions on Kremlin-backed actors, such as official Russian media, were circumvented through a network of Kremlin-aligned non-state actors who more than made up for the loss by parroting its narratives.⁴¹ The failure to contain the spread of pro-Kremlin narratives, according to the report, meant that systemic risk was not properly mitigated. The report borrows from the UN Rabat Plan⁴² to outline what constitutes harm⁴³ and argues for heightened interventions against Kremlin-aligned actors, even though it does not call for the removal of all their content.⁴⁴

The obvious problem in the last two instances is that only some subset of such disinformation is unlawful.⁴⁵ Thus, a metric that asks companies to suppress such content to 'acceptable' levels in general, regardless of establishing illegality, also suppresses views from individuals who happen to express such disinformation views *legally*. While applying an approach such as that implied by the 2023 Disinformation Study should still mean that the outcomes are generally aligned with regional and international human rights limits,⁴⁶ the key problem is the lack of *legality* of such restrictions. The legality question is a question of the rule of law. It speaks to the question of who makes the rules that govern what can be said, not whether those rules are proportionate.

Thus, declaring that the DSA's risk management approach is clearly content-neutral is premature.⁴⁷ The European Commission will have to build its approach brick-by-brick in years to come.

Depending on what powers are ascribed to the Commission as the sole enforcement of general risk management, I distinguish two potential conceptions of risk management: (a) full risk management and (b) limited risk management. In Chapter 15, I argue that the DSA is a *limited risk management* regime, meaning that the regulator does not have the power to dictate contents-specific rules.

In practice, this means that unlawful Russian propaganda can be addressed by any proportionate means, but lawful pro-Russian propaganda can be addressed only by content-neutral measures imposed on how fast *any* information travels through the

⁴⁰ DG-CONNECT (EU Commission), *DSA: Application of the Risk Management Framework to Russian Disinformation Campaigns* (EU Publications Office 2023) <<https://data.europa.eu/doi/10.2759/764631>> accessed 5 September 2023.

⁴¹ *ibid* 40, 44 (on policies of companies that enabled the circumvention).

⁴² UN Human Rights Council Resolution 16/18 and the Rabat Plan of Action clarified the relationship of arts 19 and 20(2) of International Covenant on Civil and Political Rights and set out practical guidance to clarify the obligations of states under art 20(2), Office of the United Nations High Commissioner for Human Rights, 'OHCHR and Freedom of Expression vs Incitement to Hatred: The Rabat Plan of Action' (2012) (*OHCHR*) <<https://www.ohchr.org/en/freedom-of-expression>> accessed 5 September 2023.

⁴³ DG-CONNECT (EU Commission) (n 40) 16.

⁴⁴ *ibid* 47, 25 (for definition).

⁴⁵ On the national approaches to the lawfulness of disinformation, Ronan Ó Fathaigh, Natali Helberger, and Naomi Appelman, 'The Perils of Legally Defining Disinformation' (2021) 10(4) *Internet Policy Review* <<https://policyreview.info/articles/analysis/perils-legally-defining-disinformation>> accessed 19 December 2023.

⁴⁶ ECtHR borrows from the Rabat plan in its case law, see for instance, *Lenis v Greece* App no 47833/20 (ECtHR, 31 August 2023).

⁴⁷ Also there are different views in the literature: Sharon Galantino, 'How Will the EU Digital Services Act Affect the Regulation of Disinformation?' (2023) 20(1) *SCRIPTed* 89 (criticising that the DSA is likely to adopt the Code of Practice's broad definition with all the consequences for lawful disinformation).

service, by promoting user choice to view *any* trusted content, and by curbing *any* inauthentic herd behaviour.

My proposed red line⁴⁸ is grounded in the principle of the rule of law and separation of powers under the DSA's architecture, where legislatures decide what constitutes illegal content. Because digital services are communication tools, in Chapter 15, I argue that the risk-based approach must further individual agency whenever user choice is legitimate. Thus, one of the key principles should be that *if* a risk is linked to a category of content that is perfectly legal, the empowerment of users and groups should be prioritised. If the empowerment strategy fails to address the overall risks, parliaments can always redefine what is illegal.

In contrast, some may view the DSA as a *full risk management regime* where relevant risks posed by lawful content are sufficient reasons for the regulator to expand our notions of illegality ad hoc.⁴⁹ In this potential view, the regulator becomes a surrogate legislature for digital communications and can de facto expand what constitutes illegal content for the purposes of the DSA.

I seem to be in good company⁵⁰ in believing that this is not possible; however, that is no guarantee of anything until the Court of Justice of the European Union decides on the issue. Thus, at the time of writing, no one knows how the European Commission will try to conceptualise its own enforcement powers. The first opened infringement case against Twitter suggests that the Commission is mindful of the limits described above because lawful disinformation is only addressed as a potential failure of fact-checking and not suppression.⁵¹

13.4 Precautionary Principle and Rule of Law

For the same reasons, I also argue against borrowing the precautionary principle from other areas of risk-based regulation. Wood and Perrin envisage regulators' ability to limit 'harmful behaviour'⁵² prophylactically when regulators see good reasons to do so,⁵³ invoking the precautionary principle for their version of online safety regulation. The same principle underlies food safety, regulation of chemicals, and many other areas.⁵⁴ It posits that intervention must be taken under some circumstances even *before*

⁴⁸ See explicitly applying this to disinformation, Martin Husovec, 'The Digital Service Act's Red Line: What the Commission Can and Cannot Do About Disinformation' (forthcoming, 2024) *Journal of Media Law*.

⁴⁹ Martin Husovec, 'Rising Above Liability: The Digital Services Act as a Blueprint for the Second Generation of Global Internet Rules' (2023) *Berkeley Technology Law Journal* (forthcoming). https://btlj.org/wp-content/uploads/2024/01/0002_38-3_Husovec.pdf

⁵⁰ Saulius Kaleda, Paul-John Loewenthal, and Folkert Wilman, *Digital Services Act: Commentary* (forthcoming, OUP 2024) § 35 (C:10) noting that 'the obligation to take risk mitigation measures cannot, in principle, be a way to force providers to contractually prohibit certain information that does not qualify as illegal content'.

⁵¹ European Commission, 'Commission Opens Formal Proceedings Against X Under the Digital Services Act' (18 December 2023) <https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6709> accessed 19 December 2023.

⁵² Woods and Perrin (n 12) 48.

⁵³ *ibid* 11.

⁵⁴ Art 191 of the TFEU. The concept of the precautionary principle was first set out in Commission, 'Communication from the Commission on the Precautionary Principle' COM(2000) 1 final. Generally, Marko

a complete scientific proof of risk. For instance, Article 7 of the General Food Law Regulation defines it as follows:

In specific circumstances where, following an assessment of available information, the possibility of harmful effects on health is identified but scientific uncertainty persists, provisional risk management measures necessary to ensure the high level of health protection chosen in the Community may be adopted, pending further scientific information for a more comprehensive risk assessment.⁵⁵

The European Commission in 2000 Communication explains the principle as follows:

Recourse to the precautionary principle presupposes that potentially dangerous effects deriving from a phenomenon, product or process have been identified, and that scientific evaluation does not allow the risk to be determined with sufficient certainty. The implementation of an approach based on the precautionary principle should start with a scientific evaluation, as complete as possible, and where possible, identifying at each stage the degree of scientific uncertainty.⁵⁶

The reliance on the precautionary principle is another one of the areas where analogies to food safety are once again highly problematic. As cautioned by the European Commission itself:

Decision-makers need to be aware of the degree of uncertainty attached to the results of the evaluation of the available scientific information. Judging what is an ‘acceptable’ level of risk for society is an eminently political responsibility.⁵⁷

If the above sentence rings true in the area as detached from political liberties as chemicals, it must have stronger resonance when the principle is invoked to shape the boundaries of how people can communicate with each other. Adopting the precautionary principle to online communications can easily slip into giving regulators broad, even if temporary, political powers to regulate speech. In liberal democracies, such power should rest with parliaments, which are usually supervised by constitutional courts. Since under the DSA, the European Commission was not given any formal rule-making powers that could be based on the use of the precautionary principle, it must be assumed that the exercise of authority with the content-regulating effect would be

Ahteensuu and Per Sandin, ‘The Precautionary Principle’ in Sabine Roeser and others (eds), *Handbook of Risk Theory* (Springer Netherlands 2012).

⁵⁵ European Parliament and Council Regulation (EC) No 178/2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety [2002] OJ L 31/1 (General Food Law Regulation).

⁵⁶ Commission (n 54) 2.

⁵⁷ *ibid* 3.

ultra vires. Thus, declaring, de facto or de jure, certain content to be illegal is beyond the mandate.

We should be reminded of Article 1(1) of the DSA, which states that the main goal of the law is to create ‘a safe, predictable and trusted online environment’. In policy debates, there is a tendency to emphasise safety. And often it is for a good reason. Safety from illegal content fosters trust in the ecosystem and thus improves the freedom of individuals to express themselves. For instance, citizens who are safe from harassment and hate speech are more likely to express their views publicly. Safety is rightly the dominant paradigm for the protection of children, or protection of adults from illegal content.

But safety can also undermine trust. Let me illustrate this with the example of suicide reporting. Social science research shows that sensationalist coverage of suicides can lead to copycat behaviour among vulnerable individuals.⁵⁸ Thus, in many countries, the media are encouraged to follow guidance about how to report on the suicides, which can range from not mentioning them at all to not reporting on methods and avoiding any sensationalism. There is no doubt that such interventions can be justified by the safety of vulnerable individuals. However, as countries that have tried to legislate on the issue have learned, such as New Zealand,⁵⁹ overbroad rules can become counterproductive because individuals feel under-informed. Such suppression can undermine trust.

Returning to the analogy with food safety, one can say that what is acceptable as the legal basis for restricting beef distribution along the food supply chain is not automatically sufficient for restricting content online. Online safety needs a different regulatory recipe. Beef online is not beef offline. As explained by the European Agency for Fundamental Rights report, ‘[f]reedom of expression is such an important value that its restriction should always receive the democratic legitimacy only derived from parliamentary debate and elections.’⁶⁰ The *principle of legality*, namely that state interferences are based on a law of sufficient quality, demands that many more details be laid down by the parliaments. Very general formulations cannot serve as a basis for restrictions on freedom of expression.⁶¹ This is especially the case when such restrictions are imposed without public scrutiny. According to the European Court of Human Rights (ECtHR):

⁵⁸ See, for instance, Thomas Niederkrotenthaler and others, ‘Association Between Suicide Reporting in the Media and Suicide: Systematic Review and Meta-analysis’ (2020) *British Medical Journal* 368, <<https://www.bmj.com/content/368/bmj.m575.full>> accessed 19 December 2023.

⁵⁹ S 71 of the New Zealand’s Coroners Act 2006, <<https://www.legislation.govt.nz/act/public/2006/0038/latest/whole.html#DLM377532>> accessed 19 December 2023. For the analysis, James Hollings, ‘Reporting Suicide in New Zealand: Time to End Censorship’ (2023) 19(2) *Pacific Journalism Review: Te Koako*, 136–55.

⁶⁰ Dominika Bychawska-Siniarska, ‘Protecting the Right to Freedom of Expression Under the European Convention On Human Rights’ (Council of Europe 2017) <<https://rm.coe.int/handbook-freedom-of-expression-eng/1680732814>> accessed 5 September 2023.

⁶¹ *Petra v Romania* App no 27273/95 (ECtHR, 23 September 1998), para 47 (‘they go no further than indicating in a very general way the right of convicted prisoners to receive and send mail and they give prison governors the power to keep any letter or any newspaper, book or magazine “unsuited to the process of rehabilitating a prisoner”’).

where the implementation of the law consists of secret measures, not open to scrutiny by the individuals concerned or by the public at large, the law itself, as opposed to the accompanying administrative practice, must indicate the scope of any discretion conferred on the competent authority with sufficient clarity, having regard to the legitimate aim of the measure in question, to give individual adequate protection against arbitrary interference.⁶²

This is not to say that regulators cannot act upon imminent threats. The ECtHR recognises that authorities are allowed to intervene against protesters or speakers when there is ‘a clear and imminent danger’.⁶³ However, due to the nature of the annual risk cycle, the imminence of risks are usually considered according to the society’s sense of urgency, and not in the sense of urgency in specific situations. In fact, the DSA’s incorporation of a crisis response mechanism in Article 36 demonstrates that the Commission’s ability to swiftly act in crises required a specific channel to be possible. Only in special circumstances, the Commission can ‘require’ VLOPs/VLOSEs to ‘identify and apply specific, effective and proportionate measures... to prevent, eliminate or limit any such contribution to the serious threat’. And even then, as argued above, the legality principle limits interventions in case the risk emanates from lawful content.

13.5 The Bigger Cycle of Risk Mitigation

My proposed reading does not mean abdicating the protective goals of the DSA. It means recognising that where the DSA hits its limits, the Member States’ parliaments must be engaged again. The risk mitigation cycle explicitly laid out by the DSA’s provisions is not the full picture. Implicitly, the bigger risk mitigation cycle envisaged by the DSA also involves parliaments that can change the underlying content rules subject to established democratic procedures. The bigger risk mitigation cycle is represented in Figure 13.2.

The DSA consciously distinguishes between legal and illegal content. The latter category is defined by national or European rules adopted by legislatures. Content rules across the EU can differ, and even conflict. They can be vague and unclear. However, to the extent that they are proportionate, they are backed by the legitimacy of legislatures.

The legislatures can tailor their responses to protect the rights of others, for instance, by qualifying the prohibitions. They can prohibit in one place what is legal in another. For instance, the Audiovisual Media Services Directive (AVMSD) prohibits video-sharing providers from allowing minors to ‘normally’ access ‘harmful content’ that may ‘impair the physical, mental or moral development of minors’.⁶⁴ Yet, no such prohibition usually applies to kiosks or shopping malls. But that does not mean that the

⁶² *Leander v Sweden* App no 9248/81 (ECtHR, 26 March 1987), para 51.

⁶³ *Primov and others v Russia* App no 17391/06 (ECtHR, 12 June 2014); *Gül and others v Turkey* Application no 4870/02 (ECtHR, 8 June 2010), para 42.

⁶⁴ AVMSD, art 6a.

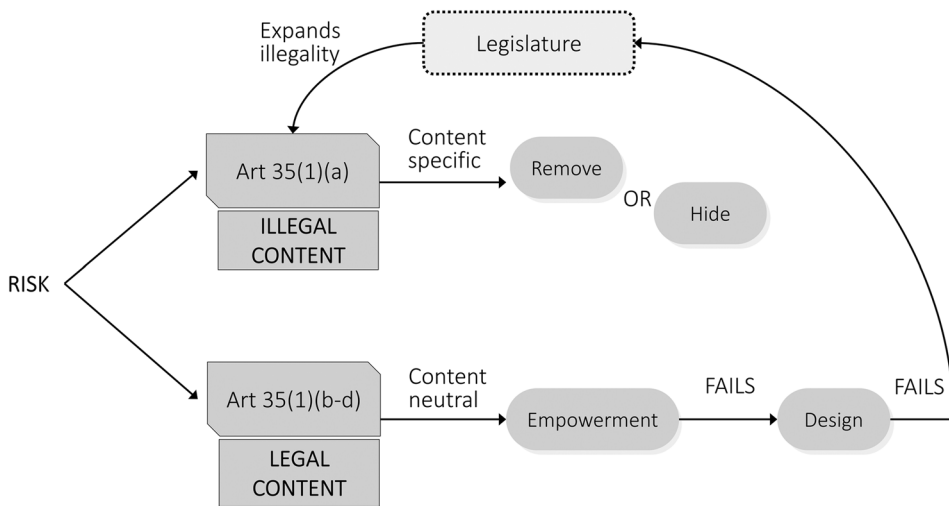


Figure 13.2 The DSA's bigger cycle of risk mitigation

rule cannot be justified. On the contrary, such different treatment is arguably a way of tailoring the applicability of prohibitions to reduce exposure to harm. Reducing ease of access is a strategy that has been used for years.⁶⁵

For instance, many countries regulate what food schools can offer to children even though the same children can buy any products once they leave school premises.⁶⁶ Similarly, we ban tobacco advertising, selling of cigarettes to children, heavily tax products, and regulate packaging, but still allow them to be sold to a part of the public despite scientific consensus about their harms and social costs.⁶⁷ In the digital realm, we ask search engines to delist some personal data, even though the same information can perfectly legally stay on the websites of newspapers.⁶⁸ Thus, prohibiting the same conduct or expression in one context (eg in schools), while allowing it in another (eg in public spaces), is not that unusual. It can be a proportionate way of restricting freedoms.

If the regulators under a risk-based approach like the DSA identify risks stemming from lawful expressions that should be contained, and no amount of empowerment or content-neutral redesign helps, they can gather the evidence and inform the parliamentarians. The DSA's data access tools can facilitate the identification and documentation of risks and thus play an important in the pre-legislative debate.

However, the question is ultimately political. As such, it is then up to the public debate to not only determine whether something should be prohibited as illegal content but also how and for whom it should be prohibited. For instance, disinformation

⁶⁵ Consider, for instance, the UK's Obscene Publications Act of 1857 which criminalised the sale and distribution of obscene material but not its possession.

⁶⁶ Patricia Lucas and others, 'Preschool and School Meal Policies: An Overview of What We Know about Regulation, Implementation, and Impact on Diet in the UK, Sweden, and Australia' (2017) 9(7) *Nutrients* 736.

⁶⁷ Michael K Cummings, 'Programs and Policies to Discourage the Use of Tobacco Products' (2002) 21(48) *Oncogene* 7349.

⁶⁸ Case C-131/12 *Google Spain SL and Google Inc v AEPD and Mario Costeja González* ECLI:EU:C:2014:317.

causing eating disorders might be prohibited as a class of content only for children, on some platforms, if distributed in large amounts, in advertising, or when used in carrying out a business activity. These tailoring options soften the impact on freedom of expression. The legislature's political decision is then open to public scrutiny and eventually constitutional scrutiny by courts. If such laws are adopted, the DSA apparatus lends them more enforcement powers.

However, regulatory expectations should be aligned with the justification for the intervention. No one expects that banning smoking on TV will magically cause people to stop smoking. It is merely a mitigation strategy.

Many risks observed on digital services are only the visible digital tip of the iceberg of larger societal problems lurking in the offline world. By definition, digital policy often cannot 'solve' age-old problems that pre-date such technology. Terrorism cannot be 'solved' by getting rid of all terrorist content from social media. Its removal might help to reduce the radicalisation of youth, but it will not 'solve' terrorism. Similarly, no perfect enforcement of hate speech rules will eradicate racist thinking. Thus, the expectations of the interventions should be commensurate with the fact that digital services only reflect the tip of the iceberg.

The DSA's statutory language appears realistic. It speaks of 'risk mitigation' across the recitals and in the all-important Article 35, which asks VLOPs and VLOSEs to 'put in place reasonable, proportionate and effective mitigation measures, tailored to the specific systemic risks'. The regulation does not talk about the eradication of risks. Instead, it emphasises the special place of freedom of expression (Recitals 86 and 90) as the brake on over-enforcement. But as I noted earlier, the big question for the future is whether the regulators will remain equally measured when enforcing the law.

Fair Design Practices

14.1 Introduction	285	14.3.3 Advertising on VLOSEs	302
14.2 Design of Recommender Systems	288	14.3.4 Ban on ads using profiling of sensitive data (Article 26(3))	303
14.2.1 Transparency of recommender systems (Article 27)	291	14.3.5 Ban on ads using profiling of children (Article 28(2))	304
14.2.2 User choice on VLOP recommender systems (Article 38)	293	14.4 Design of User Experience	305
14.2.3 Recommender systems on VLOSEs (Articles 27 and 38)	295	14.4.1 Dark patterns (Article 25)	305
14.3 Design of Advertising	296	14.4.2 Child protection by design (Article 28)	311
14.3.1 Advertising transparency on platforms (Articles 26(1) and (2))	297	14.5 Business-to-Consumer Marketplaces	313
14.3.2 Advertising archives on VLOPs (Article 39)	299	14.6 Conclusion	314

14.1 Introduction

In 1999, Lawrence Lessig observed that the technological choices of cyberspace architects, such as the design of digital services, are equally as capable of constraining individuals as other forms of regulation. He called the effect ‘Code is Law’.¹ Twenty-three years later, even in today’s increasingly complex digital ecosystem, his observations still ring true. The design of digital services as communication tools can have profound effects on cooperation and conflict between people, including when it might escalate to violence.²

Although product design is seemingly neutral, it inadvertently results in certain effects—whether positive or negative—due to baked-in incentives. The Digital Services Act (DSA) thus focuses heavily on these all-important technological choices. The underlying assumption is that product design is oftentimes jointly responsible, along with social phenomena, for influencing the behaviour of users and the societal impact of content shared on these services. Having the power to alter the design thus holds the keys to important changes in user behaviour. Undoubtedly,

¹ Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books 1999).

² Jonathan Stray, Ravi Iyer, and Helena Puig Larrauri, ‘The Algorithmic Management of Polarization and Violence on Social Media’ (*Knight First Amendment Institute at Columbia University*, 22 August 2023) <<http://knightcolumbia.org/content/the-algorithmic-management-of-polarization-and-violence-on-social-media>> accessed 10 September 2023.

inspiration from financial regulation runs in the veins of risk mitigation provisions of the DSA.³

To understand the broader policy debates, consider the case of Omegle, an anonymous chat service randomly pairing strangers online for video or text-based chat, that shut down in November 2023 as a result of a United States (US) settlement.⁴ Omegle's mixture of design decisions allowing full anonymity, zero cost and authentication, ephemeral content, and one-on-one random matching of individuals, made it very attractive for paedophile predators. While the service settled based on US product liability claims, as explained in Chapter 6, these would have been very difficult to divorce from the claims for user-generated behaviour. As persuasively argued by Goldman:⁵

Consider this thought exercise: Imagine that Omegle matched a minor with an adult but never allowed them to communicate with each other (no text, no audio, no video). ... if the problem is the matching and not the content, then Omegle violated the alleged duty to the minor simply by making this 'match'. Of course, this makes no sense. The minor has not been harmed in this circumstance and could not possibly be harmed by the adult. That's because the match itself, without any interaction, doesn't cause any problem. So the plaintiff's case absolutely does depend on third-party content—that's the only possible source of the harm.

Thus, product liability, even under the European Union (EU) law, is unlikely to become a workaround for the DSA liability exemptions in many cases. The EU legislature, recognising the need to impose some binding rules upon more impactful providers, decided to approach the problem in two basic ways: detailed prescriptive rules for medium-sized online platforms based on a traditional command-and-control approach and risk-based regulation for the most impactful players whose operations are of systemic significance. Creating a regulatory approach to the design of services arguably relieves the pressure that would have otherwise been put on the liability exemption systems. It allows for increased accountability to be more focused without increasing liability for everything that happens online (Chapter 21).

The key benefit of these provisions is that they can measure responsibility by the size of operations (eg mid-sized vs small companies) and the types of stakeholders (eg children vs adults) and invite more co-regulation. Had the legislature decided to lift liability exemptions to achieve the same goal, the result would have been an undifferentiated

³ European Commissioner Thierry Breton: 'We are imposing new risk-based obligations on very large platforms to prevent abuse—as has been done with prudential rules for banks', see Thierry Breton (Commissioner), 'Speech by Commissioner Breton on the Digital Services Act' (*EU Commission*, 19 January 2022) <https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_22_431> accessed 5 September 2023.

⁴ See BBC, 'Omegle: 'How I Got the Dangerous Chat Site Closed Down'', available at <<https://www.bbc.com/news/technology-67485561>> (BBC, 22 November 2023) accessed 18 December 2023.

⁵ See Eric Goldman, 'Omegle Denied Section 230 Dismissal—AM v. Omegle', available at <<https://blog.ericgoldman.org/archives/2022/07/omegle-denied-section-230-dismissal-am-v-omegle.htm>> (*Technology & Marketing Law Blog*, 20 July 2022) accessed 18 December 2023.

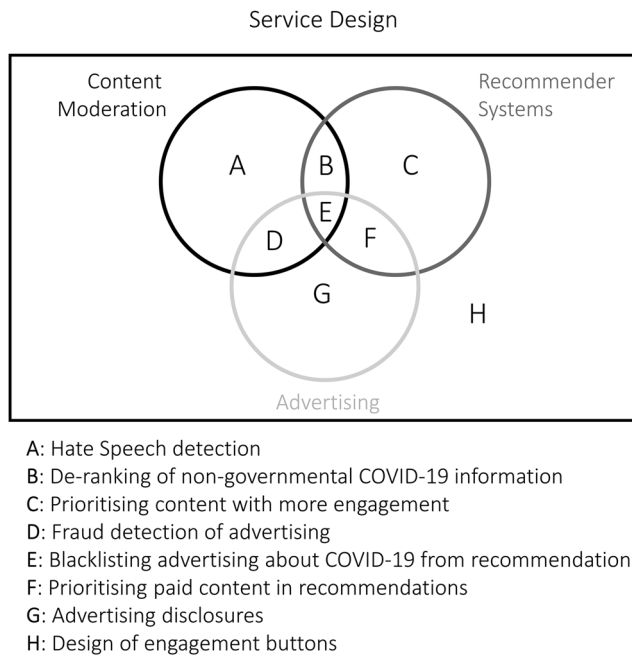


Figure 14.1 Parts of services

exposure to all sorts of legal risks created by the users of services. Thus, the regulation of the design of services is a more proportionate way to discipline self-interest by ex ante expecting the companies to protect the selected values and interests. Even such targeted regulation, however, is not without consequences. It might make some popular and more risky services simply unviable as free-of-charge operations because of the implied compliance costs.

While the DSA does not explicitly frame the prohibitions and prescriptions regarding the design of services as ‘fair practices’, the rationale of fairness arguably underlies the relevant provisions. For instance, the substantive prohibitions related to manipulative and aggressive practices are already questions of fair practices. The same can be said about data-protection-related practices in platform advertising, which underlie a general principle of fairness.⁶ Other obligations imposed by the DSA, such as the protection of children, can equally be framed as fair practices that protect the interests of children in the design of services. In practice, the concept of *fair design practices* overlaps with *fair rules* and *fair process* principles underlying content moderation (see Figure 14.1).

⁶ On role of fairness in data protection law, see Damian Clifford and Jef Ausloos, ‘Data Protection and the Role of Fairness’ [2017] CiTiP Working Paper 29/2017 <<https://papers.ssrn.com/abstract=3013139>> accessed 5 September 2023.

14.2 Design of Recommender Systems

Recommender systems, such as video autoplay, newsfeeds, suggested ads, or trending topics, are the core features of many digital services. On YouTube, they drive 70% of the viewed content;⁷ on TikTok, it is 90–95%.⁸ The recommender systems are instrumental in orchestrating user experience and securing the companies' bottom line. The studies show that predicted engagement is a significant factor that influences the content that users are served.⁹ Small design changes, such as reducing engagement-based ranking for health-related content, can significantly decrease disinformation and negative reactions.¹⁰

The DSA defines recommender systems (Article 3(s)) as follows:

... fully or partially automated system used by an online platform to suggest in its on-line interface specific information to recipients of the service or prioritise that information, including as a result of a search initiated by the recipient of the service or otherwise determining the relative order or prominence of information displayed.

The DSA only regulates what Cobbe and Singh call 'open recommending'.¹¹ Unlike 'curated recommending', which recommends from within editorial content, such as on websites of media or streaming services, 'open recommending' recommends from the pool of content not specifically vetted in any way.¹² Open recommending operates on a much larger scale and with a wider pool of potential information to recommend.¹³ It is therefore inherently more risky.

The definition thus includes all types of typical recommender systems, such as newsfeeds on social media, ranking on the front pages of video-sharing platforms, search tools on marketplaces or app stores, or matching tools on online dating or short-term accommodation apps. The crucial legal requirement is that an automated system

⁷ Joan Solsman, 'YouTube's AI is the Puppet Master over Most of What You Watch' (*CNET*, 10 January 2018) <<https://www.cnet.com/tech/services-and-software/youtube-ces-2018-neal-mohan/>> accessed 5 September 2023.

⁸ Wall Street Journal, 'Investigation: How TikTok's Algorithm Figures Out your Deepest Desires' (*WSJ Video*, 21 July 2021) <https://www.wsj.com/video/series/inside-tiktoks-highly-secretive-algorithm/investigation-how-tiktok-algorithm-figures-out-your-deepest-desires/6C0C2040-FF25-4827-8528-2BD6612E3796?mod=hp_lead_pos5> accessed 5 September 2023.

⁹ Akos Lada, Meihong Wang, and Yan Tak, 'How Does News Feed Predict What You Want to See?' (*Tech at Meta*, 26 January 2021) <<https://tech.facebook.com/engineering/2021/1/news-feed-ranking/>> accessed 5 September 2023; Arvind Narayanan, 'Twitter Showed Us Its Algorithm. What Does It Tell Us?' (*Knight First Amendment Institute at Columbia University*, 10 April 2023) <<http://knightcolumbia.org/blog/twitter-showed-us-its-algorithm-what-does-it-tell-us>> accessed 5 September 2023.

¹⁰ David Klepper and Amanda Seitz, 'Facebook Froze as Anti-Vaccine Comments Swarmed Users' (*AP News*, 26 October 2021) <<https://apnews.com/article/the-facebook-papers-covid-vaccine-misinformation-c8bbc569be7cc2ca583dad4236a0613>> accessed 5 September 2023.

¹¹ Jennifer Cobbe and Jatinder Singh, 'Regulating Recommending: Motivations, Considerations, and Principles' (2019) 10(3) *European Journal of Law and Technology*.

¹² *ibid* 2.

¹³ Paddy Leerssen, 'The Soap Box as a Black Box: Regulating Transparency in Social Media Recommender Systems' (2020) 11(2) *European Journal of Law and Technology* 7.

employed by a platform influences the *order or prominence of the information it displays*. Thus, a suggestion tool, prioritisation screen, ranking, or personalisation are all within that scope if they influence what users see. It should be noted, however, that ranking in the generalist search engines that compile their search results by crawling the Web is covered by a particular regulatory situation described below.

The term ‘recommender systems’ is, therefore, broader than ‘ranking’, which is relied upon by transparency rules in Article 5 of the Platform-to-Business Regulation (P2BR).¹⁴ In that context, the ranking means determining ‘the relative prominence given to the goods or services offered through online intermediation services, or the relevance given to search results by online search engines’.¹⁵ The provision on recommender systems in Article 27 DSA could be considered broader on the one hand because it covers the order or prominence of *any information* provided by recipients of the service, not only goods or services. Hence, it goes beyond the purely commercial recommendations.

The clear source for concerns around recommender systems was the Cambridge Analytica scandal, which unearthed various techniques of voter manipulation using psychographic profiles, determining users’ personality traits based on their activity on social media.¹⁶ Most famously, the company helped micro-target the political campaign of the US President Donald Trump in 2016.¹⁷ The Cambridge Analytica scandal and the following Mueller investigations¹⁸ into Russian election interference informed the EU policymaking on the question of risk mitigation and recommender systems for very large services.

At the time of writing, social sciences are still trying to work out the exact impacts of recommender systems on individuals.¹⁹ However, it is broadly accepted that the amplification of content through recommender systems is an important information distribution channel that impacts individuals. Recommender systems are conceptualised as ‘indirect editorial influence’²⁰ and generally ‘a gentler intervention’ to content distribution.²¹

¹⁴ European Parliament and Council Regulation (EU) 2019/1150 on promoting fairness and transparency for the business users of online intermediation services [2019] OJ L186/57 (P2BR) art 5.

¹⁵ *ibid* art 2(8).

¹⁶ Alexandra Ma and Ben Gilbert, ‘Facebook Understood How Dangerous the Trump-Linked Data Firm Cambridge Analytica Could be Much Earlier than It Previously Said. Here’s Everything That’s Happened up until Now.’ (*Business Insider*, 23 August 2019) <<https://www.businessinsider.com/cambridge-analytica-a-guide-to-the-trump-linked-data-firm-that-harvested-50-million-facebook-profiles-2018-3>> accessed 5 September 2023.

¹⁷ Matthew Rosenberg, Nicholas Confessore, and Carole Cadwalladr, ‘How Trump Consultants Exploited the Facebook Data of Millions’ *The New York Times* (17 March 2018) <<https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>> accessed 5 September 2023.

¹⁸ See Robert S Mueller, ‘Report On The Investigation Into Russian Interference In The 2016 Presidential Election’ (US Department of Justice 2019) vol 1 <<https://www.justice.gov/archives/sco/file/1373816/download>> accessed 29 August 2023.

¹⁹ See Eli Pariser, *The Filter Bubble: What the Internet Is Hiding from You* (Penguin Books 2012); Cass R Sunstein, *Republic.Com* (Princeton UP 2002); Axel Bruns, *Are Filter Bubbles Real?* (Polity Press 2019); Frederik J Zuiderveen Borgesius and others, ‘Should We Worry about Filter Bubbles?’ (2016) 5(1) Internet Policy Review <<https://policyreview.info/node/401>> accessed 10 September 2023.

²⁰ Natali Helberger, Katharina Kleinen-von Königslöw, and Rob van der Noll, ‘Regulating the New Information Intermediaries as Gatekeepers of Information Diversity’ (2015) 17(6) Info 50, 52–54.

²¹ Tarleton Gillespie, ‘Platforms Intervene’ (2015) 1(1) Social Media & Society. The case law of the ECtHR comes to a similar conclusion, see ch 3.

The DSA is influenced by the zeitgeist of the past decade, which saw recommendation algorithms as an important cause of polarisation and radicalisation in society. The link between recommender systems and radicalisation is an ongoing research agenda that is unlikely to deliver obvious answers anytime soon. Perhaps because of the early stage of our understanding, the approach taken is more light-handed than some would have liked. After all, as noted by Ananny and Crawford, ‘a system must be understood to be governed.’²² The DSA’s due diligence obligations are a step to establishing a better understanding.

Recital 70 justifies the regulation in this area by invoking the significant societal impact of these recommendations, especially given their role in the ‘amplification of certain messages, viral dissemination of information, and stimulation of online behaviour.’ Thus, while the provisions on the recommender systems are concerned with amplification through the platform’s algorithmic selection, such as newsfeeds, regulatory intervention is equally grounded in worries about spillovers to viral dissemination of information in the networks.

These concerns are often articulated differently through the phenomenon of ‘filter bubbles.’ A report by the Oxford Reuters Institute defines a filter bubble as ‘a state of intellectual or ideological isolation that may result from algorithms feeding us the information we agree with, based on our past behaviour and search history.’²³ The phenomenon is sometimes also referred to as ‘rabbit holes,’ especially to emphasise that such bubbles can lead to radicalisation.

In 2020, the New York Times ran a very impactful podcast series documenting how users can be driven to radicalisation by YouTube’s recommendation algorithm.²⁴ The term ‘filter bubbles’ is closely related to the concept of ‘echo chambers.’ An echo chamber describes the state in which an individual is overexposed to one type of narrative which can lead to a distorted view of how widely shared it is among others. While echo chambers result from algorithms, they can also result from people’s choices (eg watching and reading only newspapers close to one’s political worldview). Thus, the regulator’s concern about filter bubbles is about *pre-selected personalisation* rather than *self-selected personalisation*.²⁵

The social science research on ‘filter bubbles’ is far from settled, particularly in regards to the questions of *if* and *how* algorithms drive polarisation, including the individual’s role in it.²⁶ In a recent series of studies published in *Nature* and *Science*,²⁷ the researchers

²² Mike Ananny and Kate Crawford, ‘Seeing without Knowing: Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability’ (2018) 20(3) *New Media & Society* 973.

²³ Richard Fletcher, ‘The Truth behind Filter Bubbles: Bursting Some Myths’ (*Reuters Institute for the Study of Journalism, University of Oxford*, 24 January 2020) <<https://reutersinstitute.politics.ox.ac.uk/news/truth-behind-filter-bubbles-bursting-some-myths>> accessed 10 September 2023. The term was originally coined by Pariser to mean ‘a unique universe of information for each of us,’ see Pariser (n 19) 9.

²⁴ The New York Times podcast, ‘Rabbit Hole’ (2020) <<https://www.nytimes.com/column/rabbit-hole>> accessed 10 September 2023.

²⁵ Zuiderveen Borgesius and others (n 19).

²⁶ Leerksen (n 13) 5.

²⁷ See Andrew M Guess and others, ‘How do Social Media Feed Algorithms Affect Attitudes and Behavior in an Election Campaign?’ (2023) 381(6656) *Science* 398; Sandra González-Bailón and others, ‘Asymmetric Ideological Segregation in Exposure to Political News on Facebook’ (2023) 381(6656) *Science* 392; Brendan Nyhan and others, ‘Like-Minded Sources on Facebook are Prevalent but Not Polarizing’ (2023) 620(7972) *Nature* 137.

found that while political polarisation is rampant on Facebook, it is unclear how much it can be attributed to the company's algorithm. There are many possible explanations, including, as explained by Fletcher before the studies were published:

Most of the best available independent empirical evidence seems to suggest that on-line news use on search and social media is more diverse. But there's a possibility that this diversity is causing some kind of polarisation, in both attitudes and usage. This is interesting, because in some ways it's the opposite of what the filter bubble hypothesis predicted. The hypothesis states that we'll actually get less diversity and there'll be negative consequences from that. So the end result might be the same. But the hypothesis fails to capture the mechanisms.²⁸

Despite the well-known concerns about the impact of recommender systems on the quality of democracy, the DSA makes only very modest explicit regulatory intervention. As was the case with the P2BR, the law is first tasked to imbue further clarity about how these systems operate. The DSA seeks to achieve this with Article 27.

14.2.1 Transparency of recommender systems (Article 27)

Article 27 requires that medium and larger online platforms build transparency into their products that include recommendation algorithms. However, not all products that generate recommendations are regulated. The DSA's notion of online platforms limits the relevant digital services to those for whom the storage of third-party information and its public distribution is a principal service. This fact alone excludes a series of recommendation engines.

Firstly, it will not apply to any ranking or recommendation of the editorial content, such as on music or movie streaming services or on websites of newspapers. In these cases, the services algorithmically organise editorial content or individually hand-picked third-party content (Chapter 6). Secondly, because of the ancillary nature of the storage, Article 27 is unlikely to apply to any recommendation systems around user comments under news articles or blogs. Interesting border-line cases concern the aggregation services (eg for news) and meta-search engines (eg for used car ads). If these services can be said to source their content from suppliers who 'provided them with information' (Chapter 6), they could, in theory, also be understood as hosting services and eventually online platforms.

The obligations arising from Article 27 are twofold:

- (a) explanation of 'the main parameters used' in the recommender systems, and
- (b) explanation of 'the options ... to modify or influence those parameters' (Article 27(1)).

²⁸ Fletcher (n 23).

These two obligations are owed to recipients of the service, who are the creators of content and anyone exposed to the content. The explanation of the main parameters must be included in the terms and conditions of platforms ‘in plain and intelligible language’.²⁹ The main parameters represent ‘why’ certain information is displayed.³⁰ According to Article 27(2), this *includes* at least:

- (a) the criteria which are most significant in determining the information suggested to the recipient of the service;
- (b) the reasons for the relative importance of those parameters.

Other possible criteria, beyond these two, could be for instance, what personal information was used to tailor the recommendation, such as preferences, location, or personal browsing history.³¹

Article 27 DSA is clearly inspired by Article 5 P2BR, which uses the same approach. It requires transparency as to the main parameters and their explanation in the terms and conditions. While the P2BR’s explanations are owed to businesses, and hence are provided in a commercial environment, the logic underlying the DSA is the same: to allow affected parties to understand why certain information is and is not shown to them. What differs is that the DSA places more emphasis on the actionability following the release of that information. If the choice exists, the information shall serve to facilitate it. The law empowers users to take control and adjust their information ecosystem. The P2BR, in contrast, largely assumes that these decisions are imposed on businesses by the ranking services as their business partners. The rationale is that businesses will adjust their operations and their commercial agreement with platforms based on the information they receive.

During the legislative process, it was discussed whether personalised recommendations should be switched off by default, opted into, or even banned completely. Article 27 clearly does not force online platforms to provide options to modify or influence the recommendations given. The mandatory aspect remains limited to providing information. Article 27(3) only requires that ‘where several options are available’, the users are given ‘a functionality’ that allows them ‘to select and to modify at any time their preferred option’. Such functionality must be ‘directly and easily accessible from the specific section of the online platform’s online interface where the information is being prioritised’ (Article 27(2)). Effectively, therefore, medium and larger platforms, which do not qualify as very large online platforms (VLOPs), are not obligated to offer choice and need only explain the ‘why’ of their recommendations under Article 27. However,

²⁹ DSA, art 27(1).

³⁰ DSA, art 27(2).

³¹ The European Parliament proposed an obligation to explain, ‘if applicable’, ‘the role that the behaviour of the recipients of the service plays in how the relevant system produces its outputs’. While this is not explicitly included in art 27 of the final DSA text, it is not excluded: see European Parliament, ‘Amendments Adopted by the European Parliament on 20 January 2022 on the Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (DSA) and Amending Directive 2000/31/EC (COM(2020)0825 — C9-0418/2020 — 2020/0361(COD))’ [2022] OJ C336/48, art 24a.

if they build options into their recommendation systems (eg for advertisers), they must offer the ability to choose at any time for users in general. As will be discussed below, only VLOPs must take the extra step and design beyond transparency from the outset.

That being said, Article 27 should not be read in isolation. Practices that qualify as ‘recommender systems’ sometimes overlap with practices defined as ‘content moderation.’ For instance, a parameter that automatically de-ranks all information about COVID-19 in the newsfeed which does not originate from governments is likely to qualify as a content moderation activity. The universal obligation in Article 14, including the obligation to be objective, diligent, and proportionate, would thus apply to the inclusion of such parameters. Thus, at least for a subset of activities that form part of the recommender systems, more obligations than a commitment to transparency can apply. The extent to which fairness as a principle applies to the design of digital services that are not VLOPs or very large search engines (VLOSEs) also depends on how broadly courts construe Article 14 (Chapter 12).

14.2.2 User choice on VLOP recommender systems (Article 38)

Very large providers are subject to a special obligation to introduce an opt-out functionality for profiling-based recommendations. The rule was justified by the argument that tailor-made recommendations by VLOPs have been seen as the cause of ‘filter bubbles’ in the context of disinformation, radicalisation, and electoral manipulation.

The intuition behind a mandatory opt-out option for VLOPs in Article 38 is the fact that if ‘filter bubbles’ or ‘echo chambers’ exist and harm our civic choices, allowing individuals to limit their exposure to algorithmically driven content grants them agency. The opt-out option allows individuals to ‘vote’ on the usefulness of algorithms and the extent to which such algorithms serve their needs (as opposed to the purely commercial needs of the platform). Individuals are thus given the option to voice their dislike of algorithms and disable them without having to leave the platforms entirely. Despite this promising backdrop to the provision, the regulatory design of the opt-out is rather half-baked because it gives companies very broad discretion on how to design it.

According to Article 38 DSA, VLOPs simply must ‘provide at least one option for each of their recommender systems which is not based on profiling’. However, there is no obligation that such a non-profiled option is set as default. The exact design of these functionalities remain in the hands of the VLOP. As such, users must actively opt out of profiling-based recommendations on their own accord to access the other options, unless a provider voluntarily offers it as a default choice.

Since the DSA only prescribes *one* non-profiling-based option, this also gives providers a broad range of modalities. The meaning of the term ‘profiling’ is as defined by Article 4 General Data Protection Regulation (GDPR), which is as follows:

[A]ny form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to

analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.³²

Profiling thus covers a wide range of practices. Depending on how strictly the provision is read, potentially many automated systems that use personal data to influence the order or prominence of displayed non-editorial information are likely to qualify as a recommender system based on profiling. This is because any recommendation based on a user's personal data could be argued to inherently include an evaluative or predictive step—a particular user is likely going to find the information interesting or relevant.

If this broad understanding of profiling is adopted, it would effectively mean that platforms must always offer at least one alternative recommendation option that avoids using personal data altogether. A different view would be to allow the use of personal data, but to limit it to recommendations which intend to infer some type of personal characteristics. Typical examples of recommendations that are not based on profiling are: chronological newsfeeds, recommendations of the most popular content, or content that is trending at a particular moment. TikTok recently unveiled its attempt to implement Article 38 by creating an option to switch to a region/language-based feed.³³ Meta, on the other hand, is offering chronological newsfeeds for Facebook and Instagram.³⁴

Besides these baseline obligations, VLOPs are subject to general risk management (Article 34). The DSA explicitly and repeatedly mentions recommendation systems in the context of risk mitigation. For instance, Article 34(2)(a) emphasises that the focus must be on 'the design of their recommender systems and any other relevant algorithmic systems', while Article 35(1)(d) requires 'testing and adapting their algorithmic systems, including their recommender systems'. Finally, according to Article 40(3), 'at the request of either the Digital Services Coordinator of establishment or of the Commission, [VLOPs must] explain the design, logic the functioning and the testing of their algorithmic systems, including their recommender systems'.

The DSA's special rules on recommender systems are thus significantly complemented by the risk-management rules relating to the entire service (Chapter 15). The limited nature of Articles 27 and 38 should not be understood as exhaustive design requirements. On the contrary, it is quite possible that risk assessments will sometimes de facto demand additional design requirements for recommender systems. Given the parallel application together with general risk management, the provision is better understood as a simple baseline.

³² GDPR, art 4(4).

³³ TikTok, 'An Update on Fulfilling our Commitments under the Digital Services Act' (*TikTok Newsroom*, 4 August 2023) <<https://newsroom.tiktok.com/en-eu/fulfilling-commitments-dsa-update>> accessed 5 September 2023.

³⁴ Facebook, 'New Features and Additional Transparency Measures as the Digital Services Act Comes into Effect' (*Facebook Newsroom*, 22 August 2023) <<https://about.fb.com/news/2023/08/new-features-and-additional-transparency-measures-as-the-digital-services-act-comes-into-effect/>>.

14.2.3 Recommender systems on VLOSEs (Articles 27 and 38)

As discussed in Chapter 7.5, the position of search engines in the DSA's framework is far from settled. Recital 28 DSA mentions them as services that are covered by the DSA 'to the extent that they qualify as "mere conduit", "caching" or "hosting" services'. Even under the E-Commerce Directive (ECD), the situation of search engines was also highly disputed. Some courts understood the framework to not include them, while other courts tried to categorise its various parts as either caching or hosting. The DSA adds to the complexity. It clearly signals that search engines are not excluded from the DSA and can even be covered by many of its provisions. It also comes up with special provisions for VLOSEs to ensure that the various components of search engines are covered as complex products in their entirety.

Accordingly, search engines are currently covered by the DSA as follows:

- Search engine services in their entirety are covered by the DSA by special provisions on VLOSEs in section 5 of the 'due diligence' chapter; it applies only to search engines that reach the threshold of 45 million monthly active users.
- Parts of search engine services are covered by other DSA provisions on online platforms and hosting services if they qualify as storage of third-party information (eg keyword advertising); these provisions apply even to search engines that are not large. In my view, even the hyperlinks and excerpts in the organic search results could qualify as hosting.

As a result, recommendation systems of VLOSEs are subject to the same rules as those for VLOPs.³⁵ Article 38 introduces a mandatory choice as an add-on to the transparency requirements of Article 27. Both provisions thus apply to VLOSEs and means that they must allow their users to opt out of the personalisation of their search results when using their services. This applies to both natural as well as paid search results as they both constitute recommendations. Moreover, in addition to these mandated options, VLOSEs might be requested to go further to mitigate systemic risks.

The situation is much more complicated for search engines that are *not* very large. For them, the keyword advertising recommendation tool could be within the remit of Article 27 only if it constitutes an online platform. Furthermore, if the links and excerpts in the search results can qualify as hosting, and moreover its providers as online platforms (Chapter 7), Article 27 could also apply to natural search results.³⁶ The P2BR

³⁵ See Rec 90 DSA. Only the version agreed upon in the summer of 2022 by the European Parliament and Council made the applicability of art 38 DSA crystal clear because, during the legislative process, the European Parliament had omitted VLOSEs in their proposed amendments of what was then Rec 59. See General Secretariat of the Council, 'Information note on Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (DSA) and amending Directive 2000/31/EC - Outcome of the European Parliament's first reading (Strasbourg, 4–7 July 2022)' (2022) Document 10967/22, 84 (Rec 59); cf European Parliament (n 31) 100 (Amendment 64, Rec 59).

³⁶ However, it is very unlikely to apply to the suggestion tool which is generated by aggregating popular queries of users.

already applies to search engines of all sizes. Article 5 P2BR includes transparency criteria, including the role of remuneration for such ranking; however, this is only for the benefit of business users.

14.3 Design of Advertising

Online platforms that integrate advertising into their services must comply with two design requirements. They must: a) make sure that advertisements are accompanied by appropriate disclosures (Articles 26(1)–(2)); and b) cease providing some profiling-based ads to advertisers (Articles 26(3) and 28(2)).

An ‘advertisement’ is defined as ‘information designed to promote the message of a legal or natural person, irrespective of whether to achieve commercial or non-commercial purposes and presented by an online platform on its online interface against remuneration specifically for promoting that information’ (Article 3(r)). This means that the sole defining criterion is *remuneration to promote some information*. Thus, regardless of the cause, or the nature of the beneficiary, whenever the platforms gain something in return for the promotion of information, they must treat the underlying information as an advertisement. This means that not only regular types of advertisements are captured. The notion of promotion is very broad but arguably should not capture situations when the end-users simply pay for access to the platform. For instance, if a trader pays a fee to join the platform, but its content is not in any case pushed to consumers, there is no remuneration for promotion. On the other hand, paying to boost the ranking of its content that was posted free of charge would certainly turn the information into an advertisement. The same applies to organic content shared by the campaigns of NGOs, political parties, or charities to raise money—these would qualify as advertising if they were promoted by the platform for remuneration.

The difficult question could be how to treat *recommendation engines* that promote some type of content not based on per-item promotion but on a characteristic of the concerned content creator. An example of this is if a news organisation receives a boost for its content through a recommendation engine of a platform, although it did not pay for such a boost but receives it as a part of a broader effort to promote high-quality content. In my view, if such a promotion is not part of a quid pro quo agreement with the provider, the promotion would not qualify as advertising. However, if the changes to the recommendation engines to promote certain content creators are based on existing collective licensing agreements, such a boost could qualify as an advertisement (eg promotion of licensed news). This would, in turn, trigger not only labelling, attribution, and funding disclosures but also the requirements to report on the exposure of such ads and a ban on profiling based on sensitive categories of data. The crucial takeaway, however, is that the results of recommendation systems that get promoted ahead of other content can equally qualify as advertising, along with all the consequences.

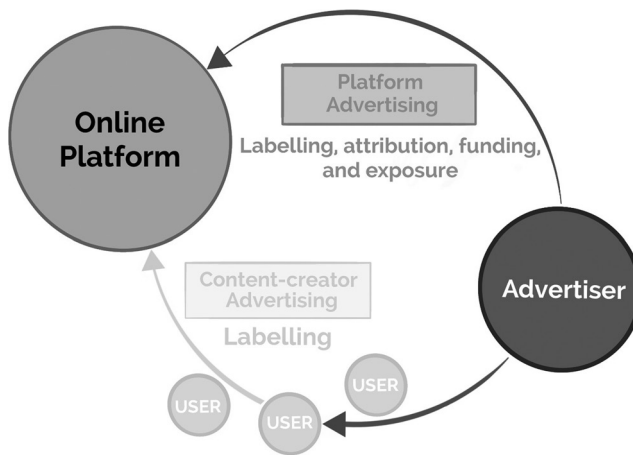


Figure 14.2 Redistribution of power

14.3.1 Advertising transparency on platforms (Articles 26(1) and (2))

Advertising online has two main shortcomings. *Platform-run advertising* can be opaque as to who is behind the advertisement, creating other risks, such as voter manipulation or disinformation. Ever since the Cambridge Analytica scandal,³⁷ pressure has been placed on online platforms to introduce transparency into who advertises on their services and using what parameters. *Content-creator-run advertising*, on the other hand, can be entirely concealed. Online influencers are known to sometimes engage in product placement without properly disclosing this.³⁸ Kim Kardashian recently settled charges brought against her in the US and paid \$1.26 million in penalties, disgorgement, and interest for failing to disclose financial incentives to promote some cryptocurrencies.³⁹ Figure 14.2 depicts the difference between two types of advertising.

In a bid to mitigate the former issue, Article 26(1) provides that online platforms must design their service in a way that allows the disclosure of relevant information ‘in a clear, concise and unambiguous manner and in real time’. The relevant information is limited to the following: (a) disclosure that the content in question is an advertisement, including through prominent markings (labelling); (b) on whose behalf the advertisement is being presented (attribution); (c) who eventually paid for the advertisement

³⁷ Nicholas Confessore, ‘Cambridge Analytica and Facebook: The Scandal and the Fallout So Far’ *The New York Times* (4 April 2018) <<https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>> accessed 5 September 2023.

³⁸ For empirical research on the scope of the problem, see Arunesh Mathur, Arvind Narayanan, and Marshini Chetty, ‘Endorsements on Social Media: An Empirical Study of Affiliate Marketing Disclosures on YouTube and Pinterest’ (2018) 2(CSCW) Proceedings of the ACM on Human-Computer Interaction 1.

³⁹ US Securities and Exchange Commission, ‘SEC Charges Kim Kardashian for Unlawfully Touting Crypto Security’ (*SEC Newsroom*, 3 October 2022) <<https://www.sec.gov/news/press-release/2022-183>> accessed 5 September 2023.

(funding); and (d) the main parameters used to determine who will see the advertisement and how to change them, where applicable (exposure).

The exposure information mentioned in (d) must be ‘directly and easily accessible from the advertisement’, which suggests the relevant information should somehow form part of the advertising screen. The reference to information about how to deactivate certain parameters is quite interesting, as the provision does not directly mandate that users should be able to switch it off. It thus only informs about the choice if it exists. If it does not exist—as there is no way to opt out—the provider should, in my view, inform the users about this as well.

However, the relevant information must be disclosed only by advertisers dealing directly with the platform using its advertising structure. Therefore, to address the latter issue relating to advertisers who deal directly with content creators, such as influencers, on a platform, Article 26(2) introduces another requirement centered around facilitating the labelling of such sponsored user-generated content. Despite the different contexts, however, this obligation again applies only to platforms, not influencers. Platforms must provide the functionality to declare that the content ‘is or contains commercial communications’ (Article 26(2)), including through prominent markings. The markings for advertising are expected to be standardised in both situations to facilitate user recognition. Article 26(2) uses the term ‘commercial communication’ instead of advertising.⁴⁰ Its meaning is understood to be defined by the ECD as follows:

any form of communication designed to promote, directly or indirectly, the goods, services or image of a company, organisation or person pursuing a commercial, industrial or craft activity or exercising a regulated profession. The following do not in themselves constitute commercial communications:

- information allowing direct access to the activity of the company, organisation or person, in particular a domain name or an electronic mail address;
- communications relating to the goods, services or image of the company, organisation or person compiled in an independent manner, particularly when this is without financial consideration;⁴¹

Thus, unlike advertising, commercial communication only targets for-profit activities. The concept is still to be understood rather broadly. The Court of Justice of the European Union (CJEU) recently clarified in the context of a different directive that ‘paid for’ content includes any ‘consideration with an asset value’, whether it takes ‘the form of payment of a sum of money or in any other form’, as long as there ‘is a definite link between the payment and consideration.’⁴² This also includes free-of-charge licensing of images protected by copyright. Despite this broad framing, which

⁴⁰ Art 3(w) DSA states that ‘commercial communication’ means ‘commercial communication’ as defined in art 2 (f), of Directive 2000/31/EC.

⁴¹ ECD, art 2(f).

⁴² The CJEU interpreting the concept of ‘paid for’ in the Unfair Commercial Practices Directive in Case C-371/20 *Peek & Cloppenburg KG v Peek & Cloppenburg KG* ECLI:EU:C:2021:674, para 49.

catches many practices of users such as influencers,⁴³ some practices, such as promoting political parties, may remain out of the scope of the provision. However, illegal political communication within such systems can be considered under general risk management.

This outcome is a curious split between advertisers who deal with platforms and the content creators of those platforms. The former type of advertising is much more regulated while the latter is subject to limited labelling rules imposed on platforms and not content creators. Some types of paid promotions, such as political advertising, arguably fly entirely under the DSA's radar. This is partly understandable because online platforms wield much more power over their audiences than regular users acting as content creators; however, some content creators can become equally powerful.

Influencers with millions of followers can inflict harm on a scale that is comparable to that of other platforms, especially if the impact is further amplified in networks by other users.⁴⁴ Thus, the glaring gap left by the DSA concerns the 'super-users' of online platforms who are subject to the same minimalistic rules that make much more sense for entry-level users than for sophisticated users who earn millions of euros annually through their endorsements. The question of super-users thus remains a primary candidate for discussion and oversight under the Codes of Conduct, general risk management, and national experimentation. In any case, if national⁴⁵ or European consumer law demands disclosures by super-users,⁴⁶ a failure to do so qualifies as illegal content for the purposes of the DSA with all the relevant mechanisms.

14.3.2 Advertising archives on VLOPs (Article 39)

For VLOPs, Article 39 DSA sets out an additional obligation to set up advertising archives. Any advertisement the provider handles must be publicly disclosed in the archive,

⁴³ See Jan Trzaskowski, 'Identifying the Commercial Nature of "Influencer Marketing" on the Internet' in Peter Wahlgren (ed), *50 years of law: the Swedish Law and Informatics Research Institute 1968-2018* (Stockholm Institute for Scandinavian Law 2018).

⁴⁴ See generally, Cătălina Goantă and Sofia Ranchordás (eds), *The Regulation of Social Media Influencers* (Edward Elgar Publishing 2020); Frithjof Michaelsen and others, 'The Impact of Influencers on Advertising and Consumer Protection in the Single Market' (Study Requested by IMCO committee, PE 703350, European Parliament 2022) <[https://www.europarl.europa.eu/RegData/etudes/STUD/2022/703350/IPOL_STU\(2022\)703350_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2022/703350/IPOL_STU(2022)703350_EN.pdf)> accessed 5 September 2023.

⁴⁵ According to AVMSD, some influencers are media service providers that are subject to notification, and publication in an official registry according to art 2(5b) AVMSD. The central database is at: European Audiovisual Observatory, 'Database on Audiovisual Services and Their Jurisdiction in Europe' (*Mavise*) <<http://mavise.obs.coe.int/>> accessed 5 September 2023. This has already caused some controversies in some EU countries, see European Parliament, 'Parliamentary Question: Answer given by Mr Breton on Behalf of the European Commission' (Question P-000261/2023(ASW), 2023) <https://www.europarl.europa.eu/doceo/document/P-9-2023-000261-ASW_EN.html> accessed 5 September 2023. French parliament adopted its new law about influencers: Simone Shah, 'France is Cracking Down on the Influencer Industry' (*Time*, 8 May 2023) <<https://time.com/6277524/france-influencer-marketing-regulation-social/>> accessed 30 August 2023.

⁴⁶ See Christine Rief and Laura Clausen, 'Towards Fairness in Digital Influencers' & #146; Marketing Practices' (2019) 8(2) Journal of European Consumer and Market Law; Giovanni De Gregorio and Catalina Goanta, 'The Influencer Republic: Monetizing Political Speech on Social Media' (2022) 23(2) German Law Journal 204.

regardless of its political or non-political nature. The obligation also extends to any advertising handled by users of services on VLOPs, such as their influencers, if correctly identified as a commercial communication (Article 39(2)(f)). It does include a broad range of commercial practices, such as paid-for ranking prioritisation, targeted ads, and advertorials. Unlike other transparency obligations, repositories must be built and maintained by the providers as ‘a searchable and reliable tool that allows multicriteria queries’ through application programming interfaces (APIs) (Article 39(1)). The VLOPs are unlikely to be entirely free to design these interfaces. Article 39(3) already foresees that the European Commission can issue guidelines on the advertising repositories ‘structure, organisation and functionalities’.

The DSA does not explicitly require that the VLOPs operate the advertising repositories. In fact, Article 46(2)(b) hints at the possibility that third parties can operate such systems using the feeds of information from one or more providers. Providers must, however, disclose real-time data and then store it for one year after it was last presented to the audience. This period is arguably very short for researchers’ purposes and better serves the needs of journalists or companies. However, researchers can rely on Article 40(12) to replicate these databases and store them in their tools for longer periods. There is even an argument that such duplicate databases can also be open to non-researchers given that they were previously disclosed to the public—thus, there are few legitimate concerns to level against their use even by a wider set of actors. In any case, databases must already be stripped of potential personal data by the providers operating them (Article 39(1)).

The elements disclosed in advertising are extensive but do not include spending data.⁴⁷ This was a conscious choice because many voluntary projects run by providers already included such information before the DSA. Each advertising included in the repository must have the following:

- content of the advertisement;
- on whose behalf it is presented;
- who paid for the advertisement;
- period for which it was presented;
- how was the advertisement targeted, including the main parameters used; and
- detailed reach data for each advertisement.

The elements clearly show that the legislature wanted to achieve disclosure of the ultimate beneficiary of the advertising. This is why agencies placing orders on advertising need to disclose the funders. However, the obligation is unlikely always to show who actually paid for the advertisement. While the providers are obliged to ‘make reasonable efforts to ensure’ accuracy and completeness, the absence of deeper

⁴⁷ Paddy Leerssen, ‘Platform Ad Archives in Article 30 DSA’ (*DSA Observatory*, 25 May 2021) <<https://dsa-observatory.eu/2021/05/25/platform-ad-archives-in-article-30-dsa/>> accessed 5 September 2023.

know-your-customer obligations makes it unlikely for them to disclose the ultimate beneficiaries. The advertisers will thus probably continue to hide behind the corporate structures or partners.

That being said, the rules are still an improvement on the status quo where we know so little about what commercial messages are distributed to whom. This makes any oversight nearly impossible. In the offline world, everyone, including the regulators, could usually view the same ads. The targeting existed, but it was not so opaque. In the digital ecosystem, the opposite is the rule—no one knows what others view and why. Thus, while there is no perfect solution, the hope is that together with other rules concerning the advertising networks, the situation can generally improve step by step.⁴⁸

This insight was not lost on the legislature which envisaged specific Codes of Conduct in the area of online advertising (Article 46). These Codes of Conduct can go beyond existing DSA obligations and address other parts of the advertising value chain, including other providers of digital services.

For researchers, the two crucial data points will be targeting and exposure data. Article 39 mandates that the duration and main parameters for each advertisement are reported. This includes information about the main parameters concerning groups included and excluded from such campaigns. This information is complemented by aggregate absolute numbers of unique viewers who were reached by the advertisement, broken down by each Member State for which the targeting was arranged (Article 39(2)(g)). The reach data, coupled with targeting information, can be useful for journalists and researchers but is also likely to be used by competitors and other firms. Undeniably, coupled with the exact details about clients and their advertisements, the data presents an important insight into the advertising campaigns of competitors. It will be interesting to observe how this transparency will affect those markets and advertising behaviour. One can imagine that transparency can also limit the type of practices that advertising agencies, including their clients, wish to engage in due to concerns about negative publicity. Moreover, transparency is also likely to facilitate enforcement of the ban on profiling-based advertising that relies on sensitive data on online platforms (Article 26(3)).

Since advertisements can be equally subject to a content moderation decision, in order to avoid publicly displaying illegal advertising, Article 39(3) limits the information which must be preserved concerning removed advertisements. Advertisements removed based on illegality or terms of use violations must still be included in the repository; however, their content and identity of the advertiser and funder may *not* be included and are instead supplemented by the statements of reasons or information about the legal basis of orders that caused their removal. Despite this, vetted researchers, according to Article 40, could qualify to obtain privileged access even to the information stripped from advertisements.

⁴⁸ *ibid.*

14.3.3 Advertising on VLOSEs (Article 26)

On its face, Article 26 applies only to all advertising orchestrated by online platforms. But advertising archives also apply to VLOSEs (Article 39(1)). Since advertising archives require the collection and disclosure of the elements that overlap with disclosure obligations under Articles 26(1)–(2), its application to VLOSEs is highly likely. There are at least three ways how such an application can come to exist: (a) qualification of the advertising systems as online platforms, (b) general risk management and Codes of Conduct, and (c) analogical application of Article 26.

First, if the advertising system qualifies for one of the liability exemptions, such as hosting, Article 26 could apply if such a system can also qualify as an online platform. The CJEU has previously held that keyword advertising qualifies as hosting.⁴⁹ If such a system could be said to ‘store and disseminate information to the public’ as part of the service’s main activity, it qualifies as an online platform (Article 3(i)). However, keywords in search engines are only visible to the system unless they perfectly match what the user is searching for. Since the keywords are the stored information, if it fails to be distributed to the users who use a search engine, the system is not an online platform.

However, even in such cases, advertising systems used by search engines can be regulated. Article 26 is not preconditioned on the idea that the system itself must operate as a relevant technical activity. On the contrary, the DSA does not define how or who operates it. Theoretically, any system, manual or automated, personalised or not, video-based or text-based, internally operated or outsourced, can qualify as long as the system *carries the advertising for* the regulated service. Outsourcing in itself is not an excuse to comply with Article 26 or 39. The existence of advertising in conjunction with user-generated content triggers the regulation, not the advertising system’s qualification as a regulated service. Therefore, even outsourced advertising systems operated by online platforms on top of user-generated content must conform to the same rules as advertising systems operated in-house.

For search engines, this is crucial because if even parts of their services qualify as online platforms, Article 26 will apply. As discussed in Chapter 7.2, there is an argument that storing hyperlinks, and potentially snippets in the search results is a service that takes place at the implicit request of the website owners. The argument for this is particularly strong when the website owners manage their relationship with search engines through dedicated tools. In these cases, it is clear that information is provided to search engines and that they wish for information to be disseminated via the search results. If the CJEU accepts the argument, inevitably, a search engine which scrapes the data following a lack of opt-out from the websites will be recognised as an online platform for some of its content. This has consequences under Article 26.

⁴⁹ Joined Cases C-236/08 to C-238/08 *Google France SARL and Google Inc v Louis Vuitton Malletier SA* ECLI:EU:C:2010:159.

Finally, even if Article 26 does not apply to VLOSEs, its obligations can be analogously extended to them by virtue of general risk management or Codes of Conduct.

14.3.4 Ban on ads using profiling of sensitive data (Article 26(3))

One of the most atypical obligations, given the DSA's other rules, is the ban on advertising based on sensitive personal data. The ban was introduced in the legislative process at the request of the European Parliament, prompted by concerns about surveillance and misuse of sensitive categories of personal data, such as race, religious or political opinions, and weaponising such insights against them. The GDPR defines these special categories of data, sometimes referred to also as 'sensitive data,' as follows:

[P]ersonal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.⁵⁰

The GDPR's list is meant to be exhaustive.⁵¹ However, the CJEU recently accepted that even the publication of the name of a partner could reveal sexual orientation and thus count as sensitive.⁵² This means that many different types of data that do not have an expressly sensitive character can become sensitive on the basis of the reasoning that the data controller might employ. Thus, even without a declaration regarding one's political or religious views, information can nonetheless be sensitive. For instance, information about joining the picket line is likely to suggest membership in the trade union, although it is not an entirely reliable proxy. The crucial question is how cogent the reasoning must be. After all, not all persons in heterosexual partnerships are straight, either. In the CJEU's view, even personal data 'liable indirectly to reveal sensitive information concerning a natural person' should benefit from the strengthened protection.⁵³

Similar to the GDPR, the DSA's rules are that while the processing of sensitive data is generally prohibited in principle, such processing can still be allowed under strict conditions.⁵⁴ However, Article 26(3) DSA adds a novum: for the purposes of the use of profiling in advertising on online platforms, such processing can never be justified. The interpretation of this provision will surely give rise to many enforcement actions.

⁵⁰ GDPR, art 9(1).

⁵¹ Ludmila Georgieva and Christopher Kuner, 'Article 9 Processing of Special Categories of Personal Data' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (OUP 2020) 375.

⁵² Case C-184/20 *OT v Vyriausioji tarnybinės etikos komisija* ECLI:EU:C:2022:601.

⁵³ *ibid* para 127.

⁵⁴ GDPR, art 9.

While Article 26(3) requires such processing to also qualify as ‘profiling’, the very broad definition of the term in data protection legislation⁵⁵ makes it hard to imagine when advertising systems’ use of such parameters would not fall within the practice of analysing or predicting someone’s future behaviour or personal preferences. These activities are at the core of what targeted advertising tries to achieve: increased customer retention and extraction of attention by predicting someone’s interest in the information.⁵⁶

First, it will take time to settle the question of what information leads to the processing of sensitive personal data. It is one thing to redesign advertising systems to explicitly prohibit parameters of race, ethnic origin, religion, political views, union membership, or sexual orientation. It is quite another to interpret what information constitutes philosophical beliefs and data concerning one’s health or sex life and yet another to settle what information can reveal any of the sensitive characteristics. Second, the situation is further complicated because advertising is construed broadly. Even recommender engines could be classified as advertising systems if they used some parameters as *quid pro quo*.

14.3.5 Ban on ads using profiling of children (Article 28(2))

Article 28(2) prohibits platform from offering advertisements based on profiling using personal data ‘when they are aware with reasonable certainty’ that they are minors. Unlike the ban on profiling-based advertising based on sensitive personal data in Article 26(3), Article 28(2) is much broader.

The obvious difficulties with applying the provision are identifying when a minor uses a service and who exactly qualifies as a minor. The DSA, unfortunately, follows the GDPR⁵⁷ and fails to come up with a common age threshold for minors. In the context of GDPR, this has led to fragmentation in the context of consent.⁵⁸ However, according to the EU’s Fundamental Rights Agency, the age of majority according to private law is 18 years in all the current Member States.⁵⁹ The consensus in data protection law is around the same age with the argument that all the Member States are signatories to the UN Convention on the Rights of the Child, which defines a child as ‘every human

⁵⁵ Art 4(4) GDPR: “‘profiling’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.”

⁵⁶ For a discussion on the trade-offs that companies face in this regard, see Tom Cunningham, ‘Ranking by Engagement’ (8 May 2023) <<https://tecunningham.github.io/posts/2023-04-28-ranking-by-engagement.html>> accessed 5 September 2023.

⁵⁷ GDPR, art 8.

⁵⁸ The European Commission also noted this in its first evaluation of the GDPR: see Commission, ‘Data Protection as a Pillar of Citizens’ Empowerment and the EU’s Approach to the Digital Transition—Two Years of Application of the General Data Protection Regulation’ (Communication) COM (2020) 264 final 8.

⁵⁹ European Union Agency for Fundamental Rights, ‘Age of Majority’ (12 November 2017) <<http://fra.europa.eu/en/publication/2017/mapping-minimum-age-requirements/age-majority>> accessed 5 September 2023. Note that only in Scotland, which does not belong to the EU anymore, children are considered to have full legal capacity from 16 years.

being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier’.⁶⁰ This would suggest that DSA can arguably adopt one single standard through uniform interpretation by the CJEU despite the missing definition.

No less difficult is the question of when the minor-related protection is activated. Recital 71 confirms that there are two standards under Article 28: ‘accessibility’, which applies to Article 28(1)—the general obligation, and narrower ‘reasonable certainty’, which applies to a specific prohibition in Article 28(2)—the ban on profiling-based advertising for children. The accessibility standard is explained by Recital 71 as follows:

An online platform can be considered to be accessible to minors *when its terms and conditions permit minors to use the service, when its service is directed at or predominantly used by minors, or where the provider is otherwise aware* that some of the recipients of its service are minors, for example, because it already processes personal data of the recipients of its service revealing their age for other purposes.⁶¹

14.4 Design of User Experience

The previous two sections dealt with the design requirements that concerned specific parts of digital services—advertising and recommendation systems. In this section, I explain the additional due diligence obligations that concern the design of user experience on digital services.

14.4.1 Dark patterns (Article 25)

The DSA imposes a general obligation on online platforms to design their ‘online interfaces’ fairly (Article 25). An interface is defined as ‘any software, including a website or a part thereof, and applications, including mobile applications’ (Article 3(m)). Thus, any surface of a digital service that interacts with users is effectively covered. Those that users never access have no one to deceive or manipulate. Hence, one can easily speak of an obligation to design a fair user experience.

A user experience specialist, Harry Brignull, has been exposing abusive design practices for years.⁶² His term ‘dark patterns’ became a standard way of how to refer

⁶⁰ UNGA Res 44/25 ‘Convention on the Rights of the Child’ (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3, art 1. The art 29 Data Protection Working Party notes that: ‘The term “child” is not defined under the GDPR, however WP29 recognises that, in accordance with the UN Convention on the Rights of the Child, which all EU Member States have ratified, a child is a person under the age of 18 years’, see art 29 Data Protection Working Party, ‘Guidelines on transparency under Regulation 2016/679’ (wp260rev.01, adopted on 29 November 2017, as last revised and adopted on 11 April 2018) 10 <<https://ec.europa.eu/newsroom/article29/items/622227/en>> accessed 6 September 2023.

⁶¹ DSA, Rec 71 (emphasis mine).

⁶² Harry Brignull, ‘What are Deceptive Patterns?’ (*Deceptive Patterns*) <<https://www.deceptive.design/>> accessed 5 September 2023.

to unfair practices embedded in the design of digital services, such as when platforms hide existing choices from their users.⁶³ A dark pattern is thus an enigmatic name for a centuries-old practice—trickery.

The Commission's proposal did not envisage any rules on dark patterns. However, both the European Parliament and the Council agreed to include rules prohibiting deceptive interfaces.⁶⁴ The final text navigates between their two positions. According to Article 25, providers of online platforms:

shall not design, organise or operate their online interfaces in a way that deceives or manipulates the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions.

The provision thus targets *deceptive* and *manipulating* practices. While the provision would seemingly primarily apply to transaction websites, like marketplaces, its relevance is much broader. Even advertising-supported platforms that offer free access to content can engage in such practices to increase the value of their advertising systems, for instance, by undermining choices made by users to protect themselves against profiling.

Article 25(3) includes an illustrative list of three such practices. The first one consists of giving more prominence to certain choices when asking the recipient of the service to make a decision. This typically includes choice buttons that try to mislead the user into making decisions that are not in their interests but are guided by their fast thinking (eg clicking an intuitive colour or icon). The second one, known as 'nagging', consists of repeatedly requesting that the recipient of the service make a choice where that choice has already been made, especially by presenting pop-ups that interfere with the user experience. An example of this practice is repeated requests for users to buy something or share data. Finally, the provision includes a practice of making the procedure for terminating a service more difficult than subscribing to it.

The literature recognises additional types of dark patterns that trick, misinform or otherwise put pressure on the decision-making of consumers. They take consumers' time or money. Mark Leiser and Mireille Caruana describe other potential examples of deceptive or manipulative design, such as:

- confirm-shaming;
- sneaking items into the shopping basket;

⁶³ Bringull defines 'dark patterns', also known as deceptive design patterns, as 'tricks used in websites and apps that make you do things that you didn't mean to, like buying or signing up for something'. He also states that '[w]hen you use websites and apps, you don't read every word on every page—you skim read and make assumptions. If a company wants to trick you into doing something, they take advantage of this by making a page look like it is saying one thing when in fact saying another': *ibid.*

⁶⁴ In the European Parliament's proposal, the scope was wide and covered all online intermediary services, consciously going beyond the interfaces regulated in the DSA and overlapping with prohibitions already existing in the GDPR realm or under consumer protection rules.

- adding hidden costs in the process;
- toying with emotions; and
- creating urgency.⁶⁵

While Article 25 is an important signal to digital service providers, its applicability will be far from straightforward. Before this provision was adopted, most consumer-facing practices were already illegal in the Union. ‘Dark patterns’ have been tackled through the Unfair Commercial Practices Directive (UCPD) in the context of business-to-consumer commercial activities.⁶⁶ Recently, the Commission even published guidelines to clarify the legality of such practices.⁶⁷ Since many interfaces for consent involve processing personal data, data protection law is also an area where the GDPR and other EU laws regulate dark patterns. The European Data Protection Board (EDPB) has released guidelines on such practices and the application of the GDPR,⁶⁸ with a particular focus on online platforms. The EDPB guidelines cover the entire ‘life cycle’ from registering on a platform, including its privacy notices, managing consent, and data protection settings, to the closing of the accounts.⁶⁹

Article 25(1) DSA mostly recycles the UCPD’s benchmark of unacceptable practice: that which ‘materially distorts or impairs the ability ... to make free and informed decisions’. The UCPD is naturally much more comprehensive.⁷⁰ It emphasises the freedom of decisions only with respect to aggressive practices which are likely to significantly impair the average consumer’s ‘freedom of choice or conduct’ in the context of a business-to-consumer commercial relationship.⁷¹ Similarly, the GDPR already includes some obligations, but the focus is more so on the individual’s personal data, including the exercise of ‘freely given, specific, informed and unambiguous’ consent (Article 4(11) GDPR).⁷²

To avoid confusion amidst overlapping laws and to prevent layering of enforcement structures,⁷³ the final last-minute compromise resulted in a ban applicable to online

⁶⁵ See Mark R Leiser and Mireille Caruana, ‘Dark Patterns: Light to be Found in Europe’s Consumer Protection Regime’ (2021) 10 Journal of European Consumer and Market Law 237.

⁶⁶ European Parliament and Council Directive 2005/29/EC concerning unfair business-to-consumer commercial practices in the internal market [2005] OJ L149/22 as amended by Directive (EU) 2019/2161 (UCPD).

⁶⁷ The UCPD includes since 2005 two open-worded clauses covering deceptive and abusive practices that equally apply to the user experience on digital services; Commission, ‘Guidance on the Interpretation and Application of Directive 2005/29/EC of the European Parliament and of the Council Concerning Unfair Business-to-Consumer Commercial Practices in the Internal Market’ (Notice) [2021] OJ C526/1.

⁶⁸ European Data Protection Board, ‘EDPB Adopts Guidelines on Art. 60 GDPR, Guidelines on Dark Patterns in Social Media Platform Interfaces, Toolbox on Essential Data Protection Safeguards for Enforcement Cooperation between EEA and Third Country SAs’ (15 March 2022) <https://edpb.europa.eu/news/news/2022/edpb-adopts-guidelines-art-60-gdpr-guidelines-dark-patterns-social-media-platform_en> accessed 11 September 2023.

⁶⁹ The Italian Data Protection Authority recently fined the use of dark patterns in the context of data collection, *Il Garante Per La Protezione Dei Dati Personali*, Case of *Ediscom SpA*, 23 February 2023 [Document 9870014].

⁷⁰ Arts 2(e) and 5 of the UCPD (general clause); see also arts 2(j) and 8 of the UCPD.

⁷¹ UCPD, art 8.

⁷² Forbrukerrådet, ‘Deceived by Design: How Tech Companies Use Dark Patterns to Discourage Us from Exercising our Rights to Privacy’ (Forbrukerrådet (Norway’s Consumer Council) 2018) <<https://fil.forbrukerra.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf>> accessed 5 September 2023.

⁷³ For instance, should the Digital Services Coordinator (DSCs) or the Data Protection Authorities (DPA) in the platform’s country of origin, let us say in Ireland, or the consumer authorities of the consumer’s country of residence, let us say in France, be responsible for the enforcement?

platforms ‘to the extent that those practices are not already covered under [UCPD] or [GDPR].’⁷⁴ While understandable, the compromise robbed Article 25 of much of its power and introduced only more complexity. The first step in applying Article 25 DSA is to determine whether other laws, such as UCPD and GDPR, apply to the situation at hand. Only once the answer for both is negative, Article 25, as a rule, would start offering the added value, including the competence of the Commission or Digital Service Coordinators. The reason for this drafting was a concern about the duplication of enforcement frameworks for the same problems.

So, where exactly will we see the added value of Article 25? In my view, apart from the DSA’s enforcement framework, the substantive added value mostly lies in regulating a few areas outside the scope of harmonised consumer or data protection laws. Since both areas of law only protect natural persons,⁷⁵ and consumer law only protects those who act outside their trade, business, craft, or profession,⁷⁶ Article 25 offers applicability in some business-to-business scenarios,⁷⁷ and to legal persons, or where the ‘dark pattern’ is used outside any commercial relationship. As a result, it does regulate some areas. However, it has little to do with the particular area in which policy circles traditionally associate dark patterns—that of business-to-consumer practices. Those remain carved out by Article 25(2).

Table 14.1 summarises the applicability of Article 25.

The table shows that Article 25 DSA has a significant role to play in the context of platform-to-business and platform-to-legal non-profits. Even though the GDPR still applies with priority, its scope is narrow—applying only to interfaces involving the processing of personal data (eg consent buttons). Where no personal data is processed through interfaces, the DSA regulates deceptive and manipulative practices. In the platform-to-business context, Article 25 DSA is *lex specialis* to the Misleading and Comparative Advertising Directive, which generally regulates misleading and comparative advertising.⁷⁸ On the level of applicable standards, Article 25(1) DSA is likely to gain a life of its own in situations of aggressive (manipulative) practices that do not affect consumers. This is because the EU law did not harmonise aggressive business-to-business practices, although some national unfair competition laws traditionally cover this area. Thus, prior to the DSA, unless there were sector-specific rules such as the P2BR, it was mostly national law that regulated instances where a trader imposed an undue burden on their business partners.

However, for misleading practices, the situation is even more complicated. Given that business-to-business practices that affect consumers are indirectly equally harmonised by UCPD,⁷⁹ the Article 25(1) standard is unlikely to gain any independent

⁷⁴ DSA, Rec 67.

⁷⁵ UCPD, art 2(a); GDPR, art 1.

⁷⁶ UCPD, art 2(a).

⁷⁷ Data protection law can still apply in these cases.

⁷⁸ European Parliament and Council Directive 2006/114/EC concerning misleading and comparative advertising [2006] OJ L376/21 (Misleading and Comparative Advertising Directive), arts 1–2.

⁷⁹ Recital 6 UCPD: ‘It neither covers nor affects the national laws on unfair commercial practices which harm only competitors’ economic interests or which relate to a transaction between traders’. The existing CJEU case law

Table 14.1 Applicability of Article 25 DSA

When does Article 25 DSA apply?		Recipient of the service		
		Natural or legal persons acting as businesses	Legal persons acting as non-profits	Natural persons acting as consumers
Platform	Platform (as a business) to: <i>Example: a marketplace with deceptive advertising design or manipulative auction design</i>	(1) GDPR (<i>narrow</i>); (2) substantial role for Article 25 DSA: (a) deceptive or, (b) manipulative design of services.		(1) UCPD (<i>broad</i>); (2) GDPR (<i>narrow</i>); (3) little role for Article 25 DSA (<i>arguably for the design of the DSA due diligence obligations</i>).
	Platform (as a non-profit) to <i>Example: an NGO operating a user-generated content website with a deceptive or manipulative donation interface</i>	(1) GDPR (<i>narrow</i>); (2) substantial role for Article 25 DSA <i>if</i> the platform at least qualifies as an economic activity: ^a (a) deceptive, or (b) manipulative design of services.		

^a Ch 6.2.6 on economic activity.

meaning of its own when the platform deceives consumers. For practices affecting consumers, if Article 25(1) applies at all, the CJEU is likely to make parallels between the standards of Article 25(1) and those governing UCPD, which are much more elaborate and horizontal. For practices affecting only traders, the meaning of standard applicable under Article 25(1) can differ from the consumer law. Arguably, Article 25's main importance is creating an EU-based cause of action for *businesses* against platforms. However, the national law must still specify the criteria under which businesses can seek injunctions or damages (see Chapter 19).

As hinted earlier, in the *platform-to-consumer* context, where most dark patterns occur, Article 25 takes a backseat in the regulatory toolkit. It only applies when the UCPD and GDPR do not. However, in my view, whenever the DSA prescribes some specific design choices, it should apply as *lex specialis* to these two horizontal frameworks. This is because the DSA has precedence over these areas, and the added value of Article 25 manifests in giving those DSA requirements a course of action against platforms. Thus, the provision arguably can serve a purpose even in the platform-to-consumer context whenever *the DSA imposes specific design through its due diligence obligations*. This reading would not only give Article 25 some meaning in the context

is well summarised by the Commission (n 66) 7 (A national provision does not fall within the scope of the UCPD 'if it aims solely, as argued by the referring court, at regulating relations between competitors and does not aim at protecting consumers').

of platform-to-consumer relations, but it also strengthens the DSA. It would not conflict with the rule of deference to these two frameworks (Article 25(2)), as whenever the DSA has special rules, they already take precedence over *lex generalis* rules of the UCPD or GDPR.

In practice, my suggested reading would mean the following: It would cover practices by *mere conduits* that make available information about contact points but hide it deep into the website, so that it cannot be found, or provide broken links to contact interfaces (Article 12); for *hosting services*, it would prohibit dark patterns created to deceive or manipulate users' choice as regards the availability of a notification mechanism, by hiding it behind many clicks through complicated interfaces (Article 16); for *online platforms*, it would cover the hiding of the complaint mechanism and the electronic submission of complaints (Article 20), information on why users are seeing an advertisement, or identifying advertisements with such vague or indiscernible markings that they remain undistinguishable from non-advertisements (Article 26); for *VLOPs*, it could cover practices that offer choices for recommender systems, but make visually prominent the option based on profiling and obscuring the others (Article 38), or presenting certain options with a particularly dissuasive emotional message ('confirm-shaming').

This interpretation regarding the application of Article 25 DSA has certain consequences. It would mean that Article 25 provides all recipients of services—be it consumers or businesses—with a Union-wide cause of action against platforms whenever they follow the DSA's design requirements in letter but not in spirit. It would turn all fair design requirements discussed in this chapter into actionable obligations. The effectiveness of the DSA would be significantly reduced if Article 25 was instead understood as only relegating the enforcement of misleading and manipulative DSA-related practices to tools such as EU consumer or data protection law or national tort law.

The final layer of complexity is to ascertain whether the full harmonisation approach under the DSA will pre-empt national laws that go beyond the UCPD or GDPR, where this is accepted by these instruments. In my view, the DSA, as stated in Recital 10, fills such gaps and pre-empts any such national rules within its area of application.⁸⁰ That being said, even Article 25 DSA has its limits too. An online platform that misleads or manipulates through its interface still must qualify as an information society service, which can be an issue for its applicability to 'platform' services that have no economic dimension.⁸¹

To conclude, despite its limited applicability, Article 25 might offer some added value if enforced. In particular, Article 25 could be seen as an enforcement tool for various fair design practice standards embedded in the DSA, thus placing the weight of

⁸⁰ Rec 10 DSA: 'However, to the extent that those Union legal acts pursue the same objectives as those laid down in this Regulation, the rules of this Regulation should apply in respect of issues that are not addressed or not fully addressed by those other legal acts as well as issues on which those other legal acts leave Member States the possibility of adopting certain measures at national level.'

⁸¹ Ch 4.

enforcement tools behind words such as ‘user-friendly’, ‘easy to use’, ‘clear’, ‘intelligible’, ‘plain’, ‘diligent’, ‘objective’, ‘reasonable’, ‘effective’ and ‘proportionate’.⁸²

14.4.2 Child protection by design (Article 28)

The DSA, informed by a myriad of tragedies about children dying because of viral challenges on social media, gives special regulatory attention to minors as a subcategory of users requiring particular protection, justified by their special vulnerability. Article 28(1) DSA puts forward specific obligations for all online platforms ‘accessible to minors’ that are not micro or small to:

put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors, on their service.

This obligation was included in the final text at the latest stage of the negotiations, as a ‘spin-off’ of the prohibition of dark patterns proposed by the European Parliament.⁸³ Article 28 can be used by affected parties, including independent specialist non-profit organisations (Article 86), as an umbrella provision to seek redress against failings of online platforms in the area of child-related privacy, security, and safety. Article 28 also offers a door for litigation or enforcement of various DSA measures to address children’s welfare by providing a cause of action, subject to national remedies (see Chapter 19).

The provision does not specify what interventions are expected to support minors’ privacy, safety, and security. In this sense, its principle-based stance is similar to the GDPR.⁸⁴ However, these iterative product design interventions must be based on some awareness and, thus, the internal assessment of the platform’s use. While the DSA does not prescribe audits, by requiring continuous adjustments of design for the benefit of minors, even medium-sized platforms must undertake some high-level due diligence assessment of children’s welfare on their services. If the assessment reveals risks to children’s privacy, safety, or security, they must act to adjust the design of their services. The key limitation would appear to be that platforms, unlike VLOPs, do not have to periodically gather in-depth evidence about the use of their service.

Some of the envisaged interventions are already part of the EU legislation in specific areas, such as the regulation of the Audiovisual Media Services Directive (AVMSD). While the content for children can be subject to specific prohibitions, such as bans on product placement, another important type of intervention concerns the creation

⁸² An example for enforceability of user-friendliness does exist in the national law: Germany’s Network Enforcement Act, *Netzwerkdurchsetzungsgesetz* (NetzDG) v 1 September 2017 (BGBl. I S 3352).

⁸³ *Interview with Irene Roche Laguna*, Deputy Head of Unit for Coordination and Regulatory Compliance, European Commission (2021–23).

⁸⁴ European Data Protection Board, ‘Binding Decision 2/2022 on the Dispute Arisen on the Draft Decision of the Irish Supervisory Authority Regarding Meta Platforms Ireland Limited (Instagram) under Article 65(1)(a) GDPR’ (28 July 2022) <https://edpb.europa.eu/system/files/2022-09/edpb_bindingdecision_20222_ie_sa_instagramchildusers_en.pdf> accessed 6 September 2022.

of tools that empower children and parents. Thus, Article 28b AVMSD, for instance, prescribes video-sharing services to provide ‘parental control systems that are under the control of the end-user with respect to content which may impair the physical, mental or moral development of minors’. Other possible interventions foreseen by the AVMSD are the user-based rating of systems, age-verification schemes, and awareness campaigns.⁸⁵

The DSA’s obligation to care for children’s welfare thus should primarily lead to the designing the services in ways that consider the best interest of the child. This should include the design that empowers children according to their state of development and, where appropriate, assist their parents in their hard task of raising young people to adulthood. While platforms are obviously expected to remove illegal content, they cannot be expected to *replace* parents and other guardians in children’s lives. Many interventions in form of better defaults, such as those restricting recommendation of children to strangers, and vice-versa, can preserve children’s choice while fostering their safety and increasing agency. Article 18(1) of the UN Convention on the Rights of the Child recognises that: ‘[p]arents or, as the case may be, legal guardians, have the primary responsibility for the upbringing and development of the child. The best interests of the child will be their basic concern.’⁸⁶ The same article places states under the obligation to ‘render appropriate assistance to parents and legal guardians in the performance of their child-rearing responsibilities’.

The design-focused approach also makes it easier to adjust interventions based on children’s age, as adolescents (ages 12–18 years) should clearly enjoy more agency than school-aged children (ages 6–12 years), or preschoolers (ages 2–6 years). Different age groups might also be susceptible to very different types of risks. Since providers, without surveilling children as users, cannot know about the vulnerabilities of each child, the role of parents in preventing harm remains crucial. Article 28 DSA leans into the demands of parents and guardians to obtain better tools to navigate parental discussions about the use of digital technologies. At the same time, it allows parents and children to adjust the design to the maturity, vulnerabilities, and capabilities of each individual child.

According to Article 5 of the UN Convention, states must ‘respect the responsibilities, rights and duties of parents ... to provide, in a manner consistent with the evolving capacities of the child, appropriate direction and guidance in the exercise by the child of the rights recognised in the present Convention.’⁸⁷ Thus, each child should be treated by the state and parents according to their ‘evolving capacities’. This equally means that while the providers are obliged to care for children’s welfare, they should empower parents to adjust various interventions according to the needs of each child. Unilateral imposition of one-size-fits-all approaches could actually violate numerous

⁸⁵ I discuss the relationship between AVMSD and DSA in ch 18.

⁸⁶ UNGA Res 44/25 ‘Convention on the Rights of the Child’ (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3, art 18(1).

⁸⁷ *ibid* art 5.

rights of children by treating them as less mature and denying them numerous rights guaranteed by the Convention.⁸⁸

The joint reading of Articles 25 and 28 can give minors powerful arguments against any aggressive practices that exploit the vulnerabilities of average children in different age groups. If providers use their design to maximise children's engagement, regardless of broader health risks for a particular age group, parents might be able to invoke the provision and demand a redesign of specific features. In this sense, the provision potentially enables much more private enforcement than general risk management, mostly subject to administrative enforcement (see Chapter 19).

Article 28 has more modest expectations than Article 35 because they are potentially directly enforceable. But even with those more modest expectations, the controversies around services like Omegle, or addictive design features of the major social media platforms could thus soon end up before the European courts on the back of Article 28.

The European Commission is given the task to issue guidance in the area and, in particular, identify specific practices that should be avoided. The envisaged targeted measures to protect minors might also be subject to standardisation (Article 44(1)(j)).

14.5 Business-to-Consumer Marketplaces

Despite the horizontal and undifferentiated applicability of most of the DSA's obligations, one specific set of digital services attracted service-specific rules in the legislative process. Business-to-consumer online marketplaces become subject to specific obligations even when they have fewer than 45 million active users if they are operated by companies that are not small or micro (Article 29(1)). If small or micro companies operate online marketplace services with more than 45 million active users, they are equally subject to these specific rules (Article 29(2)), and additional rules concerning VLOPs. Service-specific rules only apply to the online marketplaces that 'allow consumers to conclude distances contracts with traders'.⁸⁹

Business-to-consumer marketplaces must collect information about traders who sell through the platform (Article 30). They are also tasked to design their services in ways that facilitate verification. The marketplace must undertake its best efforts to try to validate the information provided generally, such as by consulting national public registries or verifying the documents provided by the trader. This process should take place upon registration with the online marketplace. For existing users, the DSA requires identity checks to take place within 12 months from the DSA's entry into force (Article 30(2)); otherwise, their accounts must be suspended for the duration of non-compliance with such requests. Upon suspicion that the information provided is

⁸⁸ See *ibid.*, arts 12(1), 13(1), 14(2), 16(1) and 31(1).

⁸⁹ Art 3(l) DSA states that 'distance contract' means 'distance contract' as defined in art 2(7), Directive 2011/83/EU; European Parliament and Council Directive 2011/83/EU on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC and repealing Council Directive 85/577/EEC and Directive 97/7/EC [2011] OJ L304/64, art 2(7).

incorrect or incomplete, the marketplace must request the trader to remedy the situation (Article 30(3)); otherwise, the account must be again suspended (Article 30(3)). All these suspensions or service restrictions shall be subject to DSA's rules on due processes, such as the internal complaint mechanism and out-of-court dispute settlement (Article 30(4) DSA), and the safeguards offered by Article 4 P2BR, such as the 30-day advance notice for some terminations.

The goal of Article 30 is that traders are traceable, not only for the benefit of consumers but also competitors and owners of intellectual property rights (Recital 72). The concern thus is not only consumers' wellbeing, but also the ability of brand owners to trace who are the re-sellers of their genuine products. The information must be stored throughout the business relationship and for six months after it has concluded (Article 30(5)). After that, the data must be deleted. However, the data collected can be subject to disclosure orders.

Business-to-consumer marketplaces must also design their trader-consumer interfaces in a way which facilitates traders' compliance with all sorts of applicable EU rules, such as pre-contractual consumer information and product safety. In addition, the marketplaces are explicitly tasked to 'make reasonable efforts to randomly check in any official, freely accessible and machine-readable online database or online interface whether the products or services offered have been identified as illegal' (Article 31(3)). However, Recital 73 cautions that this obligation should not imply 'excessive or costly online fact-finding exercises or to carry out disproportionate verifications on the spot' or 'be understood as guaranteeing the reliability of the information towards consumer or other interested parties'. While the DSA does not articulate this, any applicable restrictions applied to such traders are also subject to its due process requirements, such as the internal complaint mechanism, out-of-court redress *and* Article 4 P2BR safeguards, such as the 30-day advance notice for some terminations.

Article 32 also imposes specific *consumer notification requirements* when the platform becomes aware of traders selling illegal products or services through its business-to-consumer marketplace. If they have their contact details, they must inform the affected consumers who purchased them about such illegality, the trader's identity, and any relevant means of redress. The obligation, however, extends only to the purchase made in the last six months prior to knowledge acquisition. Thus, the relevant marketplaces cannot use this obligation as an excuse for longer retention of consumer purchasing behaviour. If the contact details of all relevant affected consumers are not known, the marketplace must inform about the same information through its public interface.

14.6 Conclusion

Articles dealing with recommender systems, advertising, and marketplaces represent a business regulation of unfair practices. Fair practices under the DSA thus mostly deal with the *design* of services, such as aggressive and misleading user interfaces,

obfuscation of key product information in advertising and recommender systems, overpersonalisation of user experience, and neglect of the special vulnerabilities of minors. The most explicit bans are on profiling-based advertising practices based on the sensitive personal data of all users (Article 26(3)), and based on any personal data concerning children (Article 28(2)). Articles 25 and 28 are starting points for potential future fair practices rules that can be imposed specifically on online platforms. They merge principles of unfair competition law, consumer law, media regulation, and contract law. Unlike fair process rules and fair content rules that are very broad and encompassing, fair design practices rules are drafted much more narrowly. For VLOPs, these rules provide a baseline for general risk management.

General Risk Management

15.1 Introduction	316	15.3.5 Step 5: Oversight by the Commission and public	331
15.2 Relevant Risks	318	15.3.6 DSA compliance officers	331
15.2.1 Systemic risks	319	15.4 A Theory of the DSA's Limited Risk Management	333
15.2.2 Hybrid services	321	15.4.1 Limited vs full risk management systems	334
15.3 Risk Management Cycle	322	15.4.2 What are the consequences for the Commission?	339
15.3.1 Step 1: Self-assess the systemic risks	324	15.4.3 Freedom of companies to mitigate risks	342
15.3.2 Step 2: Risk mitigation measures	325	15.4.4 Appraising, and allocating risks	342
15.3.3 Step 3: External auditing	328		
15.3.4 Step 4: Provider's follow-up on external audits	330		

15.1 Introduction

The crown jewel in the DSA's regulatory toolbox is the obligation of very large online platforms (VLOPs) and very large online search engines (VLOSEs) to generally manage risks on their services. The mechanism goes against Zuckerberg's mantra: 'move fast and break things',¹ and pushes Big Tech towards an 'innovate but validate' culture. With general risk management, the EU legislature has signalled that it is no longer acceptable to optimise the design of services at the expense of everyone else to achieve the fastest possible growth and profit. During the legislative negotiations, the European Commission was given exclusive competence to supervise this crucial special obligation (Chapter 19).

Articles 34–35 are an attempt to regulate technology firms through a regulatory dialogue. General risk management is by far the most open-ended DSA provision. It foresees continuous back-and-forth between designated providers, auditors, researchers, and ultimately authorities about potential systemic risks. However, this envisaged regulatory dialogue is highly enigmatic at this point. General risk management places pressure on VLOPs and VLOSEs to invest additional resources into the study and mitigation of risks posed by their services. Because of the broad range of risks that are funnelled into the system, it is a 360-degree risk management tool that covers most corners

¹ Henry Blodget, 'Mark Zuckerberg On Innovation' *Business Insider* (New York, 1 October 2009) <<https://www.businessinsider.com/mark-zuckerberg-innovation-2009-10?r=US&IR=T>> accessed 6 September 2023.

of services. It asks providers of services to demonstrate that they acted responsibly when deploying and offering their services.

From companies' perspective, the key trade-off is between profitability and responsibility for social costs. VLOPs and VLOSEs are forced to internalise many more social costs. This is a familiar problem. A quickly innovating industry is tasked to think of the bigger picture, not just of its profits. We already see this with financial regulation, which similarly tries to keep the risk-taking of banks within acceptable levels, to avoid negative effects on individuals who entrust financial institutions with their money. Here, the DSA gives the European Commission a lever to push for change whenever the risks to others are tangible and concrete.

As explained in Chapter 13, platforms offer communication tools. Their design has a serious impact on personal liberty, relationships, and human autonomy. This is not surprising, for in the offline world, architecture undoubtedly affects people too.² Every design choice cultivates a different environment. However, architects of offline spaces mostly influence how people feel or meet, and not what they can say to each other. Their digital counterparts on the other hand, have much more control over the latter in the online sphere. It is therefore understandable that people are not as concerned about the overreach of safety regulations in the offline design (eg seatbelts, fire access, etc), as they are online. Offline, barriers must be purposefully and additionally erected to prevent people from communicating. Online, the distance is the barrier to communication which platforms purport to help overcome. In designing these communication tools, the Lessigian architects also hold the key to its manipulation.

Consider the problem of virality—the rapid dissemination of information. Virality can hold to account corrupt leaders, but also suppress voting in elections by flooding people with lies. Limiting the speed at which information travels over digital services inevitably means making trade-offs. Is the design of a recommender system enabling lower virality better or worse for society? If we focus on the problem of disinformation, slower information distribution might be favoured, especially during elections. If the focus is on legitimate civil protest, faster distribution might be favoured. It is hard to have it both ways.

Many digital services carrying user-generated content are powerful channels of information distribution because they harness the power of personal persuasion by other people. The results from a famous Facebook voting experiment, for instance, suggested that 'close friends exerted about four times more influence on the total number of validated voters mobilised than the message [posted by the provider] itself'.³ Behavioural scientists have been studying principles that influence people's behaviour for years. For instance, Cialdini (2001) posits that social proof, liking, authority, and reciprocity are

² Ben Channon, *Happy by Design* (RIBA Publishing 2019).

³ Robert M Bond and others, 'A 61-Million-Person Experiment in Social Influence and Political Mobilization' (2012) 489(7415) *Nature* 295, 298. Also James H Fowler, 'Turnout in a Small World' in Alan S Zuckerman (ed), *The social logic of politics: personal networks as contexts for political behavior* (Temple UP 2005).

among the six principles that help to persuade others.⁴ Many user-generated content services rely on social proof, liking, reciprocity, or commitment. Thus, interventions against how information travels sometimes need to address these specific and deeply communicative features of services.

Moreover, the information they carry can spread exponentially rather than linearly. This means that the growth in the distribution is initially slow, but within a few steps, it accelerates rapidly.⁵ Thus, the countermeasures must be fast and decisive, otherwise it could become hard to contain the social problem that might suddenly erupt. The on-line platforms trying to deal with the information spreading in the network are handling a contagious disease rather than a large incident with single source. As a result, a flexible risk-based approach, as opposed to detailed ready-made statutory rules, is more likely to help in addressing the distribution of content on digital platforms.

15.2 Relevant Risks

The DSA defines the relevant risks in two ways. First, the risk must take place on a designated service and be confined to the ‘design’, ‘functioning’, or ‘use’ of the service (Article 34(1)). The regulation does not exhaustively enumerate parts of the service that count as relevant risk surfaces, but it mentions some of them by example. Article 34(2) mentions user-generated content, recommendation systems, third-party advertising, and related data practices, as examples. Other risk surfaces, such as the design of interfaces (eg who can share how much content with whom, or what information they can view about others), external cooperation (eg how companies interact with trusted actors), or back-end internal operations (eg what is the training or work conditions of content moderators) are equally covered, as is evident from Article 35(1). Second, the risk must fit into one of the four risk categories: (a) illegal content, (b) fundamental rights, (c) public security and elections, and (d) health and well-being (see Table 15.1). The relevant types of risks and risk areas overlap and are not mutually exclusive. A risk of interference with elections can qualify as a risk from illegal content (a) and to electoral processes (c). A risk of under-enforcement of terrorist content qualifies as a risk from illegal content (a), and the risk over-enforcement as risk to freedom of expression (b). This 360-degree design means that the regulator cannot ignore either side of the societal equation.

Some authors argue that general risk management is worded so broadly that it can incorporate consideration of environmental costs of running companies, such as the carbon footprint of their data centres, and allow the regulators to question the

⁴ For discussion of the literature, Sofia Gkika and George Lekakos, ‘The Persuasive Role of Explanations in Recommender Systems’ (Second International Workshop on Behavior Change Support Systems, BCSS 2014) 61 <https://ceur-ws.org/Vol-1153/Paper_6.pdf> accessed 6 September 2023.

⁵ For an example of the spread of a conspiracy theory about Covid, Erin Gallagher, ‘Facebook Groups and YouTube Enabled Viral Spread of “Plandemic” Misinformation’ (*OneZero*, 21 May 2020) <<https://onezero.medium.com/facebook-groups-and-youtube-enabled-viral-spread-of-plandemic-misinformation-fla279335e8c>> accessed 6 September 2023.

Table 15.1 General risk management: overview

General risk management: relevant risks	Design-driven risks	Use-driven risks	Function-driven risks
	Interfaces, recommender systems, advertising, moderation tools, etc.	Terms and conditions, content moderation rules and processes	Data practices, back-end operations, staff training, external cooperation
Illegal content (Art 34(1)(a))	<i>Examples:</i> (a) terrorist content; (b) child sexual abuse; (c) illegal hate speech; (d) intellectual property infringements; (e) defamation; (f) sale of unsafe products; (g) cyberstalking or grooming; or (h) <i>any other</i> areas of illegal content or behaviour.		
Fundamental rights (Art 34(1)(b), Recital 81)	<i>Examples:</i> (a) human dignity; (b) freedom of expression and information, including media freedom and pluralism; (c) right to private life; (d) data protection; (e) right to non-discrimination; (f) rights of the child; (g) consumer protection; or (h) <i>any other</i> fundamental rights.		
Public security and elections (Art 34(1)(c), Recital 82)	<i>Exhaustive subcategories:</i> (a) civic discourse, including democratic processes; (b) electoral process; and (c) public security.		
Health and well-being (Art 34(1)(d), Recital 83)	<i>Exhaustive subcategories:</i> (a) gender-based violence; (b) public health; (c) rights of minors; (d) physical well-being; and (e) mental well-being.		

legitimacy of product design features, such as recommender systems, from the environmental standpoint.⁶ I am personally sceptical that such risks align with the DSA's goal 'to contribute to the proper functioning of the internal market for intermediary services by setting out harmonised rules for a safe, predictable and trusted *online* environment' (Article 1(1), emphasis mine). Thus, if the link to online environment is not present, despite the broadness, such risks are not relevant.

15.2.1 Systemic risks

Article 34 does not require self-assessment of just any type of risk. It only targets 'systemic risks'; in particular, 'any systemic risks in the Union stemming from the design or functioning ... or from the use made of their services' (Article 34(1)). The DSA offers little guidance on what 'systemic risks' are. The factors that it mentions are often contradictory.

Recitals 79 to 84 also try to explain the notion through examples, but the language hardly gives away any more concrete criteria. The broadness of the exercise is partly

⁶ Rachel Griffin, 'What Does Digital Policy Have to Do with Climate? A Great Deal' (*Centre for International Governance Innovation*) <<https://www.cigionline.org/articles/what-does-digital-policy-have-to-do-with-climate-a-great-deal/>> accessed 6 September 2023.

mitigated by the userbase threshold for becoming the regulated entity. The DSA speaks of the following criteria:

- Recital 79: ‘they could assess whether the potential negative impact can affect a large number of persons, its potential irreversibility, or how difficult it is to remedy and restore the situation prevailing prior to the potential impact’.
- Recital 80: ‘dissemination or activities may constitute a significant systemic risk where access to illegal content may spread rapidly and widely through accounts with a particularly wide reach or other means of amplification’.
- Recital 81: ‘the design of the algorithmic systems used by the very large online platform or by very large online search engine or the misuse of their service through the submission of abusive notices or other methods for silencing speech or hampering competition’.
- Recital 138: ‘systemic issues, such as issues with a wide impact on collective interests of recipients of the service’.

The DSA thus interchangeably invokes the *scale* of harm, its *irreversibility* and *speed*, and *collective dimension*. In practice, it may in either case be necessary to first undertake the self-assessment for all risks, as the potential magnitude of any risk might be unclear upfront. While all risks created by VLOPs or VLOSEs are potentially systemic due to their size, not all must be followed by providers’ counteraction (section 15.3.2). VLOPs and VLOSEs must take reasonable, effective, and proportionate steps against systemic risks given the probability and severity of their occurrence (Articles 34(1), 35(1)).

Originally, the European Commission’s proposal included two thresholds in its wording. It spoke of ‘any significant systemic risks’.⁷ The idea was that while the first threshold refers to the size of the impact, the second refers to its collective rather than individual nature. In this sense, one of the meanings of ‘systemic’ was to conceptually distinguish the approach from individual harms-based legislation that tend toward content regulation. The intention was to trigger interventions whenever the aggregate risk to individuals can be described as a structural or systemic problem. Despite the legislative process that followed, where the impact threshold disappeared, it is still valid to ascribe two basic meanings to the term ‘systemic’: ‘systemic’ in the sense of being central to society; and ‘systemic’ in the sense of emanating from systems.

In the final version of the text, the underlying logic of employing the qualifier ‘systemic’ seems to be that the wide reach of content on VLOPs or VLOSEs is such that any risk is susceptible to becoming systemic quickly, amplified by the size of its very large user base.⁸ Systemic in this sense refers to the ‘systemic role in facilitating the public

⁷ Commission, ‘Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and Amending Directive 2000/31/EC’ COM(2020) 825 final, art 26(1) (‘any significant systemic risks stemming from the functioning and use made of their services in the Union’).

⁸ Rec 79 DSA.

debate and economic transactions.⁹ Therefore, it is irrelevant that some platforms do not have recommender systems. They are still platforms with large user bases for the distribution of other people's information. Similar intuition is being used by the CJEU in cases dealing with automated profiling or decision-making, where the large scale of operations and opaque setting usually suggest a higher impact on the data protection interests of an individual.¹⁰

The difficulty with the DSA's reliance on such a broad notion of *systemic* risks lies in the lack of a concrete *circle of responsibility* that could limit the risks and reveal their systemic nature. For banks under financial regulation, the focus is on the stability of the financial system which can influence businesses and individuals. For technology companies operating platforms, what exactly counts as their circle of responsibility is unclear. The DSA with its 360-degree design seems to suggest that everything is Big Tech's responsibility. This is again where parallels with other areas, such as banking, offer little help.¹¹ Thus, arguably, the Recitals invoke the *scale* of harm, its *irreversibility* and *speed*, and *collective dimension* as potential qualifiers. The Commission might reduce uncertainty by developing risk profiles for different types and registries of risks which would help companies to assess them. The Commission's counterpart in the United Kingdom, Ofcom, is currently doing just that.¹²

Researchers from many disciplines need to help regulators define the systemic relevance of various risks to adults, minors, elections, media, public security, and many others. While the DSA offers a matrix of risks to consider, what truly matters to people, and their societies can only be revealed by rigorous study of their problems. This is why the DSA provides a strong link to the research community (Chapter 16), giving them privileged access to data (Article 40) and allowing the Commission to draw on the expertise and capabilities of relevant expert bodies and centres of excellence, and to invite experts with specific expertise.¹³

15.2.2 Hybrid services

Not all services that the DSA regulates are purely about user-generated content. The DSA also similarly regulates hybrid services which combine editorial and user-generated content. For instance, marketplaces that sell their own and third-party

⁹ Commission, 'Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and Amending Directive 2000/31/EC' COM(2020) 825 final 6.

¹⁰ Case C-817/19 *Ligue des droits humains v Conseil des ministres* ECLI:EU:C:2022:491; Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* ECLI:EU:C:2014:238.

¹¹ A Centre on Regulation in Europe (CERRE) report explores whether the notion of systemic risk from financial services can be used in the context of the DSA and comes to the same conclusion: it mostly cannot (Sally Broughton Micova and Andrea Calef, 'Elements for Effective Systemic Risk Assessment under the DSA', <<https://cerre.eu/news/cerre-on-dsa-systemic-risk-assessment/>> accessed 19 December 2023).

¹² Ofcom, 'How Ofcom is approaching online safety risk assessments', <https://www.ofcom.org.uk/__data/assets/pdfs/pdf_file/0019/255340/approach-to-online-safety-risk-assessments.pdf> accessed 19 December 2023.

¹³ DSA, Rec 137.

products, video-sharing platforms that distribute their own and third-party content, and music streaming services that redistribute music but also podcasts that are uploaded by their authors. The general expectation is that the distribution of own goods or content is usually subject to higher due diligence than that required by the DSA for third-party content; thus, companies offering their own content already have necessary legal incentives to police the risks posed by their own content.

If providers can design around regulation, the DSA might be hollowed out. But if the DSA pushes too hard to include everything that vaguely *relates* to regulated services and their relevant risks, it might disincentivise good user experience. Providers could start offering User-Generated-Content services separately from those that offer editorial content, with no obvious win for consumers. In my view, some middle ground between these positions is warranted. While for the purposes of counting users, a broad approach is preferable and arguably a better interpretation (Chapter 9), for the identification of relevant risks, the prescribed risk management should have some strong link to the *function* of the online platform as an ‘intermediary service’. Thus, if editorial content is clearly separated in the customer experience, even though the same interface is being used, risk management might not need to extend to editorial content.

In contrast, a hybrid service with both editorial and non-editorial content presented through the same recommender systems and product design, should consider both sides as relevant. This is why generative artificial intelligence (AI) that is integrated into regular platforms or search engines should end up being regulated by the DSA. However, a hybrid service with both types of content which are clearly separated, with little spill-over effects between them (eg in two separate sections of the marketplace or streaming service), should consider only risks for those parts that are closely linked to storage of third-party information (eg hate speech in podcasts, but not music).

Finally, because the DSA is also about a fair moderation process, including when enforcing contracts, these hybrid services can create a paradox. Creators whose content is ‘re-sold’ by platforms end up being protected less than is offered by them directly, only using the platforms. For instance, podcasters on streaming services could gain stronger rights vis-à-vis platforms than musicians offering music. If contractual relationships are untouched by the DSA, they leave the respective suppliers of content more exposed to the contractual dictates of platforms. This, in turn, creates a strong enough reason for VLOPs and VLOSEs to argue that parts of their services are outside the general risk management tools. Zalando, an online marketplace, is arguably already trying this strategy in the General Court to avoid being regulated as a VLOP.¹⁴

15.3 Risk Management Cycle

The system of risk mitigation measures envisaged by the DSA is best described as a *regular cycle of assessments*. The cycle is broken only by the potential trigger of the crisis

¹⁴ Case T-348/23 *Zalando v Commission* (case in progress, lodged 27/06/2023).

response mechanism (Article 36) and the release of new critical functionalities (Article 34(1)).

Risk mitigation takes place at least once a year in the following five steps:

- Step 1: The designated provider, initially four months after its designation and *at least once every year* thereafter, internally assesses and documents relevant systemic risks¹⁵ for each EU language or region in a *self-assessment report*.¹⁶ Such self-assessment entails proactively identifying and analysing systemic risks for each of the four relevant risk categories (and sub-categories) looking at least at enumerated risk areas. It ought to cover the entire service, including its own ‘design’, ‘functioning’, and ‘use’ made by third parties. The provider is implicitly given the discretion to design an optimal risk mitigation strategy that fits its unique product category and features. The report is eventually notified to the Commission.¹⁷
- Step 2: The designated provider must act upon the results of the self-assessment and write a *mitigation report* about what it does to mitigate the risks.¹⁸ The provider must ‘put in place reasonable, proportionate and effective mitigation measures, tailored to the specific systemic risks’.¹⁹
- Step 3: The designated provider annually shares its self-assessment with external auditing firms. The resulting *audit report* contains ‘positive’, ‘positive with comments’, or ‘negative’ assessment of each risk, and if relevant, operational recommendations on specific measures to achieve compliance and the recommended timeframe to achieve compliance.²⁰
- Step 4: The designated provider acts upon the recommendation in the audit report, and documents its stance and adopted measures in the *audit implementation report*. Finally, it submits the original assessment and action self-report, along with the audit report, audit implementation report, and other relevant documents to the digital services coordinator (DSC) of the establishment and the European Commission.²¹
- Step 5: The European Commission evaluates these reports and contrasts them with the findings made by vetted researchers, other academics, or any other information that is readily available. It can require improvements in so far as it can establish an infringement of the DSA standards. When there is a suspected breach of the DSA, the Commission can act without needing to wait until the risk management cycle provides results.

¹⁵ DSA, art 34(1).

¹⁶ Art 34(2) DSA requires that the assessment ‘shall take into account specific regional or linguistic aspects, including when specific to a Member State’.

¹⁷ DSA, art 42(4).

¹⁸ Note that in art 42, it refers to transparency as regards the mitigation measures, but no clear obligation to ‘produce’ a report as such.

¹⁹ DSA, art 35(1).

²⁰ DSA, art 37(4).

²¹ DSA, art 42(4).

15.3.1 Step 1: Self-assess the systemic risks

Articles 34 and 35 set out the basic matrix of risks that VLOPs and VLOSEs must consider. While each service is different, the DSA effectively requires that the designated providers pay special attention to some areas of risks and categories of risks. The risk matrix depicts the initial focus. However, the DSA's assessment is adaptive. The areas of risk of the platforms, such as recommender systems, are not set in stone and are only indicative of the main risks in the minds of the legislator when the DSA was adopted.²² The categories of risk are set exhaustively,²³ but sufficiently open and flexible to react and adapt to new developments in digital services.

The first two categories of risk especially help to ensure that any new risks are covered, since any risk can potentially qualify under the category of illegal content or negative effect on fundamental rights.

During the negotiations, Article 35 became somewhat of a catch-all provision for more explicit proposals that failed to become part of the DSA. For instance, Article 35(1)(c) mentions quite mysteriously content moderation of 'illegal hate speech or cyber violence'. Naturally, the remark was not intended to suggest that other types of illegal content are less relevant. It was only inserted because the European Parliament's proposal to include such an obligation for online platforms that are primarily used to disseminate user-generated pornographic content had failed to be taken on board.²⁴ Its original purpose was to tackle emerging issues regarding 'revenge porn'. However, the final political compromise only raised the issue as a concern that requires attention under the risk mitigation obligation.²⁵

The reference to illegal hate speech has similar origins. Germany was keen to promote its national law on hate speech (NetzDG).²⁶ As a result, the Council accepted a reference in Recital 87, by way of an example, to the 2016 Code of Conduct on countering illegal hate speech online²⁷ as a benchmark for processing valid illegal hate speech notifications in less than 24 hours. The reference, as with the previous one, does not mean that those standards should become a hard timeframe. In fact, they show the opposite. There was no political agreement on such issues. The same story applies to reference in

²² The DSA leaves an open door to 'emerging issues' in relation to VLOPs and VLOSEs, for which the Commission, in cooperation with the DSCs and the Board, shall coordinate the assessment (art 64 DSA).

²³ I am of the view that the list is exhaustive, despite the language which speaks of 'shall include the following systemic risks' in art 34(1). I agree with colleagues who argue that the scope is already very broad, and there is no indication as to what other groups of interest could be included. Plus, the language can imply that the companies are not limited to these risk categories, but can go beyond. See Saulius Kaleda, Paul-John Loewenthal, and Folkert Wilman, *Digital Services Act: Commentary* (forthcoming, OUP 2024) § 35 (C:12).

²⁴ The proposed art 24b reads: 'additional obligations for platforms primarily used for the dissemination of user-generated pornographic content', European Parliament, 'Amendments Adopted by the European Parliament on 20 January 2022 on the Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and Amending Directive 2000/31/EC (COM(2020)0825 — C9-0418/2020 — 2020/0361(COD))' [2022] OJ C336/48, art 24(b).

²⁵ Rec 87 DSA.

²⁶ Network Enforcement Act, *Netzwerkdurchsetzungsgesetz* (NetzDG) v 1 September 2017 (BGBl. I S 3352).

²⁷ European Commission, 'Code of Conduct on Countering Illegal Hate Speech Online' (31 May 2016).

Article 35(1)(k) to ‘deep fakes’.²⁸ It results from the European Parliament’s proposal to impose a specific obligation on VLOPs to ensure that deep fakes are labelled as such.²⁹ The provision did not make the final cut, but found its reflection in the long list of potential risk mitigation measures. Thus, it is merely flagged as an issue politically.

There is no obvious *ranking of* relevant risks, as outlined in Article 34. However, as will be discussed below, conceptually and evidence-wise, there should be a difference between tackling aggregate risks enabled by illegal content, and those enabled by lawful or mixed content. Article 34 has mostly procedural character—that is, companies must follow the process of scoping the potential risks. The existence of a procedural obligation to analyse does not automatically translate into an obligation to act. The substantive obligation to act is determined by Article 35.

15.3.2 Step 2: Risk mitigation measures

Once the risk-assessment report is ready, the platform must contemplate and implement specific measures to mitigate risks. If successful, the risk is mitigated, but not eliminated. Some residual risks always remain and are imposed on individuals or society at large (section 15.4.4). To comply, the providers must simply demonstrate that they have credibly tried to treat the problem, not show that they found a cure. It is broadly accepted that with many systemic risks, potential solutions can require the action of a much broader set of actors than just the online platforms.

Unlike Article 34, Article 35 implies a substantive obligation to counter the risks. However, the obligation to ‘put in place reasonable, proportionate and effective mitigation measures, tailored to the specific systemic risks’ is qualified by several constraints, such as discretion given to the regulatees,³⁰ the prohibition of general monitoring (Article 8), compliance with the fundamental rights, including the principle of legality, and the scope of the DSA itself (Article 1(1)). The result of this is a certain gap between an obligation to assess and an obligation to act upon the risks (see Figure 15.1).

This is why defining the scope of the obligation to assess is comparatively less important. General risk management thus focuses on incremental improvements more than on all-solving cures. VLOPs and VLOSEs usually cannot be realistically expected to ‘fix’ society and all its ills. Ultimately, in the broadest possible terms, the ambitious goal is to lower the negative impacts that digital technologies can have on humans and society at large.

To avoid unrealistic expectations, one must keep in mind that risk mitigation measures do not have the luxury of being implemented in a perfect world where technology only brings benefits and no costs. Technology rarely has only positives. To intervene

²⁸ Described as ‘an item of information, whether it constitutes a generated or manipulated image, audio or video that appreciably resembles existing persons, objects, places or other entities or events and falsely appears to a person to be authentic or truthful’.

²⁹ European Parliament (n 24), art 30a.

³⁰ Rec 90 and art 36(5) DSA *a contrario*.

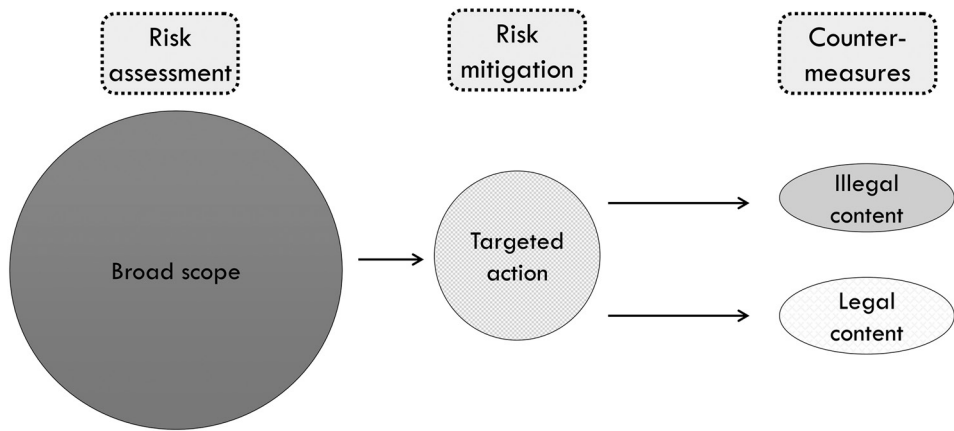


Figure 15.1 Scope of risk mitigation and risk assessment

successfully, we need to know the facts on the ground and be able to conceptualise them as wider social problems. The full extent of social costs is rarely visible from the tip of the iceberg.

Article 35(1) outlines the most obvious areas for intervention in a non-exhaustive manner. The list of interventions is aligned with the list in Recital 84. It includes:

- a) design of services, including their interfaces;
- b) terms and conditions, including their enforcement;
- c) content moderation practices, including their speed, quality, and resources;
- d) algorithmic systems, including recommender systems;
- e) advertising systems;
- f) internal processes and resources for risk detection, testing, and documentation;
- g) cooperation with trusted flaggers and implementation of ODS decisions;
- h) cooperation under codes of conduct or crisis protocols;
- i) awareness-raising measures for users;
- j) child-protecting measures, including age verification, parental control, and abuse reporting; and
- k) anti-manipulation measures, including against ‘deep-fakes’.

The list indicates that the DSA is envisaging the enlistment of legal, technical, and organisational measures of various kinds. Online platforms should consider *legal interventions*, such as changes in contractual terms, cooperating with others, and submitting themselves to self-regulation. They should also translate them into *technical interventions*, such as the design of algorithms and tools for advertisers, users, or their parents. Finally, they are asked to invest in *organisational capabilities* by improving the functioning of the internal processes and detection systems, as well as external cooperation.

The providers design their risk mitigation strategy autonomously. Unlike the Commission (section 15.4), they can freely design their policies on the interface of

legal and illegal content. They can use their discretion to design the underlying rules as they see fit, limited only by the broad limits of Article 14(4) (Chapter 12). Thus, two providers can easily adopt completely different approaches to the same risks as long as they can convincingly tailor their risk mitigation strategies. The discretion of providers is only limited by the European Commission's supervision of risk mitigation measures. Especially with respect to risks posed by legal content, there is a significant gap between what providers can legitimately do, and what the Commission can require them to do.³¹ This gap is given to the providers to experiment with underlying content policies and can always be reduced by the legislature expanding the notion of illegal content.

As argued in Chapter 13, the ability to punish uncooperative providers solely on the basis of Articles 34 and 35 is likely to be costly, due to evidence that the Commission will need to gather in order for its decisions to withstand judicial review before the Court of Justice of the European Union. This is why I argued that the Commission is likely to enforce risk mitigation provisions with Codes of Conduct, rather than solely on the basis of Articles 34 and 35 (Chapters 13 and 20). The only prescriptive content rule that the Commission could invoke cheaply against the underlying content policies is Article 14(4), which is of limited use for these purposes (Chapter 12.3.1).

The DSA does not expect interventions to be solely unilateral. On the contrary, interventions can include various collaborations with third parties or authorities. For instance, one can imagine that to mitigate risks affecting electoral processes, designated platforms could establish connections with local election commissions to better understand the landscape. More importantly, Recital 90 encourages VLOPs and VLOSEs to involve representatives of the recipients of the service, representatives of groups potentially impacted by their services, independent experts, and civil society organisations in the design of risk mitigation measures, including, as appropriate, surveys, focus groups, round tables, and other consultation and design methods.

All interventions adopted by platforms must be compliant with human rights standards. The DSA cannot prescribe actions that would violate fundamental rights, such as freedom of expression, or privacy and data protection of individuals. All the adopted measures are subject to requirements of 'reasonableness', 'proportionality', and 'effectiveness' (Article 35(1)). The entire DSA is subject to the prohibition of general monitoring obligations (Article 8 and Recital 30).

Thus, for instance, Article 35 cannot serve as a back door to impose measures, such as indiscriminate data retention, that would be impossible to impose by legislatures themselves. Any adopted measures are measures that are 'instigated' by the legislature, and the legislature is equally responsible to oversee that they do not go too far.³² This

³¹ Saulius Kaleda, Paul-John Loewenthal, and Folkert Wilman, *Digital Services Act: Commentary* (forthcoming, OUP 2024) § 35 (section B) noting that there is no automaticity between the risk assessment and the risk mitigation.

³² Case C-401/19 *Republic of Poland v European Parliament and Council of the European Union* ECLI:EU:C:2022:297. The same goes for the crisis response mechanism under art 36. For a similar view, Saulius Kaleda, Paul-John Loewenthal, and Folkert Wilman, *Digital Services Act: Commentary* (forthcoming, OUP 2024), § 34.

is why the same measures that are adopted to protect some interests could in themselves be scrutinised for potentially creating risks to other interests, such as privacy or freedom of expression. Recitals 90 and 153 make that crystal clear.

15.3.3 Step 3: External auditing

Under the DSA, compliance with all of the DSA's due diligence obligations, and additional commitments that they assumed based on codes of conduct (Articles 45–48), is subject to annual independent audits at the expense of the provider.

The DSA tries to create a robust framework for auditing providers' risk assessments. Limiting the audits to VLOPs and VLOSEs only has been criticised by some as 'unnecessary' and leaving a 'blind spot' in the regulatory landscape.³³ The concept of auditing very large services has developed in line with the underlying idea of asymmetric regulation: the bigger the firm, the greater the responsibility it attracts. While it is true that smaller companies can cause harm, it must be remembered that the DSA does not leave these smaller companies unregulated. Risk mitigation is only one of the tools, which complements the baseline rules that are created for the rest of the ecosystems.³⁴

Auditing as a means to achieve compliance acknowledges the informational asymmetry between regulators and regulated providers. At the same time, this means it is also subject to all the limitations of such a regulatory model, including the possibility of substandard audits being conducted, perhaps by auditing firms that are frequent clients of VLOPs or VLOSEs. However, the DSA innovates on several fronts to avoid these scenarios; only time will tell whether it does so successfully.

The DSA's auditors are independent but paid by VLOPs or VLOSEs. Auditors must obtain cooperation and assistance, including access to data and premises (Article 37(2)). It prohibits platforms from 'unduly influencing' or 'undermining' the performance of audits but also affords auditors with appropriate confidentiality and professional secrecy guarantees. Those, obviously, cannot come at the expense of the envisaged transparency, supervision, and enforcement. However, the guarantees should help to build trust between providers and their auditors when providing explanations and access to data. Auditors by definition must have access to more information than they can reveal in their audit reports or their publicly circulated versions.

The scope of the auditor's work includes not only all special obligations of VLOPs and VLOSEs, but all applicable due diligence obligations, including those that were accepted voluntarily through codes of conduct or crisis protocols (Article 37(1)). This

³³ Johann Laux, Sandra Wachter, and Brent Mittelstadt, 'Taming the Few: Platform Regulation, Independent Audits, and the Risks of Capture Created by the DMA and DSA' (2021) 43 *Computer Law & Security Review* 105613.

³⁴ Thus, while smaller infamous websites, such as 4chan, are unlikely to qualify as VLOPs, and anecdotally can be said to contribute to the radicalisation of youth, they remain subject to other DSA obligations concerning illegal content and content moderation. Tim Hume, '2 Men Killed Outside Gay Bar by Suspected Far-Right Gunman' *Vice* (13 October 2022) <<https://www.vice.com/en/article/v7vp8j/bratislava-slovakia-gay-bar-shooting>> accessed 5 September 2023.

means that when providers enter into these voluntary practices, they also expand the scope of audits. Each relevant code of conduct or crisis protocol thus gains a supervisory mechanism which is wholly subsidised by the providers. Given that providers also pay special regulatory attention to the European Commission, they are clearly expected to bear the financial costs of some of the externalities that they impose on others.

Article 37(3) sets several requirements for auditing firms: a) independence from and lack of conflict of interest with VLOPs and VLOSEs and connected legal persons; b) proven expertise in risk management, technical competence and capabilities, and c) proven objectivity and ethics. The independence and lack of conflict of interest are further specified by means of examples: the auditing firm must not have provided the audited VLOP or VLOSE with other non-audit (eg consulting) services relating to audited matters in the 12 months prior to and after the audit, performed the auditing services of a particular VLOP or VLOSE for more than 10 years in a row, or performed the audit in return for remuneration that is contingent upon the result of the audit.³⁵

The European Commission has the ability to issue delegated acts that further specify how to perform the DSA audits (Article 37(7)), including by harmonising the templates, procedures and methodologies. The audits can be also subject to standardisation which can be equally initiated by the European Commission (Article 44). Article 37(4) gives some hints on the basic things that will require further specification, in particular the methodology of audits, consulting of third parties, and the granularity of operational recommendations if the audit is not fully positive. Article 37(7) suggests templates as a possible way of standardising the auditing practice. At the time of writing, the Commission has only published a draft of the Delegated Act for public consultation, which has been heavily criticised by the auditing industry for its vagueness.³⁶

Audits are potentially an important check on the obligation to conduct risk assessment and mitigation by providers. Auditors are meant to independently access the data, and report on the findings to the providers in a way which is visible to everyone. If they cannot access some parts of the service, independently verify some claims or generally lack a proper explanation for what they observe, they must explicitly explain the circumstances and reasons in their reports (Article 37(5)). When VLOPs or VLOSEs follow up on the reports, they must react to this, again in public.

One of the worries expressed by researchers is that the narrow set-up of the auditing services can lead to audit capture.³⁷ The important innovation that the DSA's audit presents is the ability of researchers to independently verify and examine the audits. The DSA introduces researchers as a de facto check on audits (and regulators). Because providers no longer control the researchers' access to data, they also cannot pick and

³⁵ Some of these requirements were clearly inspired by the Audit Regulation (eg, art 17): see European Parliament and Council Regulation (EU) No 537/2014 on specific requirements regarding statutory audit of public-interest entities and repealing Commission Decision 2005/909/EC [2014] OJ L158/77 (Audit Regulation), art 17.

³⁶ See 'Digital Services Act: Delegated Regulation on Independent Audits Now Available for Public Feedback' (*Shaping Europe's digital future*, 5 May 2023) <<https://digital-strategy.ec.europa.eu/en/news/digital-services-act-delegated-regulation-independent-audits-now-available-public-feedback>> accessed 5 September 2023.

³⁷ Laux, Wachter, and Mittelstadt (n 33).

choose their researchers. Thus, if the auditors engage in audits that are too lax, their failings can be uncovered by researchers who can verify their claims. Knowledge of this possibility should be an important incentive for auditors to tread much more carefully. What the DSA lacks, however, is a proper mechanism to strip auditors of their credentials and solutions in case auditing markets are not properly competitive.

Thus, one of the crucial tasks of the delegated act should be to spell out the consequences of failing to act with objectivity and professional ethics (Article 37(3)(c)). The opposite type of worry concerns the competitiveness of the auditing markets. Because consulting services are much more lucrative than auditing, there is a risk that opportunity costs to big auditing firms can limit the market to a few players. This, in turn, could affect the competition, and quality of the services. At the time of writing, the only input from the auditing industry is the Commission's consultation on the delegated act. Thus, it is hard to evaluate whether the DSA audits might suffer these types of problems.

After the finalisation of audits, the providers must follow up and justify their actions or inaction. They must document their actions and submit them in writing to the European Commission, which publishes them in its public repository in a redacted form. This should allow the public, including journalists and researchers, to study the claims and the evidence, and further interrogate their credibility. If it works, it will create a circle of information flows that is hard to manipulate by auditors themselves. This will necessitate vibrant research communities to act as a check.

As regards what affects the risk management cycle, the DSA establishes that the audit reports (Article 37(4)) must include a summary of substantiated findings, the 'positive', 'positive with comments', or 'negative' audit compliance opinion, and operational recommendations on specific measures to achieve compliance with the DSA. Where the auditing firm was unable to audit certain elements of services, it must nevertheless conclude based on what is known from its investigations and state the reasons why some parts could not have been directly audited (Article 37(5)).

15.3.4 Step 4: Provider's follow-up on external audits

If the audit report is positive, the VLOP or VLOSE does not need to follow up. However, even a positive report does not protect a provider from potential enforcement actions by the Commission. At the same time, a negative report does not indicate the DSA has been violated in the eyes of the Commission. Fully positive audits are unlikely to be common because even a single shortcoming means that the outcome is 'positive with comments'. If the audit report is 'positive with comments' or 'negative', hence suggesting at least partial non-compliance with the DSA or commitments under the codes of conduct or crisis protocols, the provider must prepare an audit implementation report within one month.

Providers are not explicitly bound by the recommendations made by auditing bodies; however, if they decide to not implement them, they must justify why, and set

out any alternative measures to address the identified non-compliance (Article 37(6)). The risk assessment, the description of the risk mitigation measures, the audit report and the audit implementation reports have to be immediately sent to the European Commission and the DSC of establishment upon completion of each one (Article 42(4)). It must be published (Article 42(4)) at the latest three months after the receipt of each audit report.

15.3.5 Step 5: Oversight by the Commission and public

The system, as outlined above, can only work if there is sufficient public oversight of each of these steps. Apart from the authorities, both civil society and researchers have an important role to play. Thus, while the Commission is allocated exclusive competence to enforce the provision, the broader responsibility to inform the Commission's enforcement rests also with the public. While the DSA envisages a complaint mechanism only on a national level (Article 53), the Commission is likely to receive and react to complaints as a matter of good administration.

While audits performed by firms are external and to strict independence requirements, they are still performed by professionals who are paid by private companies. Thus, a 'trust but verify' approach is more than appropriate. The providers are obliged to facilitate bulk access through dedicated interfaces, such as APIs or online databases (Article 40(7)). Researchers, on the other hand, offer their own academic independence, methodological prowess, and strong subject matter expertise. As experts in various areas of social sciences, they can better spot potential problems and work on uncovering potential solutions to them. Furthermore, as experts in various areas of data science and forensics, they can help regulators shed light on opaque systems and their functioning.

The European Commission, along with the DSCs of establishment, must have access 'to monitor and assess compliance with' the DSA itself (Article 40(1)). They can additionally request an explanation of 'the design, logic functioning and the testing of their algorithmic systems, including their recommender systems' (Article 40(3)). These authorities thus access data in order to verify various statements made by providers and their auditors. The enforcement of Articles 34 and 35 is subject to exclusive competences, and even private enforcement of these provisions is generally not possible (Chapter 19.2).

15.3.6 DSA compliance officers

To further cement the risk management obligation within the companies, VLOPs and VLOSEs must create a 'compliance function'; a role that is independent of the provider's daily business operations, such as product development (Article 41(1)). This function must have sufficient authority, stature, and resources, as well as access

to the management body of VLOPs and VLOSEs. One or more compliance officers can be appointed to this DSA unit within companies. This allows the specialisation of compliance officers in the remit of DSA's responsibilities. If more compliance officers are appointed, they must be directed by the head of compliance (Article 41(2)). The head of compliance is the person who should be raising DSA awareness, compliance and risk-mitigation issues with the management body of the company.

The management body of each VLOP and VLOSE is ultimately responsible for devising the organisational structures that allow heads of DSA compliance to carry out their tasks effectively and independently within the organisation (Article 41(5)). At least once a year, the management body must approve and review 'strategies and policies for taking up, managing, monitoring and mitigating the risks' (Article 41(6)). The management body is explicitly required to devote sufficient time to and be 'actively involved' in risk management issues (Article 41(7)).

Compliance officers within the company's DSA compliance unit are tasked with monitoring how the company's services comply with all provisions of the DSA (Article 41(3)). The compliance officers employed must have the professional qualifications, knowledge, experience, and ability necessary to fulfil the tasks. The DSA does not specify a baseline for these qualifications and desired characteristics. The DSA thus does not require that compliance officers need to be lawyers, or computer scientists who understand the intricacies of the product's architecture. The head of the compliance function must be 'an independent senior manager' who has 'distinct responsibility' for DSA compliance. He or she must report directly to the management body of VLOPs or VLOSEs and must always be able to raise concerns and warn about relevant risks or non-compliance with the DSA. The head of compliance with DSA must be protected against removal without the prior approval of the company's management body. Her/his identity per each VLOP or VLOSE must be notified to the European Commission and the DSC of establishment (Article 41(4)).

Individual compliance officers have internal and external tasks. Externally, they are the primary contact for communication between the European Commission and the DSC of establishment. Internally, they are the persons advising on DSA compliance. They should guide the risk-assessment phase of their services to assure its completeness and objectivity. They must review the implemented mitigating measures for their effectiveness, proportionality and reasonableness. They organise and supervise the external audit of the risk mitigation measures. And finally, they monitor compliance with all DSA obligations, including those voluntarily accepted in the Codes of Conduct or Crisis Protocols, and internally report on any non-compliance.

The role thus is not dissimilar from that of the data protection officer introduced by GDPR. However, data protection officers can be also external persons. Because the DSA applies only to VLOPs and VLOSEs, which are assumed to be run by bigger companies, DSA compliance officers are assumed to be mostly internally employed by companies. This is clear from their expected involvement in daily operations.

15.4 A Theory of the DSA's Limited Risk Management

Since no risk management cycle had come to an end at the time of writing, the best I can do is offer a theory of what the European Commission is entitled to do in terms of risk management.³⁸

While the DSA is drafted in a balanced manner, no rules are immune to misuse. Recital 153 grounds the future role of the European Commission as follows:

This Regulation respects the fundamental rights recognised by the Charter and the fundamental rights constituting general principles of Union law. Accordingly, this Regulation *should be interpreted and applied in accordance with those fundamental rights, including the freedom of expression and of information, as well as the freedom and pluralism of the media*. When exercising the powers set out in this Regulation, all public authorities involved should achieve, in situations where the relevant fundamental rights conflict, a fair balance between the rights concerned, in accordance with the principle of proportionality.³⁹

The litmus test for how the Commission sees its own role will be what risk mitigation strategies it considers insufficient to comply with Articles 34–35 DSA.

As argued in Chapter 13, the Commission has a strong legal mandate to request mitigation measures for *illegal content*. The key limiting legal principles here are proportionality, the prohibition of general monitoring obligations, and the fundamental rights of others. The key practical limit is the Commission's resources to build cases and gather facts (Chapter 20).

The Commission must tread much more carefully when acting on risks that fall only under Articles 34(1)(b)–(d). The Commission does not have the power to step in as a surrogate legislature on the content questions. When controversies about legal content arise, such as some types of disinformation, or vulgar content, it must limit itself to what is its mandate. The mandate is not only determined by the DSA itself but also by European human rights law that requires restrictions on freedom of expression to be of sufficient 'quality of the law'.⁴⁰

Given that the Commission is imposing restrictions on the largest services, it is crucial that Articles 34–35 are viewed as what I would term a *limited risk mitigation* approach.

³⁸ Part of this text was published in Martin Husovec, 'Rising Above Liability: The Digital Services Act As a Blueprint for the Second Generation of Global Internet Rules' [2023] Berkeley Technology Law Journal (forthcoming).

³⁹ Emphasis mine.

⁴⁰ Ch 3.

15.4.1 Limited vs full risk management systems

In any risk management system, the relationship between substance and process is the most difficult one to get right. To begin, any proposal that tries to tackle ‘risks’ or overall ‘harmful behaviour’ cannot ignore that on user-generated content services, what users say or do remains a key risk factor. While ‘undesirable’ user behaviour can be influenced by the design of services, in some form it will continue to exist irrespective of this intervention; the risks involved with such services thus result less frequently from non-human external factors, and more commonly from unpredictable, and very human, factors.

Managing the risks of crowds often requires telling individuals how they must behave. If authorities subject the occurrence of selected illegal user behaviour to certain metrics, the legitimacy of such a policy is straightforward. The legislatures already agreed that such behaviour is illegal, and the authority is only trying to quantify compliance. However, if authorities subject the occurrence of some *legal* expressions to the same metrics, they will unavoidably end up policing the bounds of what people can say—that is, the content of their communications. Putting quotas on user expressions, when taken to its logical conclusion, means telling some people what they cannot say. It means creating content rules.

Whether addressing ‘harm’ or ‘risk’, the key litmus test is *who* sets the boundaries for the content of communications. One approach gives such power to decide to authorities; others leave it to individuals, providers, and parliaments.

- The *full* risk management approach gives the broadest power to authorities to ask companies about how their service design influences what happens on the platforms. Authorities observe, compare, analyse, and ask for changes, including by imposing tailored standards or quotas of ‘problematic’ user expressions, regardless of their legality. The mandate of authorities thus extends to lawful but awful content and permits them to become surrogate legislatures policing the boundaries of free expression.
- The *limited* risk management approach shares the concerns about system design that might encourage various risks but stops short of giving authorities the power to rewrite what lawful individual expression should be banned or suppressed by quotas or quota-like metrics. This approach recognises that authorities do not have the legitimacy of parliaments. Parliaments should remain responsible for setting the goalposts of illegal content of communications. If a specific risk or harm is particularly damaging, parliaments can move the goalposts further.⁴¹ As a result, the authorities limit their demands regarding legal content to solutions that

⁴¹ In the UK, the self-harm debate led to the empowerment obligation and a proposal to create a new offence of ‘encouraging or assisting serious self-harm’: Online Safety Bill (2022–23) HL Bill 87 (Rev)-VII(a) Amendments for Committee (Supplementary to the Seventh Marshalled List), 58 <<https://bills.parliament.uk/publications/51205/documents/3437>> accessed 5 September 2023.

preserve people's agency by giving them freedom of choice; such solutions mostly empower or redesign users' choice architecture.

The DSA does *not* explicitly address the problem of whether the Commission can require providers to change their contractual standards of 'lawful but harmful content' as part of the risk management strategies.⁴² Illegal content is defined by legislatures.⁴³ Due to the absence of any explicit legal mandate, any attempts to prohibit or suppress specific expression that is legal would arguably violate the rule of law because of the insufficient legal basis. Thus, I contend that the DSA adopts the limited risk management approach. This does not mean that illegal content targeting (and thus content-specific) measures cannot affect legal content, but that the legal content cannot itself become the target.⁴⁴

In Chapter 13, I discussed a 2023 Disinformation Study that seems to imply that under the DSA, the Commission requires *content-specific* interventions against disinformation, regardless of the legality of disinformation, to mitigate the risks of pro-Kremlin narratives being spread by Kremlin-aligned actors.⁴⁵ As discussed there, the key problem with such an expansive approach is that it pretends that Article 34(1)(b)–(d) constitute the legal basis for the Commission to restrict the distribution of specific expressions, and thus to go beyond existing categories of illegal content.

In my view, the internal division between Article 34(1)(a) and (b)–(d) would lose any purpose if such reading were to be accepted. Moreover, the DSA's insistence on illegal content across parts of the DSA (eg, Article 16) would have no purpose if the regulator could redraw such boundaries ad hoc. Finally, and most importantly, under the existing standards of the ECtHR, this in my view goes beyond the legal mandate conferred on the Commission.⁴⁶ And I do not seem to be alone in this view.⁴⁷

There are very few arguments that can be made in support of a full risk management approach under the DSA. Recital 88 says that mitigation measures can include 'discontinuing advertising revenue for specific information'; however, it is not clear whether this relates to legal information at all. Similarly, the focus on terms and conditions in Article 35(1)(b) does not imply any dictate of the rules on legal content but

⁴² Art 35(1)(b) speaks of 'adapting their terms and conditions and their enforcement'. In my view, this does not necessarily mean prohibiting lawful behaviour or content. It speaks to the clarity and predictability of rules.

⁴³ DSA, art 3(h).

⁴⁴ The same conclusion is reached with slightly different arguments by Saulius Kaleda, Paul-John Loewenthal, and Folkert Wilman, *Digital Services Act: Commentary* (forthcoming, OUP 2024), § 34.

⁴⁵ DG-CONNECT (EU Commission), *DSA: Application of the Risk Management Framework to Russian Disinformation Campaigns* (EU Publications Office 2023) <<https://data.europa.eu/doi/10.2759/764631>> accessed 5 September 2023.

⁴⁶ The argument is that art 34 DSA on its own is not sufficient to fulfil the human rights requirements under the EU Charter to legitimise prohibitions of speech to be 'prescribed by the law' (art 52 of the EU Charter of Fundamental Rights). See the excellent article on the rule of law requirement in this context by Graham Smith, 'Online Harms and the Legality Principle' (*Cyberleagle*, 20 June 2020) <<https://www.cyberleagle.com/2020/06/online-harms-and-legality-principle.html>> accessed 5 September 2023 ('the regulator's views about harm would sit alongside, and effectively supplant, the existing, carefully crafted, set of laws governing the speech of individuals'). For further discussion, Chapter 13.

⁴⁷ Saulius Kaleda, Paul-John Loewenthal, and Folkert Wilman, *Digital Services Act: Commentary* (forthcoming, OUP 2024) § 35 (C:10) noting that 'the obligation to take risk mitigation measures cannot, in principle, be a way to force providers to contractually prohibit certain information that does not qualify as illegal content'.

simply can be understood as a reference to other obligations, such as ease of reading, or their accessibility that matter for Article 14. The 2023 Disinformation Report invokes Recital 84, which states:

When assessing the systemic risks identified in this Regulation, those providers should also focus on *the information which is not illegal*, but contributes to the systemic risks identified in this Regulation. Such providers should therefore pay particular attention on how their services are used to disseminate or amplify misleading or deceptive content, including disinformation.⁴⁸

However, focusing on legal content as a risk factor under Article 34 is a different matter than having an obligation to intervene against such content in a content-specific way under Article 35. The measures mentioned in Recital 84, such as ‘design and functioning of their service’, ‘coordinated manipulation and use of their services’, or ‘the inauthentic use of the service, such as the creation of fake accounts, the use of bots or deceptive use of a service, and other automated or partially automated behaviours’, all point toward content-neutral interventions that are based on the authenticity of human expression and not on contents of those expressions. Other interventions mentioned by the DSA in Article 35 are either content-neutral or relate to illegal content. The Commission’s own FAQ states the following about the DSA:

How can harmful but not illegal content be effectively addressed? *To the extent that it is not illegal, harmful content should not be treated in the same way as illegal content.* The new rules will only impose measures to remove or encourage removal of illegal content, in full respect of the freedom of expression.⁴⁹

The limited risk management approach can be best explained through an analogy with managing risks during public protests. Imagine a public assembly speaking against immigration policies gathering in the streets of a city. The role of providers can be analogised to the position of protest organisers—they do not control individuals, but bring crowds together. The DSA designates the largest services in the EU to be such controlled public spaces;⁵⁰ it tasks the providers to analyse risks created by crowds, and intervene if needed.

What is the role of the state, and correspondingly a provider, in such a case?

⁴⁸ Emphasis mine.

⁴⁹ European Commission, ‘Questions and Answers: Digital Services Act’ (25 April 2023) <https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348> accessed 5 September 2023 (emphasis mine).

⁵⁰ The DSA Impact Assessment states: ‘This transforms such very large platforms into de facto public spaces for businesses to find consumers, for authorities, civil society or politicians to connect with citizens and for individuals to receive and impart information; Commission, “Impact Assessment” (Commission Staff Working Document) Accompanying the Document “Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and Amending Directive 2000/31/EC”’ SWD(2020) 348 final, 9.

The state can impose safety measures on organisers and protesters to protect them from others, and others from them, to avoid causing harm to people, property, or businesses. Physical safety measures benefit freedom of expression because they make everyone more comfortable to express their views. To achieve this, the authorities can ask organisers to take various safety measures particularly to prevent illegal behaviour by protesters or counter-protesters, including the use of excessive disruption or noise. Beyond illegal modes of expression, the *authorities* cannot control who speaks or protests, what posters or chants they use, or where they present them. However, *organisers* of a protest can go beyond illegality, whatever their motivation. They can self-impose stricter rules on crowds.

Imagine now that the public assembly has two teams of rule enforcers, dressed in red and blue jackets. Red enforcers represent the state, and they can only intervene when protesters violate the red rules—conveying messages that are illegal, or violating content-neutral rules about things like crowding or volume. Blue enforcers are paid by the organisers. They are the analogue of content moderators. Because organisers want a legitimate assembly where families can gather, they may ask all its participants to respect some of their own basic rules. These blue rules differ from red rules. Among other things, they allow organisers to intervene much earlier. For instance, they can say that posters with profanities are not permitted because they are likely to lead to illegal behaviour.

For efficiency reasons, the authorities will expect blue enforcers to also enforce red rules. This is the analogue of delegated enforcement which providers engage in daily when they remove illegal content. However, red enforcers *cannot* enforce blue rules. Blue rules are the analogue of contractual self-constraint that platforms adopt to make their services appealing to users and advertisers. Red enforcers cannot turn the self-imposed ban on profanities against the organisers to end the protest, or arrest protesters. To justify such intervention, authorities must stick to the red rules. Logically, they cannot tell organisers what blue rules to adopt either, because that is the prerogative of parliaments.

The authorities can, however, require that if the likelihood of violence by protesters is high, then organisers must take extra measures to keep bystanders safe from further escalation. These extra measures are the analogue of design interventions on digital services. There is a growing literature arguing in favour of various design interventions that limit the speed at which information travels through the networks. Such circuit-breakers,⁵¹ friction-in-design⁵² or similar interventions,⁵³ are considered the 21st-century equivalent of content-neutral time, place, and manner restrictions of speech.⁵⁴

⁵¹ Daphne Keller, 'Amplification and Its Discontents' (*Knight First Amendment Institute at Columbia University*, 8 June 2021) <<http://knightcolumbia.org/content/amplification-and-its-discontents>> accessed 5 September 2023.

⁵² Brett Frischmann and Susan Benesch, 'Friction-In-Design Regulation as 21st Century Time, Place, and Manner Restriction' 25(2) *Yale Journal of Law & Technology* 376.

⁵³ Jonathan Stray, Ravi Iyer, and Helena Puig Larrauri, 'The Algorithmic Management of Polarization and Violence on Social Media' (*Knight First Amendment Institute at Columbia University*, 22 August 2023) <<http://knightcolumbia.org/content/the-algorithmic-management-of-polarization-and-violence-on-social-media>> accessed 10 September 2023.

⁵⁴ Frischmann and Benesch (n 52).

The interventions, such as placing limits on how users can communicate with others, find third-party content, or share their material outside of closed groups, incorporating negative feedback from users, or other design choices, are proposed to potentially limit the risky features of the digital services.

Time, place, and manner restrictions are commonly accepted types of restrictions in liberal democracies.⁵⁵ They allow legislatures and authorities to ‘manage’ risks of public gatherings without interfering unreasonably in the substance of their expressive purposes. Such rules regulate speech in a manner that minimises disruption of public space while still protecting expressive activities. Timothy Zick views such constraints as a ‘multi-layered and complex system of restrictions’ that constitutes a ‘framework of managed dissent’.⁵⁶

While providers organise protests not as part of their own expressions but as a business, they nevertheless do in fact bring together crowds and similarly orchestrate their gathering, and sometimes even direct expressions through recommender systems. As such, a provider’s involvement is much deeper than that of the owners of property where protests take place. The design of their public platforms, recommender systems, and the underlying rules of engagement, heavily influence how people can express themselves in their own little crowds (eg, the groups in which they gather) and on the main stage (eg, in the main recommender systems).

The goal of the measures that are imposed on protests should be an assembly that takes a form of peaceful protest. The authorities have a ‘duty to reflect on the possible alternative solutions and propose another venue to the organisers’.⁵⁷ In the United States, the organisers can be asked to pay a fee covering certain costs, or post bonds for potential damage caused by the protests.⁵⁸ The mass protests thus can cost organisers hundreds of thousands of dollars because they must provide the necessary protest infrastructure, such as tents, restrooms, medical care, etc.⁵⁹ Thus, even if it remains legal to express opinions in some riskier ways, such as through the burning of flags, the state is managing when and how this occurs.⁶⁰

The attempts by digital regulators to curb risks posed by lawful expressions by adopting content-specific measures can be analogised to police trying to prevent clashes during public assemblies by banning certain types of assemblies altogether (eg, banning pro-Palestinian or pro-Israeli assemblies for risks of escalated violence), instead of managing the risks of illegal modes of expressions during such assemblies.⁶¹ As recently emphasised by the ECtHR,

⁵⁵ For the ECtHR, *Primov and Others v Russia* App no 17391/06 (ECtHR, 12 June 2014), para 130 (‘it is not disputed that the domestic law permitted the authorities to regulate the manner, timing and location of public events, depending on the characteristics of the specific area at issue’). For the US, *Ward v Rock Against Racism* 491 US 781 (1989).

⁵⁶ Timothy Zick, *Managed Dissent: The Law of Public Protest* (CUP 2023) 35.

⁵⁷ *Primov and Others v Russia* (n 55), para 131.

⁵⁸ Zick (n 56) 51.

⁵⁹ *ibid* 54.

⁶⁰ *ibid* 44.

⁶¹ This is what recently happened in Germany, Deutschlandfunk, ‘Gericht kippt Verbot von pro-palästinensischer Demonstration’ (13 October 2023) <<https://www.deutschlandfunk.de/gericht-kippt-verbot-von-pro-palaestinensischer-demonstration-100.html>> accessed 19 December 2023.

It should be noted that an individual does not cease to enjoy the right to freedom of peaceful assembly as a result of sporadic violence or other punishable acts committed by others in the course of the demonstration if the individual in question remains peaceful in his or her own intentions or behaviour ... Even if there is a real risk that a public demonstration might result in disorder as a result of developments outside the control of those organising it, such a demonstration does not as such fall outside the scope of paragraph 1 of Article 11, and any restriction placed thereon must be in conformity with the terms of paragraph 2 of that provision.⁶²

15.4.2 What are the consequences for the Commission?

Consider a hypothetical situation in which the Commission has gathered clear evidence that a certain type of self-harm content that is lawful across the EU is highly damaging for adults because it increases eating disorders. Can the Commission simply request its ban be imposed across the terms and conditions of all the VLOPs and VLOSEs? In my view, the answer is no. So, what can the Commission do then? How should it approach such risks?

The Commission should always clarify if it is acting on the basis of illegal content (Article 34(1)(a)), even if this is *along* with the other three grounds, *or solely* on the basis of any of the other sub-categories (Article 34(1)(b)–(d)). If illegality is missing, the interventions should be more limited and follow a different sequence of escalation of mitigation actions (see Table 15.2).

For the Commission approaching legal content, empowerment and content-neutral design interventions are much less problematic than expecting visibility restrictions and content removals for specific legal content. The DSA offers no explicit legal test to demarcate how far the Commission may go. The only obvious limit is the adherence to human rights, the prohibition of general monitoring obligations, and the need to gather evidence to support its actions.

Daphne Keller offers a typology of de-amplification policies:⁶³ (a) illegal content policies, (b) harmful content policies, and (c) content-neutral policies. Of the three, the DSA arguably does not extend to (b) if we understand it to mean content that is legal. Keller's conceptualisation, informed by US constitutional law, offers very interesting ways to think about the content-neutral approach for legal content in a European setting. However, I would categorise the policies differently. For instance, de-amplification policies based on data protection, or media laws protecting children, should be in the category of illegal content policies and not harmful content policies. This is because, from my perspective, the distinguishing factor between illegal content policies (a) and harmful content policies (b) is the existence of a legal basis for a specific restriction.

⁶² *Lurijzen and others v The Netherlands*, App nos 56896/17, 56910/17, 56914/17, 56917/17, and 57307/17 (ECtHR, 21 November 2023), para 50 (generally relying on a Grand Chamber case, *Kudrevičius and others v Lithuania*, App no 37553/05 (15 October 2015)).

⁶³ Keller (n 51).

Table 15.2 Limits of the general risk management approach

Content type	Type		Priority by type of intervention	Examples
Illegal content (e.g., hate speech, terrorist content, child-abuse material)	Full risk management system	Limited risk management system	Content removal	<i>Removal of content</i>
			Complementary actions, such as visibility restrictions, redesign, or empowerment	<i>De-ranking or demonetization of a class of content, empowerment of users who view the content</i>
Empowerment			<i>Choices to customize the user experience; labels; fact-checking;</i>	
Content-neutral redesign of services			<i>Content sharing restrictions; introducing friction; changes in neutral proxies for recommender systems;</i>	
Legal content (e.g., some disinformation, sensitive, nude, vulgar, shocking content)		Content-specific visibility restrictions		<i>Targeted de-ranking of a legal class of content based on what it expresses</i>
		Content removal		<i>Contractually prohibiting specific legal expressions in terms and conditions</i>

The (c) category then represents a subset of policies against content in either of the two categories; however, it is restricted by the type of interventions that can apply.

If the typology is seen in this light, my argument for the DSA’s limited risk mitigation approach is that Articles 34–35 allow the Commission to take action against both types of content; however, for the latter, the interventions are only limited to interventions that Keller foresees in category (c). For me, this categorisation has less to do with the proportionality of the underlying policy as with its compliance with the rule of law due to sufficient legal basis.⁶⁴

To illustrate this, consider the protection of children on video-sharing services. European content laws have adopted a broad standard of harmful content that impairs ‘the physical, mental or moral development of minors’, such as pornography and gratuitous violence.⁶⁵ Such harmful content can be made available only ‘in such a way as to ensure that minors will not normally hear or see them’, including through selecting the time of the broadcast, age verification tools, or other technical measures. While the content per se is not illegal,⁶⁶ it is illegal for platforms to show it to minors under some circumstances. This, in turn, gives the Commission the ability to invoke illegality—even though conditional.

⁶⁴ For a similar view but grounded in the balancing, Saulius Kaleda, Paul-John Loewenthal, and Folkert Wilman, *Digital Services Act: Commentary* (forthcoming, OUP 2024) § 35 (section E) noting that removing, blocking, or disabling of access to legal disinformation is likely to be problematic from the viewpoint of freedom of expression.

⁶⁵ Audiovisual Media Services Directive (AVMSD), art 6a.

⁶⁶ Seen from this perspective, little of the content is illegal per se. Copyright laws also only impose constraints conditionally, as do many other areas of law.

If no comparable rule exists for adults, restricting such content would mean restricting legal content. Thus, for instance, if the content that promotes some problematic diets is not prohibited by any legal norm, the scope for acceptable interventions narrows. The ability of the regulator to demand interventions against risks posed by such lawful content should be limited first to empowering users, and if that fails, they should progress to impose other content-neutral policies, such as changes to how content is shared on platforms. This is what I called 'the DSA's red line'.⁶⁷ Content neutrality, however, does not immediately imply proportionality.

To summarise, the possible limiting test could be whether the mitigation measures targeting lawful behaviour impose content-neutral or content-specific restrictions. If the measures are content-neutral, the Commission is free to impose them as long as they are proportionate and otherwise in line with the DSA. If such restrictions are content-specific, they do not even have to be tested on proportionality, because they exceed the legal mandate given by the DSA. To return to my previous example of managing public protests, it would stop the Commission from blaming the lack of self-imposed restrictions on profanities against the providers as evidence of a violation of general risk management. However, it would allow it to scrutinise how the design features of the system, such as registration, or interfaces, escalate to illegal actions and generally affect the well-being of individuals.

In risk management under the DSA, especially when the risks are posed by legal content, it is critical to separate the *obligation to investigate risks* (Article 34) from the *obligation to mitigate risks* (Article 34). While the obligation to investigate is very broad, the obligation to mitigate is confined by legality and proportionality. For this very reason, joint screening of risks posed by legal and illegal content is possible, but for the formulation of the enforcement goals, the means must substantially differ:

- The risks posed by *illegal content* can have as their goal suppression of specific content (eg, 'reduce hate speech within recommendations by X%') because they are based on the legislature's articulation of illegality; the selected means must remain proportionate, and thus cannot disproportionately impact other fundamental rights, including the freedom to share lawful expressions, as collateral damage.
- In contrast, where risks are posed *also by legal content*, the enforcement goal for mitigation measures should only take the form of content-neutral interventions (eg, 'redesign sharing options for all content') but not of content-specific measures (eg, 'de-rank all incorrect information about diet XY') due to missing legal mandate for suppression of such content. The selected content-neutral interventions must remain proportionate.

⁶⁷ Martin Husovec, 'The Digital Service Act's Red Line: What the Commission Can and Cannot Do About Disinformation' [forthcoming, 2024] *Journal of Media Law*.

15.4.3 Freedom of companies to mitigate risks

The fact that the Commission cannot prescribe a content-specific intervention for risks posed by legal content does not mean, however, that the provider cannot freely adopt such measures. On the contrary, the provider is free to do so. The red line suggested above only applies to the European Commission as the sole enforcer of Article 35 DSA.

Since the companies mostly retain the freedom to design their policies to fit their business, they can naturally exceed the obligations that the European Commission can impose on them. Thus, for instance, even if the Commission might be unable to limit some type of disinformation or nudity, providers can decide to contractually restrict it anyway.

As a result, companies do not have to make as strict distinctions between legal and illegal content in their risk assessment and mitigation. However, it also means, that the metrics that are used to quantify compliance need to be treated with utmost caution because the vocabulary used by companies can differ substantially from legal definitions.

The key limit of providers' rule-making powers is Article 14(4) DSA and risk mitigation strategies that devolve some decision-making to individuals and groups (eg, an obligation to give choice in recommender systems or allow user-level moderation). I have explained the first point in Chapter 12. The second point is discussed in the next section.

15.4.4 Appraising, and allocating risks

Julia Black's work mapping reliance on risk-based regulation in financial services offers a number of lessons for how the technology industry might address risk mitigation. Under the DSA, the industry enjoys considerable discretion in how to structure its operations.

The first step is to recognise that the general risk management, in contrast to the DSA's command and control regulation side (with its detailed rules about the fairness of processes and design practices), requires a different mindset. In financial services, the same challenge exists between prudential regulation and business conduct regulation.⁶⁸ The Commission and responsible DSCs will have to undertake careful balancing of resources that they devote to each side of the DSA.⁶⁹

In practical terms, given the broadness of risk management, the industry will likely need to converge upon some solutions that compartmentalise the types of risks in order to track progress. In UK financial services, for instance, risk assessment leads to a firm-specific 'multidimensional risk picture' that relates to statutory objectives, such as

⁶⁸ Julia Black, 'The Development of Risk Based Regulation in Financial Services: Canada, the UK and Australia' (ESRC Centre for the Analysis of Risk and Regulation, LSE 2004) 27 <<https://www.lse.ac.uk/law/people/academic-staff/julia-black/Documents/black19.pdf>> accessed 5 September 2023.

⁶⁹ *ibid.*

consumer understanding, financial crime, etc.⁷⁰ These are then further developed into separate 'risks to objectives'.⁷¹ Each risk element of the firm is then scored according to each RTO, and then aggregated into an overall risk score.⁷² If any element cannot be scored due to a lack of information, the aggregate defaults into the medium/high region.⁷³

At the time of writing, the World Economic Forum had tried to come up with potential taxonomies of digital risk.⁷⁴ However, the resulting taxonomy does not map well into the categories of the DSA. It neglects risks to freedom of expression, data protection, or privacy—which are key considerations for the DSA. Moreover, with the explosion of the debate about AI-specific risks, several institutions developed notable approaches to risk management that can be transposed to the DSA. For instance, the US National Institute of Standards and Technology has developed an Artificial Intelligence Risk Management Framework that offers some interesting parallels.⁷⁵

In contrast, AlgorithmWatch, an NGO, developed a DSA-specific framework for assessing risks to media diversity.⁷⁶ Access Now, another NGO, published a general DSA risk assessment for fundamental rights.⁷⁷ Stiftung Neue Verantwortung, a think tank, developed a DSA-specific auditing framework for recommender systems.⁷⁸ Ada Lovelace Institute, another think tank, suggests methods for regulatory inspection of algorithmic systems on social media platforms.⁷⁹

Developing a DSA-specific taxonomy of risks is beyond the scope of this book. However, sub-categories of Article 34(1)(a)–(d) provide a good starting point. A potential taxonomy could break down these categories further (eg, risks to children, consumers, adults, etc) but would have to keep in mind that over-blocking, and surveillance, are two risks that are present across all the categories. Moreover, it needs to consider the primacy of illegal content as a type of risk, because the legitimacy to intervene and the ability to intervene is the strongest for these types of risks.

One of the big challenges for risk assessments will be how to treat the role of *individuals* in risk mitigation. Regulators will need to balance individual autonomy with the

⁷⁰ *ibid* 25.

⁷¹ *ibid.*

⁷² *ibid.*

⁷³ *ibid.*

⁷⁴ For the overview, Global Coalition for Digital Safety, 'Digital Safety Risk Assessment in Action: A Framework and Bank of Case Studies' (World Economic Forum 2023) <<https://www.weforum.org/reports/digital-safety-risk-assessment-in-action-a-framework-and-bank-of-case-studies/>> accessed 5 September 2023.

⁷⁵ NIST, 'AI Risk Management Framework' (*NIST Information Technology Laboratory*, 12 July 2021) <<https://www.nist.gov/itl/ai-risk-management-framework>> accessed 5 September 2023.

⁷⁶ Michelle Loi, 'Making Sense of the Digital Services Act: How to Define Platforms' Systemic Risks to Democracy' (Algorithm Watch 2023) <<https://algorithmwatch.org/en/making-sense-of-the-digital-services-act/>> accessed 5 September 2023.

⁷⁷ Eliška Pirková, 'Fundamental Rights Impact Assessments are key for effective DSA Enforcement' (Access Now, 18 September 2023) <<https://www.accessnow.org/fundamental-rights-impact-assessments-for-dsa-enforcement/>> accessed 5 September 2023.

⁷⁸ Anna-Katharina Meßmer and Martin Degeling, 'Auditing Recommender Systems' (Stiftung Neue Verantwortung 2023) <<https://www.stiftung-nv.de/de/publication/auditing-recommender-systems>> accessed 5 September 2023.

⁷⁹ Ada Lovelace Institute, *Technical Methods for Regulatory Inspection of Algorithmic Systems* (2021) <<https://www.adalovelaceinstitute.org/report/technical-methods-regulatory-inspection/>> accessed 5 September 2023.

allocation of risks to platforms. If risks are heavily centralised with platforms, this not only implies that individuals are more protected, but also that the risk mitigation measures must be mostly dictated by providers. Arguably, different individuals, including children, their parents, bystanders, content creators, or users, should be granted diverging levels of agency across the different types of risks that they encounter.

In Figure 15.2, I offer a hexagon as an illustration of how to think of risk allocation. Hexagon envisages six basic stakeholders who can be allocated risks along with VLOPs and VLOSEs: users, content creators, victims, bystanders, children, and their parents. Each of these stakeholders can exercise some level of care, and thus manage their own risks. Theoretically, there is a limit for each one of them in terms of the benefits and how much agency they can reasonably absorb in a way that is still conducive to their personal autonomy. Ideally, the Commission should try to maximise the optimal level of empowerment for each of the stakeholders by forcing companies to give them tools to manage their experience. For some stakeholders, such as children, the optimum might depend on age. For others, such as bystanders, on their type (eg, whether an NGO or an individual).

Once the optimal zone of empowerment is maximised for each stakeholder, the residual risks are absorbed by the VLOPs/VLOSEs. Empowerment effectively carves out

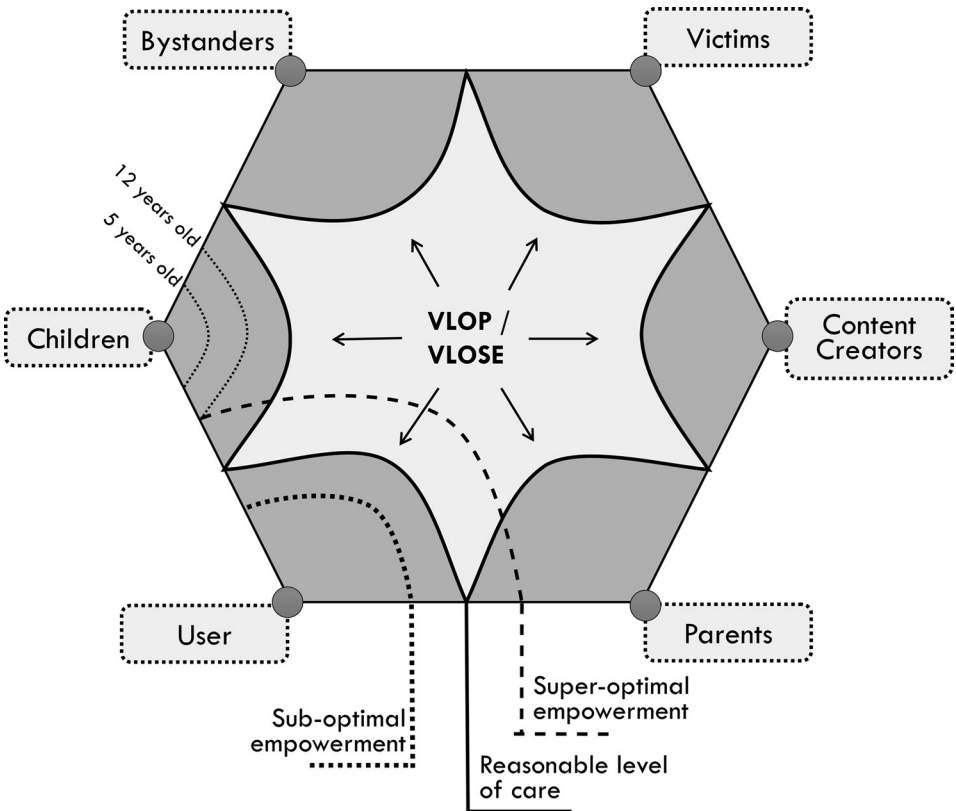


Figure 15.2 Risk distribution under risk management

some responsibility; it reallocates it from providers to individuals for the benefit of individual freedom. Because users often can only exercise as much agency as is granted to them by the design of services, they cannot be legally expected to do more than they are empowered to do.

Consider digital risks specific to children. According to existing research, children can be exposed to many types of risks online.⁸⁰ However, the occurrence of negative impact is influenced by their resilience and digital literacy.⁸¹ Only a quarter of European youth report having experienced something online that left them feeling bothered or upset.⁸² Online resilience—the ability to bounce back from online adversity—acts as a protective factor.⁸³ Through years of use, young users learn how to cope and gradually improve at adapting to future online stressors.⁸⁴ Social psychologists like Sonia Livingstone have been arguing for years that protecting young people from online risks is impossible ‘without also radically curtailing their online opportunities.’⁸⁵ The rationale that underlies this argument is the same one that explains why, in the offline environment, the design of playgrounds for children takes into account the need for children to learn. For instance, the European Committee for Standardisation’s (CEN) Child Safety Guidance states:

An essential part of the process of a child becoming an adult is the need, and desire, to explore limits and to try new experiences. Minor injuries are part of every child’s learning process and are a far more normal part of their lives than is the case for adults. This should be borne in mind when considering what levels of safety are reasonably practicable within the limits imposed by functionality and affordability. However, children require greater protection than adults against fatal or permanent injuries because they may not be capable of assessing the risks involved in potentially hazardous situations or may be too young to take responsibility.⁸⁶

The solution to the trade-off between opportunities and learning on one hand, and protection against risk on the other, is not unfamiliar to the design of the legal system. Law and economics scholars have been pointing out that legal institutions often intuitively try to prevent moral hazard—a situation where victims have reduced incentives to protect against risk because he or she is not fully exposed to the consequences of their own

⁸⁰ May O Lwin, Benjamin Li, and Rebecca P Ang, ‘Stop Bugging Me: An Examination of Adolescents’ Protection Behavior against Online Harassment’ (2012) 35(1) *Journal of Adolescence* 31.

⁸¹ Joyce Vissenberg, Leen d’Haenens, and Sonia Livingstone, ‘Digital Literacy and Online Resilience as Facilitators of Young People’s Well-Being?: A Systematic Review’ (2022) 27(2) *European Psychologist* 76.

⁸² David Smahel and others, ‘EU Kids Online 2020: Survey Results from 19 Countries’ (EU Kids Online 2020) <<https://www.eukidsonline.ch/files/Eu-kids-online-2020-international-report.pdf>> accessed 5 September 2023.

⁸³ Vissenberg, d’Haenens, and Livingstone (n 81) 2.

⁸⁴ John Coleman and Ann Hagell (eds), *Adolescence, Risk and Resilience: Against the Odds* (J Wiley & Sons Ltd 2007).

⁸⁵ Sonia Livingstone and Ellen Helsper, ‘Balancing Opportunities and Risks in Teenagers’ Use of the Internet: The Role of Online Skills and Internet Self-Efficacy’ (2010) 12(2) *New Media & Society* 309.

⁸⁶ European Committee for Standardization (CEN), ‘Child Safety – Guidance for Its Inclusion in Standards 2009’ (CENELEC 2009) CEN/CENELEC Guide 14 <<https://www.cencenelec.eu/media/Guides/CEN-CLC/cencclguide14.pdf>> accessed 6 September 2023.

actions. As pointed out by Tom Baker, the overarching question this poses across the legal system is: to what extent are those who suffer responsible for their condition?⁸⁷

For instance, European tort law accepts the principle of contributory negligence. According to Article 8.1.1 of Principles of the European Tort Law (PETL): ‘Liability can be excluded or reduced to such extent as is considered just having regard to the victim’s contributory fault and to any other matters which would be relevant to establish or reduce the liability of the victim if he were the tortfeasor.’⁸⁸ Thus, where a victim could act to reduce the damage, it should have done so; otherwise, the compensation owed can be reduced.

The argument for optimal precautions, as illustrated by the example of children, extends beyond the justification on the basis of avoidance of moral hazard. Taking risks is often part of learning and improves individual resilience. The legal system is dosing risks all the time. If speech is kept lawful, it is not only a constitutional imperative that the authorities do not curtail it specifically beyond parliamentary mandates, but also an expression of respect for people’s freedoms and autonomy.

As explained by Recital 40 DSA:

[Due diligence] obligations should aim in particular to guarantee different public policy objectives such as the safety and trust of the recipients of the service, including consumers, minors and users at particular risk of being subject to hate speech, sexual harassment or other discriminatory actions, the protection of relevant fundamental rights enshrined in the Charter, *the meaningful accountability of those providers and the empowerment of recipients and other affected parties*, whilst facilitating the necessary oversight by competent authorities.

Thus, ‘meaningful accountability of providers’ and ‘the empowerment of recipients and other affected parties’ are not presented as two opposites. Accountability answers the calls of individuals for more protection. However, this does not mean that as part of the programme of protection, individuals should not take some responsibility. Pre-DISA, such responsibility was often denied to individuals because it conflicted with companies’ profit motives; post-DISA, it should not be denied due to overzealous enforcement. The DSA aims to establish a digital environment worthy of people’s trust. Thus, they must be also trusted to decide whenever possible. To make sure that we understand how stakeholders experience their newly gained responsibilities, the regulators, together with companies, could periodically run longitudinal standardised surveys of the stakeholders’ views on matters such as trust, safety, and their experiences across the entire ecosystem of VLOPs/VLOSEs.

⁸⁷ Tom Baker, ‘On the Genealogy of Moral Hazard’ (1996) 75(2) Texas Law Review 237.

⁸⁸ European Group on Tort Law, ‘Principles of European Tort Law (PETL)’ <<http://www.egtl.org/PETLEnglish.html>> accessed 4 September 2023.

Transparency

16.1 Introduction	347	16.3.1 Annual reports on content moderation (Article 15)	359
16.2 Access to Data of VLOPs/VLOSEs (Article 40)	349	16.3.2 Advanced reporting for online platforms and search engines (Article 24)	363
16.2.1 Privileged access to data for vetted researchers (Article 40(4)–(11))	350	16.3.3 VLOPs' and VLOSEs' content moderation reports (Article 42)	365
16.2.2 Access to public data (Article 40(12))	355	16.3.4 Transparency of other actors	366
16.2.3 Access to other data enabled by the DSA	359	16.4 Conclusion	367
16.3 Transparency Reports	359		

16.1 Introduction

Light has disinfectant properties. Although it might not be the best disinfectant for everything, its power is universal once cast. The same can be said about transparency. While the Digital Services Act's (DSA) transparency rules are framed as obligations observing the business of platforms, they are not actually about platforms. They are about *us*—the individual users of those platforms. When people voice their views in pubs or public squares, anyone can observe. If they do so in pseudo-anonymous chatrooms, it is less likely. Such data is suddenly *proprietary*, as it is amassed by the digital gatekeepers that operate chatrooms, newsfeeds, social media, and other services. Without transparency, we are in the dark about what is happening within our societies.

Consider the recent United States (US) lawsuit initiated by X (formerly Twitter) against the Center for Countering Digital Hate (CCDH), a non-profit organisation that tracks hate speech on social platforms.¹ X complains about researchers scraping its proprietary data to study societal risks. Its real purpose is to shut down any independent monitoring of its services to be able to woo back its concerned advertisers. Amazon's legal case against its designation as a very large online platform (VLOP) was potentially motivated by the possibility of temporarily suspending the obligation to create advertising archives.² There is no doubt that meaningful transparency undermines some of the practices that the companies would engage in otherwise. If companies are allowed

¹ *X Corp v Center for Countering Digital Hate Inc*, No 3:23-cv-03836 (ND Cal)

² Case T-367/23 R *Amazon Services v Commission* ECLI:EU:T:2023:589.

to protect their commercial interests via data ownership aggressively, a lot of important research can be put at risk, and everyone will be in the dark about what is happening in the digital environment.³

To protect research, the DSA must think about the data access questions extraterritorially. If global non-governmental organisations (NGOs) can be sued for their DSA-endorsed analytical work outside of Europe, researchers might be discouraged from undertaking legally risky evaluations of how digital services pose risks to society at large. While the DSA transparency reports are a step forward, they do not provide the granular data needed to assess product-specific problems. Transparency reports only provide a rear-view mirror of what has transpired in society. To see forward, researchers' access to data is key.

Prior to the DSA, civil society and providers tended to negotiate the scope of transparency. The Santa Clara Principles were the most influential.⁴ The principles largely envisaged what the DSA now delivers as binding rules. Its success is reflected in the fact that all major US platforms today issue some form of transparency reports.⁵ Apart from the Santa Clara Principles, some other transparency tools, such as Harvard's Lumen Database,⁶ directly inspired the European Commission in its DSA proposal.⁷ Thus, undoubtedly, the DSA builds upon many years of voluntary disclosure and even attempted regulation in this area. For instance, the German hate speech law (NetzDG) that preceded the DSA also mandated certain transparency reporting, although with mixed results as to its actual usefulness, partly due to reliance on idiosyncratic methodologies.⁸

The early European legislation tended to omit rules on transparency. Only recently have the newly introduced Terrorist Content Regulation (TCR) (2021) and Child Sexual Abuse Regulation (2021) envisaged some transparency reporting by relevant actors.⁹ The lack of transparency was sometimes remedied by voluntary reporting by companies, such as when Google published reports about the newly created right to be delisted from the search results.¹⁰

³ Vittoria Elliott, 'How X is Suing Its Way Out of Accountability' *Wired* (15 August 2023) <<https://www.wired.com/story/twitter-x-cdh-lawsuit-data-crackdown/>> accessed Joshua A Tucker and Nathaniel Persily (eds), *Social Media and Democracy: The State of the Field, Prospects for Reform* (CUP 2020).⁵ September 2023.

⁴ 'Santa Clara Principles on Transparency and Accountability in Content Moderation' (*Santa Clara Principles*) <<https://santaclaraprinciples.org>> accessed 3 September 2023.

⁵ For the pre-DSA situation, Daphne Keller and Paddy Leerssen, 'Facts and Where to Find Them: Empirical Research on Internet Platforms and Content Moderation' in

⁶ 'The Lumen Database' (*Lumen Database*) <www.lumendatabase.org> accessed 3 September 2023.

⁷ Commission, 'Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and Amending Directive 2000/31/EC' COM(2020) 825 final, art 17(5): ('Online platforms shall ensure that the decisions, referred to in paragraph 4, are not solely taken on the basis of automated means.')

⁸ Heidi Tworek and Paddy Leerssen, 'An Analysis of Germany's NetzDG Law' [2019] Working paper of the Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression <https://www.ivir.nl/publicaties/download/NetzDG_Tworek_Leerssen_April_2019.pdf> accessed 6 September 2023.

⁹ Arts 7 TCR, and 8–9 European Parliament and Council Regulation (EU) 2021/1232 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse [2002] OJ L274/41 (Child Sexual Abuse Regulation).

¹⁰ Theo Bertram and others, 'Five Years of the Right to be Forgotten', *Proceedings of the Conference on Computer and Communications Security* (2019).

Going forward, the DSA will likely transfer reporting behaviour into one of the general safeguards of any delegated enforcement in the digital environment. The reason is that as a horizontal measure, it applies in all areas of the law where illegality leads to content moderation. Thus, even if specific areas do not think of transparency, the DSA serves as a back-up set of default safeguards.¹¹

The DSA transparency obligations create important data points for scrutiny regarding content moderation and risk mitigation practices by digital service providers. In their totality, they unveil many parts of previously impenetrable services for outsiders. The DSA increases the obligations incrementally according to a services' categorisation. The lowest level of universal transparency obligations is expected of all hosting, caching, and mere conduit services. The next level of advanced obligations is expected from hosting services that qualify as online platforms. Finally, VLOPs and very large online search engines (VLOSEs) are subject to special transparency obligations.

16.2 Access to Data of VLOPs/VLOSEs (Article 40)

Researchers are given an important role in the DSA. They help identify what counts as a risk. In effect, they formulate the agenda for the regulators and providers of digital services. They also monitor and assess those risks, their causes, and contributing factors, and suggest ways to mitigate them. Their suggestions are directly relevant to providers' compliance with the DSA.

To be able to do so, they get special access to data under the DSA, which cannot be easily refused. The DSA has changed the norm: now researchers pick their projects and platforms, not the other way around. Once their research demonstrates evidence of particular risks and their causes or suggests a way forward, it cannot be ignored (by providers or regulators) either. However, researchers need time and money to do this properly. Moreover, researchers act as a check on the abuse of power by the regulators. They hold regulators' legal demands and actions to account in line with what science says, not what politics finds convenient.

Unlike in other sectors, under the DSA, the relevant risks are to individuals, communities, and society at large—basically, everything we cherish. Starting from scratch can overwhelm and disorient regulators as to what the enforcement priorities should

¹¹ At the time of writing, transparency is hotly debated in other jurisdictions, such as the US. For instance, the 'Platform Transparency and Accountability Act' is a bipartisan bill that is currently being discussed. See Laura Edelson, 'Platform Transparency Legislation: The Whos, Whats and Hows' (*Lawfare*, 29 April 2022) <www.lawfareblog.com/platform-transparency-legislation-whos-whats-and-hows> accessed 6 September 2023. Many state and federal bills are trying to introduce some form of transparency to content moderation or other practices of online platforms. The US Supreme Court might soon hear a case about the permissible scope of general and individual transparency rules that can be imposed on platforms in the context of content moderation in several pending cases concerning two state bills (*NetChoice & CCIA v Paxton* No 1:21-cv-00840 (WD Tex) (1 October 2021) and *NetChoice & CCIA v Moody* No 4:21-cv-00220 (ND Fla) (30 June 2021)). It is likely that at least some of the DSA-style rules will be seen as unconstitutional if the Court is taken up, see Daphne Keller, 'Platform Transparency and the First Amendment' [2023] Stanford Cyber Policy Center <<https://www.ssrn.com/abstract=4377578>> accessed 6 September 2023.

be and how to deal with them. And this is where researchers are key. Researchers' tool-kits and literature reviews¹² can become incredibly important.

Researchers have two broad data access tools: (a) project-based access to data held by providers (privileged access to data), and (b) general access to public data held by providers. In addition, regulators have their own routes for data access to assess the DSA compliance. Table 16.1 depicts the options.

The DSA does not explicitly limit access to either type of data to only European researchers. However, because of the requirement to assure data protection, security, and confidentiality, the data flows from outside of the European Union (EU) can be complicated by the General Data Protection Regulation (GDPR).¹³

16.2.1 Privileged access to data for vetted researchers (Article 40(4)–(11))

For privileged access to data, the DSA creates a system of vetting researchers who are granted project-based access to data (Article 40(8)). The access requests are issued by the Digital Services Coordinators (DSCs) of the establishment upon a duly substantiated application from the researchers.¹⁴ Given that many VLOPs and VLOSEs are established in Ireland, this will be often the Irish regulator.¹⁵

To qualify as a vetted researcher, the persons must be:

- a) affiliated with a research organisation,¹⁶ including an NGO;¹⁷
- b) independent from commercial interests;
- c) disclose any relevant funding;
- d) have capabilities to assure data security, confidentiality, and personal data protection;

¹² For an example of a toolkit for disinformation, see Anastasia Kozyreva and others, 'Toolbox of Interventions Against Online Misinformation and Manipulation' (16 December 2022) <<https://interventiontoolbox.mpib-berlin.mpg.de/index.html>> accessed 6 September 2023.

¹³ On the latest situation, see Robert Maddox and others, 'Take Three: New European Adequacy Decision Gives Green Light to EU-U.S. Data Protection Framework' (*Debevoise Data Blog*, 31 July 2023) <<https://www.debevoisedatablog.com/2023/07/31/take-three-new-european-adequacy-decision-gives-green-light-to-eu-u-s-data-protection-framework/>> accessed 6 September 2023.

¹⁴ The application can be also made in the country of the researcher's institution but it will be transmitted to the DSC of the establishment anyway, see the DSA, art 40(9).

¹⁵ Mathias Vermeulen, 'Researcher Access to Platform Data: European Developments' (2022) 1(4) *Journal of Online Trust and Safety* 4.

¹⁶ Art 40(8)(a) together with art 2, point 1 Copyright in a Digital Single Market (CDSM) Directive: "research organisation" means a university, including its libraries, a research institute or any other entity, the primary goal of which is to conduct scientific research or to carry out educational activities involving also the conduct of scientific research: (a) on a not-for-profit basis or by reinvesting all the profits in its scientific research; or (b) pursuant to a public interest mission recognised by a Member State; in such a way that the access to the results generated by such scientific research cannot be enjoyed on a preferential basis by an undertaking that exercises a decisive influence upon such organisation;

¹⁷ Rec 97 seems to interpret the definition for the purposes of the DSA as allowing the NGOs to qualify as research organisations: 'a research organisation within the meaning of Article 2 of Directive (EU) 2019/790, which may include, for the purpose of this Regulation, civil society organisations that are conducting scientific research with the primary goal of supporting their public interest mission.'

Table 16.1 Types of data access

Article 40 DSA	Privileged access to data (Art 40(4)–(11))	Public data (Article 40(12))	Regulator's access (Art 40(1)–(3))
Beneficiaries	Vetted researchers	Any 'researchers'	DSA authorities
Sources of data	VLOPs and VLOSEs	VLOPs and VLOSEs	VLOPs and VLOSEs
Flexibility of access	Project-based	General-purpose access	Necessity for regulators
Speed of access	Slower (in months)	Faster	Faster
Eligible purposes	(1) detection, identification and understanding of systemic risks in the EU; (2) assessment of adequacy, efficiency and impacts of risk mitigation measures	detection, identification and understanding of systemic risks in the EU	Monitoring and assessment of compliance with any DSA obligation
Required affiliation	Affiliation with an entity anywhere in the world devoted to scientific research that operates: (a) on a not-for-profit basis or reinvests all the profits in its research; or (b) pursuant to a public interest mission recognised by an MS	Researchers from anywhere in the world, including those working for non-profits, charities, think tanks, consumer groups, journalists, etc.	Digital Services Coordinator of provider's establishment, or the European Commission
Procedure to obtain access	DSC approval process for projects	None	Reasoned request
Conditions for use of data in teams	Use within the scope of the approved project and among its members	Use for any own research purpose, and sharing with any other eligible researchers	Use to monitor and assess compliance within the regulator's powers
Explicit funding, access and publication requirements	GDPR, data security and confidentiality safeguards; independence from commercial interests; funding disclosure; free of charge publication;	GDPR, data security and confidentiality safeguards; independence from commercial interests; funding disclosure;	Balancing the regulatory needs with the rights of others

- e) explain how the data access is necessary and proportionate given their methodology and research questions;
- f) fulfil at least one of the DSA's accepted purposes (detection, identification, and understanding of systemic risks or assessment of the risk mitigation measures); and
- g) committed to making the research results publicly available free of charge.

The access to researchers can be granted only 'for the sole purpose of conducting research that contributes to the detection, identification and understanding of systemic

risks in the Union', including 'the assessment of the adequacy, efficiency and impacts of the risk mitigation measures' (Article 40(4)). Vermeulen referred to these two functions of researchers as 'pathfinders' and 'quasi-auditors'.¹⁸

Given the scope of the DSA's covered threats, the provision has a much broader impact than offering only an opportunity to conduct some parallel external audits. It invites scientists to come and scrutinise the most significant platforms to better understand the systemic risks and how to effectively approach them. The provision is a giant subsidy to social sciences which otherwise have to collect their own data, and find research subjects. While the scope of access to data is limited to the DSA's regulatory remit, it is clear that through understanding risks to individuals, communities, and society at large, we also advance our understanding of people in their social interactions. The close linkage to regulatory purposes also means that the research must be limited to issues within the EU. It is thus not possible to only gain access to study risks specific to the Global South. However, the issues studied can be universally applicable, and the insights gained are also useful for other jurisdictions. It should also be possible, for instance, to use non-European settings as control groups for the EU-focused studies. Finally, the Codes of Conduct can extend the reach of the data access provisions and 'non-EU' issues.

With the privileged access, the hope is that researchers eventually formulate an agenda for the risk-assessments, methods of capturing various risks, and reflect upon various ways to mitigate them. Article 40 is thus designed as a crucial accountability tool because it makes providers accountable not only to the state authorities but also to science. While the authorities might be temporarily deaf to scientific evidence, providers should listen to it very carefully for the sake of their own compliance; science and evidence, after all, is also a check on authorities and auditors.

The access to data can take various forms. Recital 97 highlights that data access requests could cover questions like 'the number of views or, where relevant, other types of access to content by recipients of the service prior to its removal by the providers'. The DSA does not limit the compliance only to the type of data that the platform already has in a ready-made dataset. Thus, a certain amount of data collection and preparation is implied in the DSA's data access regime.

Each data access request is submitted by researchers to the DSCs. They can either directly submit to the DSC of the provider's establishment or the DSC of their affiliation. In either case, the DSC of the provider's establishment decides about the request. The DSC then forwards each data access request to providers who can propose to modify it within 15 days. However, they can propose amendments only on two grounds: (a) if they 'do not have access to the data', or (b) if 'giving access would lead to significant vulnerabilities in their security or the protection of confidential information, in particular trade secrets' (Article 40(5)). In both situations, they must be constructive and propose alternative means of access which the researchers could use in

¹⁸ Vermeulen (n 15) 3.

their projects. Ultimately, the DSC of the establishment decides whether to modify the access request or not.

For the ground of modification under Article 40(5)(b) regarding confidential information, the compromise is that while access is allowed, the researchers are required to observe applicable laws, including trade secrecy and data protection laws, when reporting their results. However, these laws often include considerations of legitimate research interests in their statutory designs. As such, the trade secrecy defence cannot be relied upon to trump legitimate research projects. Indeed, Recital 97 also makes it clear that purely ‘commercial interests of providers should not lead to a refusal to provide access to data necessary for the specific research objective’. The research of the relevant risks is thus given priority over absolute commercial secrecy.¹⁹

Moreover, access to data according to Article 40(4) does not immediately mean that trade secrecy rights are endangered. Trade secrecy does not mean no one outside the company can see the information. If this were true, licensing agreements with business partners would be impossible without destroying secrecy. Trade secret rights are preserved as long as ‘it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret’.²⁰ In practice, this usually means asking such parties to sign non-disclosure agreements.

Thus, to even have a conversation about rejection based on Article 40(5)(b), VLOPs/VLOSEs must explain why the non-disclosure agreements are not sufficient to solve the risk of public disclosure. Only if this is convincing can the provision be relied upon. As a result, it should be expected that VLOPs/VLOSEs might require researchers to sign non-disclosure agreements regarding certain aspects to preserve their protection of trade secrets. Such agreements are, however, very sensitive because they can endanger academic integrity. The regulators, including the European Commission, should try to standardise such agreements to prevent VLOPs/VLOSEs from using their bargaining position to impose undue conditions. One can borrow from existing practices in the area of court-appointed experts (eg in competition cases) who are often asked to receive sensitive information from firms to produce their assessments. However, the DSCs should be aware that protection claims can sometimes be overstated. The companies’ reflex is to try to protect factual secrecy over algorithms, data or components; however, often those components have little chance to be also protected legally by trade secrecy laws.²¹

If the vetted researchers fail to live up to the above requirements of trust, the DSC of the provider’s establishment can terminate their status (Article 40(10)). The European

¹⁹ For a comprehensive report on data access under the DSA, see Laura Edelson, Inge Graef, and Filippo Lancieri, ‘Access to Data and Algorithms: For an Effective DMA and DSA Implementation’ (CERRE 2023) <<https://cerre.eu/publications/access-to-data-and-algorithms-for-an-effective-dma-and-dsa-implementation/>> accessed 6 September 2023.

²⁰ European Parliament and Council Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use, and disclosure [2016] OJ L 157/1, art 2(1)(c).

²¹ See Sharon K Sandeen and Tanya Aplin, ‘Trade Secrecy, Factual Secrecy and the Hype Surrounding AI’ in Ryan Abbott (ed), *Research Handbook on Intellectual Property and Artificial Intelligence* (Edward Elgar (forthcoming)) <<https://papers.ssrn.com/abstract=3929928>> accessed 6 September 2023.

Commission and the Board will have been collecting the names of vetted researchers and descriptions of their projects, including those whose status was previously terminated.

The European Commission is also empowered to adopt a delegated act within five years of the DSA's entry into the force (Article 87). Such delegated acts can further specify technical conditions addressing access to data and addressing important compliance questions (Article 40(13)). The data access rules also form parts of the Codes of Conduct, such as the Code of Conduct on Disinformation, which have regulatory relevance too.²²

The clear disadvantage of privileged access to vetted researchers is its limitation to project-based investigations. Without prior access to data, it might be hard to properly formulate research projects. The risk is that the vetting process is conceived too formalistically and pushes researchers to construe very narrow research questions, thus not allowing any changes in the research trajectory. If the researchers are forced to resubmit numerous requests to reflect the inherently iterative character of the research, it can not only slow down the researchers but also discourage them from using the tool. Thus, the delegated acts must carefully calibrate the requirements to avoid being too prescriptive. The DSCs might borrow some procedures from the elaborate European grants systems that allow more risk-taking by the researchers, such as European Research Council grants.

Any disputes about the scope of Article 40(4) requests are going to be losing battles for researchers. If VLOPs/VLOSEs start seeking judicial review of the data access grants, the system can be slowed down to the point of complete uselessness. To avoid this, amicable and fast resolution of disputes should be preferred. Article 40(13) allows the Commission to create 'independent advisory mechanisms in support of sharing of data'. This mechanism could also help with the informal resolution of disputes. It should be composed of specialised lawyers, ethicists, and leading social scientists, including data scientists, who can provide amicable resolution of any disputes by providing advisory opinions. The Commission might encourage its use in the delegated act by allowing parties or regulators to initiate such opinions in controversial or difficult cases before proceeding to the final decision, according to Article 40(8).

Article 40(13) empowers the European Commission to specify 'technical conditions' regarding the privileged data access by vetted researchers, including on issues such as 'relevant objective indicators, procedures and, where necessary, independent advisory mechanisms in support of sharing of data'. Thus, the DSA foresees the emergence of additional structures of advisory mechanisms that could help the DSCs when assessing research projects, including compliance with data protection, security, and confidentiality.

The Achilles heel of researchers as agents of public interest lies in funding their work. The researchers engaging in such data-intensive projects need money to conduct them properly and independently. If the only funding available to do research comes from

²² For more detail, see Vermeulen (n 15).

the industry, even remotely, we have a problem. European academia needs specific grants for researchers who want to use the data opened up by the DSA. However, the financial support must be equally independent of the authorities that act as regulators. Researchers cannot act as a check on the abuse of state power exercised by regulators if they also need funding from the same authorities.

Researchers also play another role in the DSA's design. The more robust their evidence, the less need for regulators to demand data access. Because digital platforms store a lot of sensitive information about individuals and their mutual interactions, keeping the state from accessing such data protects individuals' privacy. This is another reminder of why digital services regulation cannot employ the same approach to data handling that regulators take when dealing with chemicals or food. There, the key consideration is trade secrecy. With online platforms, it is user privacy, data protection, and freedom of expression. The DSA's design empowers researchers to reduce the need for state powers to exercise as close oversight directly as is customary in other areas. This is not only a result of the resource constraints of authorities, but also of the sensitive nature of the data and risks being studied.

16.2.2 Access to public data (Article 40(12))

To complement the privileged access tool, the DSA also considers the role of publicly available data that is already often mined and studied by researchers. This data already disclosed to the public by platforms and their users is usually accessible through various interfaces. The provision was inspired by Crowdtangle,²³ a tool that independently tracks how user-generated content spreads around the web. Such data aggregation tools often serve various stakeholders enforcing their rights or by providing insights into how content travels from one service to another. For researchers, the tool helps to aggregate what is going on in the digital public sphere, such as on social media, thus providing a kind of real-time pulse of the web.²⁴

Article 40(12) foresees access to such publicly accessible data, which often includes real-time data from social media or video-sharing platforms. The provision grants access to a broader set of 'researchers' than those eligible to become 'vetted'. Recital 98 explains the provision as follows:

In addition, where data is publicly accessible, such providers should not prevent researchers meeting an appropriate subset of criteria from using this data for research purposes that contribute to the detection, identification and understanding of systemic risks. They should provide access to such researchers including, where technically possible, in real-time, to the publicly accessible data, for example on aggregated

²³ *ibid* 5.

²⁴ Casey Newton, 'Facebook Buys CrowdTangle, the Tool Publishers Use to Win the Internet' *The Verge* (11 November 2016) <<https://www.theverge.com/2016/11/11/13594338/facebook-acquires-crowdtangle>> accessed 6 September 2023.

interactions with content from public pages, public groups, or public figures, including impression and engagement data such as the number of reactions, shares, comments from recipients of the service.

The goal is thus clearly to extend the scope of access to data provisions to researchers who cannot be become vetted for specific research projects but who build or use real-time tools from the already publicly accessible data, such as feeds of social networks. While Article 40(12) is worded as a 'shall' provision, the recital seems to emphasise mostly the defensive dimension, ie that providers may not shut down or obstruct such analytical tools. Article 40(12) does not seem strong enough to force the companies to build such a tool for the research community. However, if advertisers already benefit from some such tools, Article 40(12) would seem strong enough to ask providers to extend such tools to researchers. In practice, where data is publicly accessible, researchers can build their own tools to scrape and analyse the content. However, doing so might be very expensive; thus, ready-made tools others provide are crucial. Providers often try to impose technical constraints on scrapping tools operated by researchers or other companies or use legal threats based on intellectual property rights to stop them.

Article 40(12) acts as a *sword* and a *shield*. As a shield, it provides a legal defence to unjustified attempts to shut down access because it acts as a *lex specialis* to the rights of providers.²⁵ As a sword, it provides researchers with a claim against obstructing access to publicly available data.

The use as a shield is important for any litigation that providers might initiate against researchers, such as on the basis of violations of *sui generis* database protection rights, copyright law, technical protection measures, unfair competition law or contract law.²⁶ Article 40(12) of the DSA here goes beyond Articles 3–4 of the Copyright in the Single Digital Market (CDSM) Directive that equally permits some forms of data mining, including for research purposes.²⁷ Any litigation trying to shut down these activities or tools is pre-empted by the provision, as long as its conditions are met. Article 40(12) thus acts as a safe harbour against other areas of law.

The use as a sword is crucial when providers use technical restrictions, such as blocking Internet Protocol (IP) addresses or reliance on captchas, that are clearly meant to frustrate access by researchers. It allows them to rely on the DSA to lift technical restrictions that are seen as illegitimate obstacles to data access, or at least to obtain special 'scraping exceptions' from these technical restrictions.

²⁵ A similar analogy is presented by Paddy Leerssen, 'Seeing What Others Are Seeing: Studies in the Regulation of Transparency for Social Media Recommender Systems' (PhD thesis, University of Amsterdam 2023) <<https://pure.uva.nl/ws/files/125112610/Thesis.pdf>> accessed 6 September 2023.

²⁶ See Martin Husovec, 'The End of (Meta) Search Engines in Europe?' (2014) 14(1) *Chicago-Kent Journal of Intellectual Property* 145. For after the change in case law, see Estelle Derclaye and Martin Husovec, 'Sui Generis Database Protection 2.0: Judicial and Legislative Reforms' [2021] *European Intellectual Property Review* (Forthcoming) <<https://papers.ssrn.com/abstract=3964943>> accessed 6 September 2023.

²⁷ See generally, Thomas Margoni and Martin Kretschmer, 'A Deeper Look into the EU Text and Data Mining Exceptions: Harmonisation, Data Ownership, and the Future of Technology' (2022) 71(8) *GRUR International* 685.

The eligible persons building or using the tools must be ‘researchers’ who use the data solely for studies that contribute to the detection, identification and understanding of systemic risks in the Union. Article 40(12) does not address how these researchers can further provide access to others. Presumably, any researcher could invoke the provision for access to data that is provided to them by other researchers. However, potential access by citizens is probably not possible. Article 40(12) incentivises researchers to build and maintain the tool only for other researchers. Thus, the public can learn from using such tools only through research publications.

The privileged access is limited to those eligible to become vetted researchers. The access to public data allows access by a broader set of researchers. Who exactly are such researchers under Article 40(12) is not further specified anywhere in the DSA. Thus, they can include persons who are *not* affiliated with a ‘research organisation’ within the meaning of the CDSM Directive.²⁸ This creates legal risks for any unaffiliated researchers, such as NGOs, who might decide to maintain or build a tool with access to public data of platforms. The European Commission should thus further clarify the concept.

The reliance on application programming interfaces (APIs) offered by online platforms has not been without problems.²⁹ The tools have their internal limitations and have been increasingly either shut down or made subject to high fees. The online platforms have been found to restrict access to APIs to selected researchers.³⁰ Some academics have also accused online platforms of potentially manipulating the data in APIs, and argued extensively that scraping techniques are necessary to identify potential instances of manipulation.³¹

Thus, while API access based on Article 40(12) should be further developed through Codes of Conduct, the researcher-initiated scraping should remain central. Scraping provides alternative access to public data regardless of what APIs or other tools are offered by providers. It is a technique important for the validation of any API-provided data sets. Moreover, scraping puts pressure on firms to create properly functioning APIs, and facilitates researchers explore the relevant risks before they formulate their requests pursuant to Article 40(4).

This fact is also underscored by the General Product Safety Regulation, which states that online marketplaces must ‘allow the scraping of [their platform] data only for product safety purposes based on the identification parameters provided by the requesting market surveillance authorities,’ including by removing the technical obstacles.³²

²⁸ Art 40(8)(a) DSA, read together with art 2(1) CDSM Directive.

²⁹ Axel Bruns, ‘After the “APocalypse”: Social Media Platforms and their Fight against Critical Scholarly Research’ (2019) 22(11) *Information, Communication & Society* 1544.

³⁰ See Nicolas Kayser-Bril, ‘AlgorithmWatch Forced to Shut down Instagram Monitoring Project after Threats from Facebook’ (*AlgorithmWatch*) <<https://algorithmwatch.org/en/instagram-research-shut-down-by-facebook/>> accessed 16 September 2023.

³¹ Jade Garcia Bourrée and others, ‘On the Relevance of APIs Facing Fairwashed Audits’ [2023] arXiv2305.13883 [cs.LG] 1.

³² European Parliament and Council Regulation (EU) 2023/988 on general product safety, amending Regulation (EU) No 1025/2012 and Directive (EU) 2020/1828, and repealing Directive 2001/95/EC and Directive 87/357/EEC [2023] OJ L135/1, art 22(12)(i) (General Product Safety Regulation).

The European Commission should encourage the research in the following ways:

- The delegated act should clarify that Article 40(12) is the backstop for any qualified researcher and that it covers scraping and highlights its exploratory value for Article 40(4).
- The European regulators should develop a detailed safe harbour for scraping according to Article 40(12), which specifies under what conditions scraping is manifestly legal and cannot be legitimately opposed by VLOPs and VLOSEs. This would not serve as an exhaustive statement of the law but would make IRB approvals much easier. The safe harbour could be adopted as an EC Guidance or a Code of Conduct.

The expanded scope of beneficiaries is particularly relevant to non-profit organisations, consumer groups, charities, investigative journalists, security researchers, etc. However, even researchers are subject to the requirement for their ‘independence from commercial interests’. This term, which can be further specified by the delegated act, limits both types of data access. The hint that this term should be construed narrowly is also clear from the fact that the broader set of researchers, according to Article 40(12), do not have to publish their results in freely accessible publications.³³ Thus, a journalist who use the tools to write an investigative story for their media outlet that is subject to a paywall would seem to still qualify. However, given that media owners are increasingly in legal rows with platforms about the licensing of their content, such journalists could also be seen as not independent from commercial interests.

In contrast to privileged access, access to public data remains a faster, more horizontal but less in-depth scrutiny tool. The main challenge here is to create tools which decrease the costs for researchers to access the data. Clearly, not every researcher has the skills and resources to set up their own tools or even comply with data protection, security, and confidentiality requirements. There is hope that universities will build specific infrastructure that researchers can use similarly to libraries that facilitate access to books and databanks. The same approach can be taken by consortia of investigative journalists, non-profit organisations, and think tanks. There is thus room for collaboration on building some intermediaries who set up tools to be used by different eligible individual researchers.

Finally, the obvious unresolved issue concerns data protection laws and how they will shape access to data by researchers. Recital 97 reminds us of the GDPR’s applicability and that ‘providers should ensure appropriate access for researchers, including, where necessary, by taking technical protections such as through data vaults’. Similarly, Recital 98 says that ‘providers and researchers should pay particular attention to the protection of personal data, and ensure that any processing of personal data complies with Regulation (EU) 2016/679. Providers should anonymise or pseudonymise personal data except in those cases that would render impossible the research purpose

³³ Art 40(12) drops the requirement art 40(8)(g).

pursued'. In other words, the DSA does not resolve exactly how data protection interests shall be resolved in practice. The data protection authorities will thus have to develop approaches that do not compromise the goals behind Article 40 which sufficiently safeguard the data protection rights of affected individuals.

16.2.3 Access to other data enabled by the DSA

It should be emphasised that data access is not limited to Article 40 DSA. Various transparency obligations discussed in this chapter further increase the scope of public data about regulated services. Transparency reports (Articles 15, 24, and 42) include rich and valuable information about content moderation decisions and the internal workings of companies running them. Archives for advertising (Article 39) track information about advertisers, their commercial communications, the duration of individual campaigns, and their audience, including ways in which they are targeted by advertisers. The fair design requirements, such as codification of content moderation rules, including notification of significant changes (Article 14), central collection of statement of reasons for each content moderation decision (Article 24(5)), or disclosure of the main parameters in the recommender systems, further improve the data collection capabilities of researchers. The auditing requirements also publish reports concerning how VLOPs and VLOSEs identify and mitigate risks. The DSA often anticipates researchers and their bots when upgrading obligations of various kinds to 'machine-readable'.³⁴

16.3 Transparency Reports

The transparency obligations in the DSA deal with three basic areas: content moderation, advertising, and user base. Content moderation is at the centre of transparency obligations. Advertising and user-base information are relevant for players who potentially qualify as VLOPs or VLOSEs.

16.3.1 Annual reports on content moderation (Article 15)

All intermediary service providers must issue annual reports that 'engage in any content moderation'. The DSA, however, uniquely exempts micro and small enterprises *if* their services do not qualify as VLOPs or VLOSEs.³⁵ It equally exempts those services which did not engage in any content moderation, both on its own initiative, and

³⁴ Arts 14(1), 14(5), 15(1), 22(5), 24(5), 31(3), and 55(1).

³⁵ Commission Recommendation of 6 May 2003 concerning the definition of micro, small, and medium-sized enterprises [2003] OJ L124/36.

Table 16.2 Universal transparency reports (Article 15 DSA)

	Content moderation activity	Mere conduits	Caching	Hosting
Universal obligations (Article 15)	Any orders from the EU Member States (Art 15(1)(a))	(1) absolute number of orders, categorised by: (2) type of illegal content, (3) issuing Member State, (4) median time for handling, and (5) taking the action		
	Notices sent by third parties (Art 15(1)(b))	Voluntary use and reporting		(1) absolute number of notices, (2) divided per types of illegal content, (3) absolute numbers for trusted flaggers, (4) actions taken based on ToS or law, (5) absolute number of automated decisions, and (6) median time for taking the action
	Any content moderation based on own investigations (Art 15(1)(c))	(1) absolute number of relevant restrictions, categorised by: (2) each restriction type, (3) detection method, (4) type of illegal content, (5) basis in ToS or law, and providing (5) other information concerning automated tools, training, and assistance to content moderation staff		
	Any internal appeals of content moderation decisions (Art 15(1)(d))	<i>At least:</i> (1) absolute number of internal appeals, (2) median time for taking the action, (3) absolute number of reversals; <i>for online platforms only:</i> categorisation by (4) the restriction type, and (5) basis in ToS or law		
	Any use of automation for content moderation (Art 15(1)(e))	<i>At least:</i> (1) qualitative description, (2) specification of the precise purposes, (3) indicators of the accuracy, (4) error rates and (5) any safeguards applied.		
	Any orders from outside the EU	No, voluntary reporting (however, if they affect accessibility in the EU, they should be disclosed under their own investigations).		

because it had not receive any requests to do so. Thus, an internet access provider, or messaging service that does not store any messages, could avoid issuing reports only if it received no requests to block websites or notices concerning such websites.³⁶ Engaging in content moderation, therefore, means both refraining from moderating content and also not being exposed to any requests to conduct content moderation by others. All the reports must be made publicly available in a machine-readable and easily accessible format on an annual basis. Given that content moderation not only relates to individual content but also user accounts and privileges, it is thus safe to say that most of the relevant regulated services will have to issue annual transparency reports (see Table 16.2).

³⁶ Given that providers of browsers could also qualify as mere conduits (ch 6), laws that allow blocking orders against browser operators would be subject to art 15 transparency disclosures. For a French example, Udbhav Tiwari, 'France's Browser-Based Website Blocking Proposal Will Set a Disastrous Precedent for the Open Internet' (*Open Policy & Advocacy*, 26 June 2023) <<https://blog.mozilla.org/netpolicy/2023/06/26/france-browser-websites-blocking/>> accessed 16 September 2023.

The *orders* caught by Article 15(1)(a) are only orders issued by the Member State authorities. Orders issued by authorities outside the EU are not covered because they are generally presumed not to impact citizens in the EU. However, a special case might be orders with extra-territorial effects from outside of the EU. These orders produce effects in the EU although they were not issued by local authorities.

The *notices* received must be published only by hosting providers (Article 15(1)(b)). However, if mere conduits or caching providers act upon notices, from the DSA's perspective, they act without being obliged to do so. Thus, they must report such actions under their investigations. Notices are only an input for these investigations. The notices covered includes both notices sent on the basis of illegality or terms of service violations. The share of notices processed by automated means must also be noted.

What counts as a notice is not specified by the DSA. However, inferring from other uses of the term across the regulation, it is clear that the term is not about individual claims which are notified but rather the *message* in which they are notified. Thus, a single notice, can may put providers on notice concerning many items of content. This fact alone, which is hard to avoid, makes any simple benchmarking of numbers akin to the comparison of apples and oranges. For online platforms, any data reported in transparency reports can be analysed together with the EU database of statements of reasons that should give the public further insights into specifics of industry notification practices. The same insights, however, are not available for services other than online platforms, as they are either not obliged to issue a statement of reasons at all (caching and mere conduits), or do not have to report it (non-platform hosting services).

Similar obligations regarding notices likewise apply to the *internal appeals* concerning content moderation decisions submitted to providers (Article 15(1)(d)). However, here, the obligation applies equally to other intermediary service providers—those being caching and mere conduits. The reason is that these providers can equally engage in content moderation, although such behaviour is voluntary. If they do so, they must report it as their own investigations and the complaints to such decisions under the section dedicated to complaints. Naturally, online platforms subject to the most elaborate rules concerning content moderation have the most extensive obligations to report.

Any content moderation based on provider's own investigations—ie investigations where the provider exercises some discretion—must be further elaborated by qualitative description that offers meaningful and comprehensible information about the content moderation practices (Article 15(1)(c)). This includes information about content moderation professionals employed and their training. The qualitative information is complemented by numerous statistics, as summarised above. In this context, it is worth noting that the scope of relevant activities that qualify as content moderation is vast. It captures any activities 'aimed, in particular, at detecting, identifying and addressing illegal content or information incompatible with their terms and conditions, provided by recipients of the service' (Article 3(t)). Thus, demotion, de-ranking,

Table 16.3 Examples of transparency reports

Examples for each service	Mere conduits	Caching	Hosting
Any orders from the EU Member States (Art 15(1)(a))	<i>Identity disclosure orders or website blocking orders</i>	<i>Preservation orders, or service blocking or mandates</i>	<i>Identity disclosure and content removal orders, staydown-orders, or user-blocking-orders</i>
Notices sent by third parties (Art 15(1)(b))	N/A	N/A	<i>Removal requests sent to webhosts, social media, cloud-based messaging apps, or app stores</i>
Any content moderation based on own investigations (Art 15(1)(c))	<i>Detection activities concerning child abuse or piracy</i>	<i>Termination of services to some clients by CDNs</i>	<i>De-ranking of users or content in the recommendation systems or demonetisation of accounts</i>
Any internal appeals to content moderation decisions (Art 15(1)(d))	<i>Appeals to account suspensions</i>	<i>Appeals to account terminations</i>	<i>Appeals of notifiers or content creators on video-sharing platforms</i>
Any use of automation for content moderation (Art 15(1)(e))	<i>Detection tools for abuse on networks</i>	<i>Detection tools for abuse of services</i>	<i>Detection tools for abuse, or decision-assistance for human moderators, prioritisation tools</i>

demonetisation, removal, suspension, or termination all qualify as relevant activities, regardless of whether their basis is terms and conditions or illegality.

Finally, to round up the process of content moderation, all automated tools regardless of their content (detection, initial assessment or assistance, decisions, or complaints), must be qualitatively and, to the extent possible, also quantitatively described. The DSA's significant innovation is that it includes horizontal safeguards for many of these tools by forcing disclosure of error and accuracy rates, safeguards, and specification of purposes for which such technologies are used. This information will make important contributions in many areas, including in copyright law, where filtering technology is mandated in some cases (Chapter 18.3).

Table 16.3 provides an overview of typical orders falling under each of the sections.

Given that transparency obligations form part of due diligence obligations, for VLOPs, they form part of the audits. To enhance the usefulness of data points, the Commission is empowered to adopt implementing acts³⁷ laying down templates in which the above information is to be reported.³⁸ The first such implementation can be adopted only following the advisory procedure, and thus is unlikely to enter into effect before providers issue the first round of reports.

³⁷ TFEU, art 291.

³⁸ DSA, art 88(3).

16.3.2 Advanced reporting for online platforms and search engines (Article 24)

Online platforms are subject to elaborate procedural norms regarding content moderation. Transparency is thus understandably extended for these services to cover other aspects of such procedures, such as disputes using out-of-court dispute settlement (ODS) and mandatory suspensions. These obligations are complemented by separate reporting obligations of the ODS bodies (Article 21(4)), trusted flaggers (Article 22(3)), and potentially also state authorities.

Online platforms also have an enhanced reporting obligation concerning their monthly active users. This information should establish whether they are designated as very large. Although search engines have no other reporting obligations unless they qualify as one of the intermediary services, they do have an obligation to report their monthly users regardless of their size. This disclosure of active users must follow the methodology adopted by the European Commission through a delegated act. The disclosure must take place via the provider's dedicated online interface and updated every six months.³⁹ If requested by the DSC of establishment or the European Commission, the provider must provide the latest data at a point in between these periodic disclosures. They can also request further explanations regarding the exact underlying calculations.

Table 16.4 provides an overview of specific transparency reporting based on tiers.

The most far-reaching transparency requirement concerns the statement of reasons to the EU's central databases.⁴⁰ These statements must be first stripped of any personal data. As explained by Recital 66, 'in order to keep the database continuously updated, the providers of online platforms should submit, in a standard format, the decisions and statement of reasons without undue delay after taking a decision, to allow for real-time updates where technically possible and proportionate to the means of the online platform in question'. The volume of these individuals' statements is likely to be massive.

The challenge will be how to apply this reporting obligation in a way which does not discourage more nuanced forms of content moderations due to the compliance costs considerations of providers.⁴¹ Keller argues that '[h]ighly prescriptive transparency obligations might also drive de facto standardisation and homogeneity in platform rules, moderation practices, and features'.⁴² The concern about the cost of standardisation to

³⁹ At time of writing, we already see the first stages of such reporting playing out in February 2023 and August 2023, but at present, without guidance from the delegated act as it has yet to come into force. For the full discussion and examples of such disclosures, ch 9.

⁴⁰ DSA, art 17(5).

⁴¹ This point was raised by Daphne Keller, 'Some Humility About Transparency' (*The Center for Internet and Society – Stanford Law School*, 19 March 2021) <<https://cyberlaw.stanford.edu/blog/2021/03/some-humility-about-transparency>> accessed 6 September 2023.

⁴² See *ibid.*

Table 16.4 Platform transparency reports

	Content Moderation Activity	Mere Conduits	Caching	Mere Hosting	Online Platform	Search Engines
Platform transparency obligations (Article 24)	ODS (Art 24(1)(a))	Voluntary use and reporting			(1) absolute number of disputes, (2) their outcomes, (3) median time for completion, and (4) the share of implemented decisions	Voluntary use and reporting
	Mandatory suspensions (Art 24(1)(b))				(1) absolute numbers of mandated suspensions, categorised by: (2) the grounds (illegal content, manifestly unfounded notices, or manifestly unfounded complaints)	
	Monthly active users (Article 24(2))	Voluntary use and reporting			at least every six months: (1) average monthly active recipients of the service, categorised by: (2) each relevant service operated by the provider	
	Statement of reasons (Article 24(5))	Voluntary use and reporting			continuous submission of statements of reasons to the EU database	Voluntary use and reporting

innovative content moderation practices indeed should not be lost on regulators, as the potential trade-off between two pursuits—innovation and standardisation—is well established.⁴³ However, standardisation can equally act as a catalyst of innovation.⁴⁴ Standardisation does not only lock in suboptimal solutions, as was argued in the debate around QWERTY keyboards,⁴⁵ but can actually also encourage innovation through newly gained scale, such as standardised shipping containers.⁴⁶ There is no reason to believe that content moderation standardisation will be any different. That said, the innovation concerns should still be on the radar of the regulators to avoid lock-ins into content moderation practices of the past.

⁴³ Knut Blind, ‘Standards and Innovation—What Does the Research Say?’ (ISO 2022) ISO research and innovation papers <<https://www.iso.org/publication/PUB100466.html>> accessed 6 September 2023.

⁴⁴ For overview of the academic debate, Knut Blind, ‘Standardisation as a Catalyst for Innovation’ [2009] ERIM Report Series Reference No EIA-2009-LIS <<https://papers.ssrn.com/abstract=1527333>> accessed 6 September 2023.

⁴⁵ The QWERTY keyboard is a famous example of suboptimal solutions that lock in everyone. However, the situation seems a bit more complex, even from the innovation standpoint: Neil M Kay, ‘Rerun the Tape of History and QWERTY Always Wins’ (2013) 42(6) Research Policy 1175.

⁴⁶ Steve Saxon and Matt Stone, ‘Container Shipping: The Next 50 Years’ (McKinsey & Company, October 2017) <www.mckinsey.com/~/media/mckinsey/industries/travel%20logistics%20and%20infrastructure/our%20insights/how%20container%20shipping%20could%20reinvent%20itself%20for%20the%20digital%20age/container-shipping-the-next-50-years-103017.pdf> accessed 6 September 2023.

16.3.3 VLOPs' and VLOSEs' content moderation reports (Article 42)

VLOPs and VLOSEs have enhanced obligations to issue content moderation annual reports in one of the official languages of the EU. They must be issued more frequently (at least every six months) and be more elaborate when setting out:

- content moderation staff dedicated to each relevant official EU language;
- qualification and linguistic expertise of content moderation staff;
- accuracy of automated tools for each relevant official EU language; and
- average monthly recipients of the service for each EU Member State.

The content moderation staff must only include numbers about those members whose work is relevant for the EU single market. Thus, employees or contract staff in Asia or the Americas are irrelevant. Information about the staff must also be reported 'in respect of the service offered' (Article 42(2)(a)). This means that each regulated service must be subject to a specific report. Thus, information about the content moderation staff of an app store can be copied and reported for a video-sharing service if the same staff worked on both services.

Article 42(2)(a) also implies that the breakdown should specifically reveal what resources are dedicated to internal complaint mechanisms, and enhanced support for trusted flaggers.

The breakdown per the relevant official EU language is meant to unveil structural differences between how platforms allocate their resources. The providers must report their average monthly users per the Member State individually. At the time of writing, it is impossible to find out how many content moderators even bigger services employ for each language in which they operate. This is reinforced by the requirement that such numbers are accompanied by a qualitative description of their training and linguistic expertise.

The reported information is an indication that helps to understand the attention given by providers to individual societies within the EU and its corresponding effect. After the DSA, they can be contrasted with the reported amount of advertising and content moderation decisions related to individual countries to unveil interesting connections and correlations. Indeed one of Frances Haugen's important revelations about Facebook concerned how providers under-invest in some countries, even though they have a substantial presence in them.⁴⁷ These revelations informed policymaking.

Furthermore, automated tools must be specifically tested for their accuracy in each language. This obligation is particularly important as the training of technologies often

⁴⁷ Rebecca Staudenmaier, 'Whistleblower: Facebook stirs global conflicts' *DW News* (Berlin, 6 November 2021) <<https://www.dw.com/en/facebook-whistleblower-warns-company-is-neglecting-languages-other-than-english/a-59739260>> accessed 6 September 2023.

takes places in the cultural and linguistic context of some larger countries, and thus potentially neglects the effects of the tools on smaller countries when scaled up to serve the same needs.

Finally, VLOPs and VLOSEs must publish their audit documentation (Article 42(4)). This includes the following documents:

- self-assessment regarding the results of the risk assessment;
- report outlining the specific risk mitigation measures;
- audit reports by auditors;
- follow-up audit implementation report;
- any consultations held to support risk assessment or risk mitigation.

The providers are allowed to redact confidential information. The latter can only be redacted if it is likely to ‘cause significant vulnerabilities for the security of its service, undermine public security or harm recipients’ (Article 42(4)). Any such redaction must be accompanied by a public statement explaining why such information is omitted. Unredacted reports must be sent to the European Commission and the DSC of the establishment.

16.3.4 Transparency of other actors

Content moderation and advertising concerns are not limited to behaviour of providers of digital services. Content moderation activities are shaped by content creators, notifiers of content, such as victims, NGOs or enforcement agencies, and authorities which issue relevant orders. Ills of the advertising ecosystem are also shaped by advertisers and their agencies. The DSA places some transparency obligations on these other actors.

Trusted flaggers (Article 22) are given a privileged position among notifiers. Their notices carry more weight because they ought to represent notifications that are well-considered. Although trusted flaggers are subject to certification by regulators, in order to shine some light on their performance, the DSA obliges them to publish annual transparency reports. The reports cover only illegal content.

The mandated reports must be ‘comprehensive and detailed’ and include information about the absolute number of notices with a breakdown according to providers, type of illegal content, and the follow-up action taken. They must also detail how the trusted flagger retains its independence from any provider. While the text does not mandate reporting for each service, to facilitate general comprehension of the reports, they should not make only general statements about the number of notices sent to large companies that operate hundreds of different services but distinguish between individual services. In addition to Article 22(3), whenever a trusted flagger is operated by a public entity, such as Europol, the applicable freedom of access legislation can offer additional data points to scrutinise its practices.

Publication of reports about notices concerning content that ‘only’ violates terms and conditions is not mandated. They can be, however, introduced by the relevant Codes of Conduct.

Despite the importance of the *ODS bodies* (Article 21) in the DSA, their transparency is arguably underdeveloped. The ODS bodies do not have to publish public annual reports or their individual decisions. They only have to annually report to the DSC who certified them, specifying an absolute number of disputes received, broken down by the outcomes, and the average time for a dispute handling. They should also report any shortcomings that they have encountered. The relevant DSCs then must issue biannual reports summarising the data for all certified ODS bodies, including best practices and recommendations for how to improve the system.

Given the limited reporting obligations, one of the possible improvements surely can be the transparency of the ODS bodies, specifically the process of reporting decisions and publication of reports concerning their own activities. The DSCs can arguably require increased transparency as part of fair procedural rules. As explained in Chapter 11.5, the DSCs are tasked with certifying and supervising such bodies across the EU.

Finally, the DSA does not explicitly deal with the question of transparency by *public authorities*.⁴⁸ However, if such authorities operate as trusted flaggers, they have obligations under Article 22(3). If they issue orders, they might have obligations based on national or European law, such as Article 8 TCR. If authorities send simple notifications and thus are not acting as trusted flaggers, the only possible sources of transparency are national freedom of information laws or annual activity reports.

16.4 Conclusion

The DSA creates a set of default safeguards applicable to most of the situations of delegated enforcement. By putting gatekeepers of digital services under scrutiny, it will help to reveal the extent of content moderation undertaken and some aspects of its quality. However, as much as the conventional method of annual transparency reporting serves its purpose, it ultimately only acts as a rear mirror to what has already happened. Therefore, the DSA has supplemented it with an exciting new measure: the involvement of researchers in transparency endeavours. Indeed, if we wish to better examine what is happening now in the digital ecosystem, and potentially what will happen in the future, data access by researchers presents a novel way forward. Here, too, the DSA institutionalises data access as a general safeguard that can step in to provide a look at the actions of regulators and companies alike. Because the researchers’ mandate is

⁴⁸ For instance, Europol’s pre-DSA reports: European Union Agency for Law Enforcement Cooperation., *EU Internet Referral Unit Transparency Report 2021: Terrorist Propaganda Monitoring and Analysis, Referrals, and Public Private Partnerships*. (EU Publications Office 2022) <<https://data.europa.eu/doi/10.2813/341047>> accessed 6 September 2023.

worded very broadly, the sky is the limit for its potential application. This access can put even some of the most controversial policies of the EU, such as Article 17 CDSM Directive, on a corrective course even after they were already adopted. However, for this to happen, there will be numerous practical obstacles to access that first have to be cleared.

PART IV

THE DSA AS A POLICY TOOL

The DSA as a Cornerstone of the EU Single Market

17.1 Introduction	371	17.4.3 View from the national parliament	380
17.2 Five Main Pillars of the Digital Single Market	372	17.5 Pre-emption by the DSA	380
17.3 The Period 1995–2022	374	17.5.1 Liability rules for search engines	384
17.4 National Experimentation Post-DSA	376	17.5.2 Accountability rules	385
17.4.1 Notification obligations	377	17.5.3 Content rules	386
17.4.2 Country-of-origin principle	379	17.4.4 Other gaps in the DSA	388
		17.6 Conclusion	389

17.1 Introduction

The DNA of any European rules on digital services—be it the General Data Protection Regulation (GDPR) or the Digital Services Act (DSA)—is the promotion of the internal market as a space without frontiers. Given the internet’s cross-border nature, the digital ecosystem is a natural candidate for the efforts to construct the market without internal regulatory barriers. Compared to many other policy areas, it is characterised by a lack of legacy policies and complex challenges of a global nature, which places the uniquely positioned European Union (EU) at an advantage. Looking at the flurry of legislative acts introduced by the Von der Leyen Commission,¹ this advantage is being used considerably.

My goal in this chapter is to put the DSA into the perspective of the EU digital single market architecture and explain why the DSA is more than just a new Regulation. Its systemic importance can probably be best compared to the GDPR, although its reach is much more limited. Should the Member States wish to introduce any additional national regulation of digital services, it would have to fit them into the elaborate framework already set up by the DSA, along with a set of related policies, including the remaining provisions in the E-Commerce Directive (ECD). I argue that the space left to the Member States is increasingly shrinking, and the existing mechanisms, such as the country-of-origin principle, will likely make national regulation even

¹ The DSA, Digital Markets Act, Data Act, Data Governance Act, Digital Operational Resilience Act, Artificial Intelligence Act, Directive on Platform Work, Network and Information Security (NIS2) Directive, and European Digital Identity Regulation.

more difficult. Politically, the DSA is thus likely to direct any national frustrations to the EU level through Codes of Conduct or as related European sectorial legislation. Systemically, the DSA is a significant—though porous—regulatory roadblock for national rulemaking.

17.2 Five Main Pillars of the Digital Single Market

The European regulation of digital services is based on five important *horizontal* regulatory pillars, further supplemented by sectorial regulation.

The first pillar relates to *the procedure of national law-making*. In 1998, the first mechanism was introduced to improve the coordination of technical standards.² It established the concept of information society service providers and created an obligation to notify the European Commission of national ‘rules on services.’³ While the Member States often forget this rule,⁴ the result of a failure to notify is significant—it leads to the ineffectiveness of the underlying legislation, which cannot be applied to individuals.⁵ Post-DSA, this pillar is likely to receive more attention because the losing stakeholders tend to utilise the tool in litigation to undermine the applicability of national law.⁶

The second and related pillar is *the country-of-origin principle*. It was introduced in 2000 through the ECD. It further strengthened the coordination by legislating a rule, according to which ‘for reasons falling within the coordinated field, [it is prohibited to] restrict the freedom to provide information society services from another Member State.’ The Union thus started to restrict the ability of the individual Member States to apply their own stricter rules to information society services when firms from the other Member States provide them. The Directive then postulated that ‘any measures,’ not just ‘requirements of a general nature’ as under the Single Market Transparency Directive, directed against information society services providers, must be subject to an elaborate procedure constraining the reasons for such measures, their proportionality, conditioning them to cross-border consultation, and finally to a notification process before the European Commission.⁷ The legal effect of the failure to notify is the same under the Single Market Transparency Directive—the loss of applicability.⁸

² European Parliament and Council Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services [1998] OJ L204/37 as amended by Directive 98/48/EC (Amended Single Market Transparency Directive 98/34/EC).

³ Amended Single Market Transparency Directive 98/34/EC, art 1(5): “rule on services”, requirement of a general nature relating to the taking-up and pursuit of service activities within the meaning of point 2, in particular provisions concerning the service provider, the services and the recipient of services, excluding any rules which are not specifically aimed at the services defined in that point’.

⁴ Case C-299/17 *VG Media v Google LLC* ECLI:EU:C:2019:716.

⁵ Case C-194/94 *CIA Security International SA v Signalson and Securitel* ECLI:EU:C:1996:172, para 54.

⁶ *VG Media* (n 4) and recent attempts to invoke the principle in the pending case of KVB 56/22 dealing with newly adopted competition rules.

⁷ ECD, art 3.

⁸ Case C-390/18 *Airbnb Ireland* ECLI:EU:C:2019:1112, para 90.

Post-DSA, this pillar will gain importance for the very same reason as the notification process.

The third pillar relates to *data flows*. The Data Protection Directive introduced in 1995 enabled the free flow of personal data across the EU. Without the positive harmonisation, the data flows between the Member States would have hindered the functioning of most of the digital services. The area has seen a lot of new legislative activity over recent years, such as the adoption of the E-Privacy Directive and the Law Enforcement Directive.⁹ In 2016, this pillar was reformed through the GDPR, which is only starting to shape many areas of digital policy. The EU is also increasingly introducing policies to regulate non-personal data.¹⁰

The fourth pillar concerns the *liability of providers of digital services*. It was also introduced by the ECD in the form of provisions concerning the liability of intermediary services. Unlike other pillars, its coordination is mainly negative. It states what is not possible in national law. These rules subjected the entire national legal system to coordinating rules that excluded any liability of selected digital services for storing or giving access to third-party content. These rules directly pre-empt any national legislation, new or old, that would try to impose such legal obligations. The provisions create a common level playing field in the Union for most digital services that work with other people's content.

Finally, the DSA has now built a fifth pillar of *accountability of digital services*. Its obligations create due process obligations and risk management safeguards throughout the Union. The DSA builds on top of the previous pillars and incorporates and extends the fourth pillar from the ECD. It will soon be further expanded by the Artificial Intelligence Act and the Directive on Platform Work.¹¹

These five pillars are the building blocks supporting the free movement of digital services across the EU and form the backbone for its digital services regulation. In the coming years, the third and fifth pillars will surely take centre stage. This is an effect known from many other areas of harmonised law, where free movement-related coordination provisions tend to take the backseat whenever the positive substantive harmonisation expands. However, pillars one and two will continue to discipline the lawmakers who need to ensure that national experiments clear such hurdles in advance.

⁹ European Parliament and Council Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L201/37 (ePrivacy Directive); European Parliament and Council Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties [2016] OJ L119/89 (Law Enforcement Directive).

¹⁰ These include the Regulation on Free-Flow of Non-personal Data, Data Act, and Data Governance Act.

¹¹ Commission, 'Proposal for a Directive of the European Parliament and of the Council on improving working conditions in platform work' COM(2021) 762 final; Commission, 'Proposal for a Directive of the European Parliament and of the Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts' COM(2021) 206 final.

17.3 The Period 1995–2022

When the ECD was adopted in 2000, the number of internet users was incomparably lower and digital technology was not so central to our lives. Before the ECD, there was little national experimentation (Chapter 4). European countries and the EU legislators of the late 1990s were more concerned with how to coordinate future legislation. This is why the ECD left even the most basic questions, such as how to notify and remove content, to the states' experimentation.¹² The idea was that national experiments could provide the Union with some precedents for how things could work. However, no country has developed a comprehensive approach in the past two decades. This is despite the fact that there was no shortage of controversies in this period. The DSA learns much more from the self-regulatory practices emerging from this period than from national experiments.

The formative period for some of the crucial American and European legislation, 1995–99, was a period of moral panic about the safety of children online. Time Magazine's 'Cyber Porn' cover from July 1995 famously asked—'Can we protect our kids – and free speech?' It is no coincidence that Mr Somm's German criminal case about CompuServe's distribution of child abuse material (1995), the adoption of the Communication Decency Act (1996) and the establishment of the UK's Internet Watch Foundation to blacklist child abuse material (1996) all took place only a few months apart. As predicted by media theorist, Marshall McLuhan in 1960s, the world was slowly becoming a 'global village'.¹³

From the 1990s onward, new problems only piled up, with an especially intense period in the late 2010s. From 2013–15, Europeans were made aware of terrorist threats and aggressive recruitment by ISIS through social media services.¹⁴ In 2015, European newspapers started being filled with headlines about the influx of hate speech after 1.3 million people came to the continent to request asylum.¹⁵ The refugee crisis gave pause to many politicians, some of whom started asking for European rules for social media and looking at the Commission for solutions.¹⁶ But the Commission did not act. On the contrary, in 2016, it had effectively announced that it would not reopen the ECD¹⁷ and thus delayed any intention to legislate horizontally.

¹² ECD, Rec 46 and art 21.

¹³ Marshall McLuhan, *The Gutenberg Galaxy: The Making of Typographic Man* (Repr, Univ of Toronto Pr 2008).

¹⁴ Sam Jones, 'Jihad by Social Media' *Financial Times* (28 March 2014) <<https://www.ft.com/content/907fd41c-b53c-11e3-af92-00144feabdc0>> accessed 30 August 2023; Gianna Grün, 'How "Islamic State" is Fighting Its Battles Digitally' *dw.com* (6 March 2015) <<https://www.dw.com/en/tweets-as-weapons-how-islamic-state-is-fighting-its-battles-digitally/a-18493604>> accessed 30 August 2023.

¹⁵ Dagmar Breitenbach, 'Racism on Facebook' *dw.com* (31 August 2015) <<https://www.dw.com/en/how-facebook-deals-with-openly-racist-comments/a-18684379>> accessed 30 August 2023; Mike Wendling, '2015: The Year That Angry Won the Internet' *BBC News* (30 December 2015) <<https://www.bbc.com/news/blogs-trending-35111707>> accessed 31 August 2023.

¹⁶ Andrew Rettman and Aleksandra Eriksson, 'Germany Calls for EU Laws on Hate Speech and Fake News' *EUobserver* (6 April 2017) <<https://euobserver.com/world/137521>> accessed 31 August 2023; Joanna Plucinska, 'Brussels at Odds with Germany on Hate Speech' *POLITICO* (1 June 2017) <<https://www.politico.eu/article/commissions-hate-speech-stance-puts-it-at-odds-with-german-proposal/>> accessed 31 August 2023.

¹⁷ Commission, 'Online Platforms and the Digital Single Market Opportunities and Challenges for Europe' (Communication) COM(2016) 0288 final, 9: 'The Commission will review the need for formal notice-and-action

Tired of waiting,¹⁸ some Member States, such as Germany and France, decided to adopt their own rules. These national laws were mostly about reporting mechanisms but also imposed transparency obligations and obligations to appoint a legal representative.¹⁹ The Commission, probably due to political sensitivity, did not slow down any of these national experiments even though they technically often violated the EU law. Quite surprisingly, the Commission did not always make use of its tools, even where breaches of the EU legislation were obvious (eg in the case of German law).²⁰ The Commission de facto tolerated violations of the ECD's country-of-origin principle and was not the strongest guardian of the free movement of services under the Treaty.

During this time, the EU was still legislating, but only on sectorial issues. In 2018, the EU adopted its updated Audiovisual Media Services Directive (AVMSD), the Terrorist Content Regulation (TCR), and in 2019, the Copyright in the Digital Single Market (CDSM) Directive.

The political turning point might have come around 2017–18. The Cambridge Analytica scandal²¹ along with other investigations into Russian interference in the United States (US) elections²² and the Brexit campaign,²³ only solidified the broader view that a comprehensive Union regulation is needed. After the German and French experiments did not achieve much change,²⁴ it became obvious that the Member States could not act effectively against the largest transnational companies on their own. In other words, the past 20 years have made a perfect case for more detailed EU rules on the matter.

procedures, in light of the results of, inter alia, the updated audio-visual media and copyright frameworks and ongoing self-regulatory and co-regulatory initiatives.

¹⁸ In February 2017, the German Minister for Economy and Energy asked Commission's Vice-President, Andrus Ansip, for European rules on the procedures and regarding notice-and-action: 'Letter from Brigitte Zypries MdB to Andrus Ansip (17 February 2017)' <https://www.bmwk.de/Redaktion/DE/Downloads/B/brief-zu-hate-speech-fake-news.pdf?__blob=publicationFile&v=8> accessed 30 August 2023.

¹⁹ Commission, "Impact Assessment" (Commission Staff Working Document) Accompanying the Document "Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and Amending Directive 2000/31/EC" SWD(2020) 348 final, Annex 6, 122.

²⁰ The expert services of the German parliament itself were of the view that the law likely violates the country-of-origin principle, Deutscher Bundestag, 'Zur Europarechtskonformität des Entwurfs Netzwerkdurchsetzungsgesetzes' (PE 6–3000–36/17, Fachbereich Europa, 2017) <<https://www.bundestag.de/resource/blob/515830/948c282fef4c87d915f22d5d28864402/PE-6-036-17-pdf-data.pdf>> accessed 29 August 2023. The same opinion was presented by a number of leading German scholars, such as Prof Hoeren and Prof Spindler, Thomas Hoeren, 'Netzwerkdurchsetzungsgesetz europarechtswidrig' (*beck-community*, 30 March 2017) <<https://community.beck.de/2017/03/30/netzwerkdurchsetzungsgesetz-europarechtswidrig>> accessed 29 August 2023; Gerald Spindler, 'Legal Expertise Commissioned by BITKOM Concerning the Notified German Act to Improve Enforcement of the Law in Social Networks (Netzwerkdurchsetzungsgesetz)' (Institute of Commercial and Media Law, University of Göttingen 2017) <<https://www.bitkom.org/sites/default/files/file/import/Legal-Expertise-Official-2-0.pdf>> accessed 29 August 2023.

²¹ The European Consumer Organisation (BEUC), 'European Parliament Hearing on the Use Of Facebook Users' Data by Cambridge Analytica and Its Impact on Data Protection (25 June 2018)–Testimonial by BEUC Deputy Director General Ursula Pahl' (BEUC 2018).

²² Robert S Mueller, 'Report on the Investigation into Russian Interference in the 2016 Presidential Election' (US Department of Justice 2019) vol 1 <<https://www.justice.gov/archives/sco/file/1373816/download>> accessed 29 August 2023.

²³ *Ben Bradshaw v United Kingdom* App No 15653/22 (ECtHR, pending).

²⁴ William Echikson and Olivia Knodt, 'Germany's NetzDG' (CEPS 2018) <<https://www.ceps.eu/ceps-publications/germanys-netzdg-key-test-combatting-online-hate/>> accessed 29 August 2023.

In terms of drafting, the DSA heavily borrows from earlier soft laws of the European Commission. In 2017, the Commission published a Communication on tackling illegal content,²⁵ which was supplemented a year later by a Recommendation.²⁶ These were the first building blocks for the agenda that the Directorate-General CONNECT²⁷ prepared for the next Commission. Once von den Leyen started her tenure in December 2019, the drafting of the DSA officially started. Within one year, just before Christmas 2020, the European Commission unveiled its DSA proposal²⁸ along with a proposal for the Digital Markets Act.

Undoubtedly, the COVID-19 pandemic and the Russian attack on Ukraine only heightened the sense of urgency to create new rules. The DSA was adopted within less than two years in October 2022.

17.4 National Experimentation Post-DSA

From a bird's-eye perspective, the DSA on the one hand constrains private decision-making by giving due process rights to individuals, and on the other, regulates the design of services to protect individuals from various risks. Typical platforms are only obliged to consider the design of specific product features (eg advertising, or recommender system) or risks to children or consumers and are regulated mostly prescriptively. Providers with very large user bases are regulated through an open-ended regulatory dialogue about their risk mitigation efforts.

Without a doubt, one of the benefits of the DSA is that many initiatives that only pretended to be 'self-regulatory' now gain a proper framework, which is subject to institutional rules and transparency. While the DSA cannot stop private ordering outside of its remit, the fact that it can offer some regulatory relevance to such rules should act as an incentive for many areas to consider transforming their soft rules into the DSA-approved co-regulatory Codes of Conduct or standards (Chapter 20).

For the EU legislature, these co-regulatory schemes will provide more visible evidence about what works and what does not and perhaps reduce any pressure to introduce hastily enacted legislation. Where regulatory maturity is missing, the stakeholders will likely push for co-regulatory dialogues. This creates a risk that private ordering can lead to too much rulemaking with little practical value.

Except for some areas outline below, I think the Member States will find it difficult to identify what issues they can still regulate on their own. From now on, they will have to navigate not only the EU's coordination framework but also substantive European rules that can pre-empt national law-making. It is expected that this will be a prolonged

²⁵ Commission, 'Tackling Illegal Content Online Towards an Enhanced Responsibility of Online Platforms' (Communication) COM(2017) 0555 final.

²⁶ Commission Recommendation (EU) 2018/334 on measures to effectively tackle illegal content online [2018] OJ L63/50.

²⁷ Directorate-General for Communications Networks, Content and Technology.

²⁸ Commission, 'Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC' COM(2020) 825 final.

process of realisation, and it will take many decisions from the Court of Justice of the European Union (CJEU) to drive home some of the points made in this chapter.

So why am I sceptical about national experimentation?

There are many aspects of digital services that the Member States might wish to regulate. However, whichever direction they look, they will increasingly find that they can easily step on the toes of the EU law. Any national legislature is subject to a series of rules that constrain its law-making powers:

- Any draft rules specifically about information society services are subject to *notification* before their adoption by the European Commission under the Single Market Transparency Directive 2015.²⁹
- Any measures restricting the free movement of services that are provided from another Member State are subject to the *country-of-origin principle*. If an information society service is established in one Member State, the principle restricts other states from imposing their own stricter rules on such providers. Any attempts to regulate more strictly are subject to a proportionality test and notification process (under Article 3 ECD).
- Any national rules, not only those targeting digital services that overlap with the DSA's full harmonisation, are *pre-empted by EU law* and must be set aside by national authorities. This follows from case law on the primacy of the EU law from the CJEU.³⁰
- Any rules restricting the free movement of services within the single market are subject to *scrutiny* by the rule of the free movement of services established in Article 56 TFEU.

These four *regulatory constraints of the digital single market* collectively restrict the ability of the Member States to regulate. Every year, the ability of the states to regulate is further constrained by new harmonised rules adopted by the EU legislature in addition to the DSA. In other words, regulating digital services will be increasingly tricky and often require the Member States to carefully navigate a web of the EU rules. One wrong step and the entire legislation can be inapplicable.

17.4.1 Notification obligations

The Single Market Transparency Directive introduced a notification system to monitor national *draft* technical regulations in 1998 to allow the EU to see what rules the Member States are adopting. Technical regulation, such as standards, was an important source of binding or de facto binding restrictions that hampered the free movement

²⁹ European Parliament and Council Directive (EU) 2015/1535 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services [2015] OJ L241/1 (Single Market Transparency Directive 2015).

³⁰ Case 106/77 *Amministrazione delle Finanze dello Stato v Simmenthal* SpA ECLI:EU:C:1978:49.

of goods. At its inception, the initial Directive only dealt with technical regulation of products,³¹ but information society services³² were added to its scope by an amendment in the same year³³ and remain to this day in its latest iteration, the Single Market Transparency Directive 2015. The system covers any rules ‘of a general nature’³⁴ but only if they are ‘specifically aimed at’ information society services.³⁵

Information society services were defined as ‘any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.’³⁶ The elements were then further specified in the same provision as follows:

- (i) ‘at a distance’ means that the service is provided without the parties being simultaneously present;
- (ii) ‘by electronic means’ means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means;
- (iii) ‘at the individual request of a recipient of services’ means that the service is provided through the transmission of data on individual request.

This very broad definition was thereafter also used by the ECD in 2000 when constructing the country-of-origin principle. In the Single Market Transparency Directive however, the term was employed for its slightly different purpose of scrutinising the rules for their compatibility with EU law.

As part of the system of transparency through notification that the Directive creates, it essentially asks the Member States to pace their national rule making in the non-harmonised regulatory area (Article 6).³⁷ For instance, the Member States are expected to refrain from adopting new rules once the Council has adopted a position at first reading on a Commission proposal concerning that sector.³⁸

³¹ European Parliament and Council Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations [1998] OJ L204/37 (Original Single Market Transparency Directive 98/34/EC).

³² ‘Information society services’ being services within the meaning of art 1(2) of the Amended Single Market Transparency Directive 98/34/EC; art 1(1)(b) of the Single Market Transparency Directive (EU) 2015/1535.

³³ European Parliament and Council Directive 98/48/EC amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations [1998] OJ L217/18 (Single Market Transparency Directive 98/48/EC).

³⁴ Single Market Transparency Directive (EU) 2015/1535, art 1(1)(e) (“rule on services” means a requirement of a general nature relating to the taking-up and pursuit of service activities ...”).

³⁵ *ibid* (‘... excluding any rules which are not specifically aimed at the services defined in that point.’).

³⁶ Amended Single Market Transparency Directive 98/34/EC, art 1(2); Single Market Transparency Directive (EU) 2015/1535, art 1(1)(b).

³⁷ Single Market Transparency Directive (EU) 2015/1535, art 6.

³⁸ *ibid* Rec 16, art 6(5).

17.4.2 Country-of-origin principle

The ECD further strengthened the notification system. The country-of-origin principle set out under Article 3 ECD limits how national rules can apply to information society services. Despite its significance, the provision continues to invite a lot of confusion about its actual meaning. To date, 15 cases have shaped the provision's meaning.³⁹

The relevant laws that might be caught under Article 3 ECD do not have to single out information society services. It is enough that they affect them. The country-of-origin principle only applies to what is known as the 'coordinated field' (Articles 2(h) and 3(3) ECD). All rules in such an area are then subject to an overarching prohibition to restrict the cross-border provision of information society services from another Member State (Article 3(2) ECD) unless they can invoke a limited set of reasons and follow a specified ordinary (Article 3(4) ECD) or urgent procedure (Article 3(5) ECD).

If Article 3 is applicable, the national rule can be applied; however, its outcome cannot be stricter for the provider of relevant services than the laws in the Member State where it is established. This follows from the *eDate Advertising* ruling, which conceptualised the rule as a substance limitation rather than a conflict of law rule.⁴⁰ Thus, a provider established in Ireland cannot be held to higher standards in Germany, even though the same countries can continue to apply higher standards to identical providers established in Germany.⁴¹

The goal of the mechanism, according to the CJEU, is to monitor measures capable of undermining the free movement of services by putting the Commission and the Member State, on whose territory the service provider in question is established, on alert about the upcoming measures.⁴² This, in turn, allows them to assess whether those 'measures are necessary for furtherance of overriding reasons in the general interest'.⁴³

Article 3 ECD applies to any measures restricting 'for reasons falling within the coordinated field ... the freedom to provide information society services from another Member State' (Article 3(2)). These measures need only be 'applicable' to such services that fall within the scope of Article 3 ECD, and this will be the case 'regardless of whether [the measures] are of a general nature or specifically designed for them' (Article 2(h)). Article 3 ECD thus clearly applies to both measures of a specific nature, such as injunctions or orders against providers, and measures of a general nature, such as laws that restrict such services. It can also be an administrative practice or a behaviour by an administration.⁴⁴

³⁹ The most important ones are *Airbnb Ireland* (n 8); Case C-434/15 *Asociación Profesional Elite Taxi v Uber Systems Spain* ECLI:EU:C:2017:9811; Case C-320/16 *Uber France* ECLI:EU:C:2018:221; Case C-320/16 *Star Taxi App* ECLI:EU:C:2020:980; Case C-376/22 *Google Ireland and others* (case in progress, lodged 10 June 2022); Case C-376/22 *Google Ireland and others* ECLI:EU:C:2023:835.

⁴⁰ Joined Cases C-509/09 and C-161/10 *eDate Advertising GmbH and others v X and Société MGN Limited* ECLI:EU:C:2011:685.

⁴¹ See also Case C-62/19 *Star Taxi App* (n 39) para 72.

⁴² *Airbnb Ireland* (n 8) para 91.

⁴³ *ibid.*

⁴⁴ Emmanuel Crabit, 'La Directive Sur Le Commerce Électronique. Le Projet "Méditerranée"' (2000) 4 *Revue du Droit de l'Union Européenne* 749, 786.

The Court has recently given the country-of-origin principle a strong boost in *Google Ireland and others* where it held in no unclear terms that:⁴⁵

Member States are not, as a matter of principle, authorised to adopt [measures of a general and abstract nature which are aimed at a category of given information society services described in general terms], so that verification that those measures are necessary to satisfy overriding reasons in the general interest is not even required.

The Court explained that the opposite holding would undermine mutual trust between the Member States and be in conflict with the principle of mutual recognition on which Directive 2000/31 is based.⁴⁶

17.4.3 View from the national parliament

When the notification and country-of-origin rule combine with not only the pre-emption arising from DSA's harmonisation but also the backstop protection of the free movement of services under the TFEU, the big picture from the perspective of the national parliaments looks rather complex. For instance, a legislature considering age verification laws to be imposed on social media must first query the draft law's compatibility with Articles 28 and 35 DSA. Even if no pre-emption exists for such rules, the legislature must notify such draft laws, and if the law applies to the other EU companies, keep in mind the country-of-origin principle. Table 17.1 provides an overview of the scope of the rules and their consequences.

Most prospective 'platform laws' will arguably fail to navigate the above four constraints. Any rules dealing with content moderation, or contestation of content moderation decisions are almost certain to fail on the barbed wire of the EU pre-emption. The same applies to notification rules targeting social media platforms, marketplaces, or infrastructure services. In fact, most of the digital ecosystem, as depicted in Figure 17.1, is strongly insulated from the DSA add-on due to conflict or field pre-emption. The blind spots in the DSA coverage, such as payment and advertising intermediaries (that do not qualify for any of the liability exemptions), software tools or editorial services, are less protected against national experimentation.

17.5 Pre-emption by the DSA

The DSA lays down harmonised rules of the area (Article 1) that it '*fully* harmonises'⁴⁷ (Recital 9). The explicit reference in Recital 9 and the absence of a minimum harmonisation clause clearly indicate the full harmonisation approach. This means the EU

⁴⁵ Case C-376/22 *Google Ireland and others* ECLI:EU:C:2023:835, para 59.

⁴⁶ *ibid* para 53.

⁴⁷ Emphasis mine.

Table 17.1 Limits on regulation of digital services

Restriction	Pre-emption by full harmonisation (DSA)	Notification obligation (TRIS)	Country-of-origin principle (ECD)	Services Directive & TFEU Free Movement
Geographical scope	Cross-border and domestic	Cross-border and domestic	EU cross-border	At least potentially EU cross-border
Material scope	Any overlapping, conflicting rules	Any draft of 'a requirement of a general nature' ^a	Any (stricter) measure in the coordinated field ^b	Any restriction of freedom to provide services
Personal scope	Mostly, any rules applicable to mere conduit, caching and hosting services	Any requirement 'specifically aimed at' information society services ^c	Any measures 'applicable ^d to information society services	Services, including those of users who use the information society service
Legal consequence	Always inapplicable	Inapplicable if it is not notified	Inapplicable if it does not pass the test and is not notified	Inapplicable if it does not pass the test

^a Single Market Transparency Directive (EU) 2015/1535, art 1(1)(e).

^b ECD, art 3(2) (as interpreted by *eDate Advertising*).

^c Single Market Transparency Directive (EU) 2015/1535, art 1(1)(e).

^d ECD, art 2(h) ('requirements laid down in Member States' legal systems applicable to information society service providers or information society services, *regardless of whether they are of a general nature or specifically designed for them*') (emphasis mine).

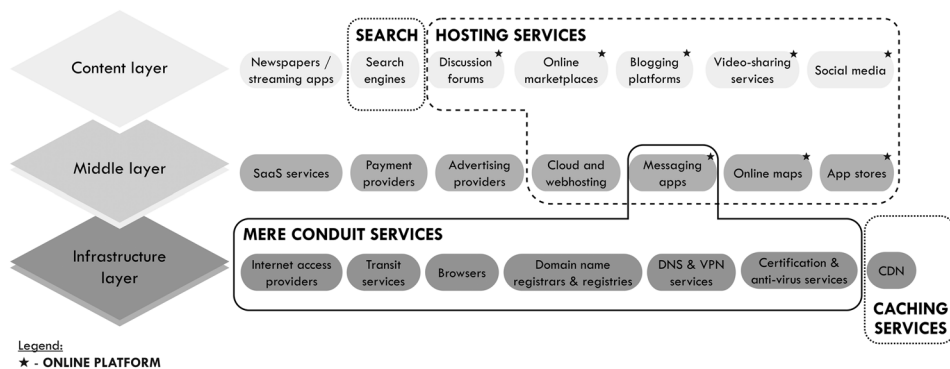


Figure 17.1 The DSA's regulatory coverage

legislature has adopted rules that cannot be deviated from in either direction. The only minimum harmonisation within the DSA is in Articles 9–10.

Once pre-emption applies, the principle of primacy requires that Union law takes precedence in cases of conflict.⁴⁸ Such conflicting national rules then have to be repealed by the Member States due to the principle of loyal cooperation,⁴⁹ and potentially

⁴⁸ Case 6/64 *Costa v ENEL* ECLI:EU:C:1964:66.

⁴⁹ Case 74/86 *Commission v Germany* ECLI:EU:C:1988:198, para 11.

set aside by courts due to the doctrine of direct effect.⁵⁰ To clarify which Union rules pre-empt which national rules, it is necessary to conduct a two-pronged analysis. First, (1) it has to be determined whether national and Union rules overlap in scope (scope of applicability). If they do, (2) it has to be examined whether the EU legislator *intended* to exclude national rules such as those at stake.⁵¹

As explained by Amedeo Arena, in practice, the CJEU can find pre-emption because of (a) an actual conflict due to wording and/or frustration of goals of harmonisation (conflict pre-emption), or (b) an intention of the EU legislator to displace any national regulation in the area (field pre-emption).⁵² The basic rule concerning the pre-emptive effect of the Union rules is that whenever national laws pursue the same goal as Union laws, they are pre-empted if they overlap and collide.

The legislative goal is set out in Article 1(1) DSA:

The aim of this Regulation is to contribute to the proper functioning of the internal market for intermediary services by setting out harmonised rules for a safe, predictable and trusted online environment that facilitates innovation and in which fundamental rights enshrined in the Charter, including the principle of consumer protection, are effectively protected.

Recital 2 makes clear that the full harmonisation effect of the DSA aims at eliminating existing (and growing) legal fragmentation. It states that:

This Regulation *fully harmonises the rules applicable to intermediary services in the internal market with the objective of ensuring a safe, predictable and trusted online environment*, addressing the dissemination of illegal content online and the societal risks that the dissemination of disinformation or other content may generate, and within which fundamental rights enshrined in the Charter are effectively protected and innovation is facilitated. Accordingly, Member States should not adopt or maintain additional national requirements relating to the matters falling within the scope of this Regulation, *unless explicitly provided for in this Regulation*, since this would affect the direct and uniform application of the fully harmonised rules applicable to providers of intermediary services in accordance with the objectives of this Regulation.⁵³

As a result, the Member States, such as France, Germany, and Austria, that previously introduced rules such as notice and takedown regimes, transparency obligations or

⁵⁰ *Simmenthal* (n 30) para 17.

⁵¹ Amedeo Arena, 'Exercise of EU Competences and Pre-Emption of Member States' Powers in the Internal and the External Sphere: Towards "Grand Unification"?' (2016) 35(1) *Yearbook of European Law* 28.

⁵² *ibid* part B; for a discussion in the area of IP, Martin Husovec, 'Closing the Gap: How EU Law Constrains National Rules Against Imitation' in Ansgar Ohly and others (eds), *Transition and Coherence in Intellectual Property Law: Essays in Honour of Annette Kur* (CUP 2021).

⁵³ DSA, Rec 2 (emphasis mine).

other due diligence obligations must largely repeal them.⁵⁴ These laws may have had partly shaped the DSA, but now they must give way to it. The aspects of these laws which did not make it to the political agreement on the EU level, such as the mandatory communication of data about users in the context of criminal prosecutions,⁵⁵ must be abandoned by the Member States because the EU-wide rules now pre-empt them.

Pre-emption is easier to establish if the DSA includes some explicit rules and alternatives that were considered and rejected in the legislative process, such as an obligation to remove content on the basis of a notice.⁵⁶ The Union legislature's choice would be undermined if national laws could easily 'top-up' the DSA with additional requirements. The whole point of pre-emption is that full harmonisation constrains the policy choices of those adopted in the Union law, ie in this case, the DSA. For instance, the Portuguese government is currently considering new notification rules⁵⁷ for social media, asking them to inform the judiciary of possible crimes, which would clearly be in violation of the DSA's exhaustive and explicit rules in Article 18 DSA.

In contrast, it will be much harder to determine if some national rules are pre-empted by the DSA if such rules do not have any twins in the DSA itself. Such rules can still be pre-empted as a form of field pre-emption with the argument that the DSA is an exhaustive statement on all possible due diligence obligations for an intermediary of that type. Such silent conflicts will require clearly delineating what the DSA tries to achieve and how national law frustrates that effort. Good examples of such pre-emption are potential obligations imposed on infrastructure services.

Infrastructure providers, such as access providers or domain name authorities, are subject to only very light due diligence obligations in the DSA. For infrastructure services, the DSA lays down basic liability exemptions in Articles 4, 5, and 8, and very limited due diligence obligations in Articles 11–15 covering mostly contact points, transparency and terms and conditions. Given the increasing push for the enforcement of illegality through the infrastructure layer (eg filtering by access providers or content delivery networks) or user devices (eg client-side scanning of grooming and child abuse), this presents an essential weakness in the DSA's coverage. However, infrastructure services that qualify as intermediary services, unlike the manufacturers of smartphones, remain within the DSA's scope, and thus, potential national rules are subject to field pre-emption if they relate to trust, safety and predictability. For instance, rules

⁵⁴ Germany's Network Enforcement Law, *Netzwerkdurchsetzungsgesetz (NetzDG)* v 01.09.2017 (BGBl. I S 3352); France's Avia law, *Loi n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet*; Austria's *Kommunikationsplattformen-Gesetz (KoPl-G)* (BGBl. I Nr 151/2020). For more information on these laws, DG-CONNECT (EU Commission) and others, *Overview of the Legal Framework of Notice-and-Action Procedures in Member States SMART 2016/0039: Final Report* (EU Publications Office 2018) <<https://data.europa.eu/doi/10.2759/030261>> accessed 30 August 2023; Commission, "Impact Assessment" (Commission Staff Working Document) Accompanying the "Proposal for a Regulation of the European Parliament and of the Council on Preventing the Dissemination of Terrorist Content Online" SWD(2018) 408 final; and also partially, in Commission (n 19).

⁵⁵ Compare § 3a of the NetzDG vs Art 18 DSA.

⁵⁶ Compare § 3 NetzDG vs art 16 DSA.

⁵⁷ ANSAMed, 'Portugal Wants to Stiffen Revenge Porn Punishments' *ANSAMed* (4 October 2022) <https://web.archive.org/web/20230123102457/https://www.ansamed.info/ansamed/en/news/sections/generalnews/2022/10/04/portugal-wants-to-stiffen-revenge-porn-punishments_e0d08cf5-95e5-40af-92f8-05b0fcf27d9a.html> accessed 23 January 2023.

relating to know-your-customers or data retention would seem to be field pre-empted by the DSA. Any top-up must take place on the EU level.

As a principle, Recital 2 articulates a strong presumption in favour of field pre-emption. It effectively says that ‘unless explicitly provided for in [the DSA], if the rules are within the DSA’s remit of creating a trustworthy, predictable, and safe online environment, the DSA does not allow any specific additional solutions. Thus, the list of the DSA’s due diligence obligations for the relevant digital services should be treated as finite until the EU legislature further updates it. This leaves intact national rules adopted for reasons other than trust, safety, and predictability, such as those pursuing taxation. However, even such rules can be legislated on the national level only if they comply with the other EU rules, including the country-of-origin principle.’⁵⁸

17.5.1 Liability rules for search engines

The DSA as an EU Regulation repeals *four liability provisions* of the ECD. This means that the national implementation of Articles 12–15 ECD must be repealed by the Member States from their national law. If the Member States fail to do so, national authorities will have to set them aside anyway.⁵⁹ There is hope that an EU Regulation will bring greater uniformity to application, given that some of the national implementations often further complicate the already complex subject matter by unnecessary innovations in wording.⁶⁰ The pre-emptive effect of liability rules is the same as it was under the ECD. They continue to stop any liability for third-party information from being imposed on conduit, caching, and hosting services under the conditions spelt out by the DSA.⁶¹

Given that the ECD previously did not explicitly address the question of a liability exemption for *search engines*, and the ECD was a minimum harmonisation instrument, it remains open now under the DSA whether additional exemptions for search engines or hyperlinking services added at the national level can continue to exist. In Austria,⁶² for example, the liability exemption for search engine services and hyperlinks is modelled after the exemption for mere conduits. Bulgaria,⁶³ Portugal,⁶⁴

⁵⁸ As much as art 1(5) ECD allows the Member States to protect cultural heritage, in line with the EU law.

⁵⁹ *Simmmenthal* (n 30).

⁶⁰ Examples include the Slovak and Czech implementations, Martin Husovec, *Zodpovednosť Na Internet: Podľa Českého a Slovenského Práva* (CZ NIC 2014).

⁶¹ There was an interesting pending case before the CJEU concerning pre-emption by liability exemptions, however, it was settled before the Court had a chance to decide it. The Czech Supreme Court argues in its case law that the hosting liability exemption does not limit unfair competition law and that the outcome is not pre-empted by European copyright law. See Case C-470/22: *Hellspy SE* [2022] OJ C418/12; The context of this pending preliminary reference is explained in Martin Husovec, ‘Nekalá súťaž na steroidoch (a jej trampoty s právom EÚ)’ (30 September 2021) <<https://husovec.eu/sk/2021/09/nekala-sutaz-na-steroidoch-a-jej-trampoty-s-pravom-eu/>> accessed 25 August 2023.

⁶² S 14(1) of the Austrian E-Commerce-Gesetz (BGBl. I Nr 152/2001) (ECG) and the Austrian Supreme Court case, OHG 19 December 2005, 4 OB 194/05s.

⁶³ Art 16(4) of Bulgaria’s Law on Electronic Commerce, promulgated, SG No 51/23 June 2006, effective 24 December 2006.

⁶⁴ Art 17 of Portugal’s, Decreto-Lei n° 7/2004 de 7 de Janeiro (Electronic Commerce Law).

Romania,⁶⁵ and Spain⁶⁶ have enacted a liability exemption for search engines and hyperlinks modelled after the exemption for hosting.⁶⁷

The CJEU will need to clarify whether parts of search engines do not fall under one of the existing ones (Chapter 7). If important parts of search engines do not qualify as hosting, national experimentation with liability exemptions remains possible; however, it still remains constrained by the DSA rules for very large search engines (VLOSEs). The Member States will need to disapply those aspects of the liability exemptions that collide with the DSA's due diligence obligations for VLOSEs.

17.5.2 Accountability rules

Due diligence provisions cover a wide range of issues, including transparency, advertising, recommendation engines, disinformation, terms and conditions, content moderation processes, protection of minors, and many others. Any additional national rules can thus easily end up in the crosshairs of the DSA's due diligence obligations in Chapter 3 DSA. For very large online platforms (VLOPs) and VLOSEs, the DSA establishes fully harmonised and 360-degree rules that will likely catch everything that touches these services.

For instance, any rules intended to protect minors on platforms are likely to be in conflict with Article 28 DSA; any content moderation add-ons are likely to collide with the very prescriptive due process and transparency requirements; and many measures to avoid the spread of disinformation are likely to collide with the risk mitigation measures. Given the broad scale of challenges, it is impossible to map the entire range of conflicts in this brief outline.

Minimum harmonisation legislation that applies only to platforms allows the Member States to go beyond European rules. In particular, Article 28b(6) AVMSD establishes that 'Member States may impose on video-sharing platform providers measures that are more detailed or stricter than the measures referred to in paragraph 3 of this Article'. However, some of these rules have now been spelt out and fully harmonised by the DSA. But Recital 10 DSA makes clear that when sector-specific rules:

pursue the same objectives as those laid down in this Regulation, the rules of this Regulation should apply in respect of issues that are not addressed or not fully addressed by those other legal acts as well as issues on which those other legal acts leave Member States the possibility of adopting certain measures at national level.

⁶⁵ Art 15 of Romania's Law no 365/2002 on Electronic Commerce, published in the Official Gazette no 877 of 12 May 2001, Part 1.

⁶⁶ Art 17 of Spain's Ley N° 34/2002, de 11 de julio de 2002, de servicios de la sociedad de la información y de comercio electrónico (Act on Information Society Services and Electronic Commerce).

⁶⁷ DG-CONNECT (EU Commission) and others (n 56).

Hence, in practice, the DSA will pre-empt national action beyond Article 28b AVMSD. For instance, this will be the case for contact points⁶⁸ or measures ‘to ensure the appropriate prominence of audiovisual media services of general interest’ (Article 7a AVMSD). The DSA thus considerably eliminates the legislative wiggle room from the minimum harmonisation framework of the AVMSD (Chapter 18).

17.5.3 Content rules

One area where national parliaments retain their legislative powers is content rules. Broadly speaking, the laws defining what content or behaviour is illegal are not the subject matter of the DSA. The DSA only builds enforcement and due process machinery *if* they exist. Thus, a national rule sanctioning disinformation does not collide with procedural due diligence obligations and rather relies on the DSA to be enforced on digital services. The Member States thus enjoy broad room to define what they consider illegal. The broadest limit is compliance with fundamental rights, as such freedom of expression. The EU Charter applies to all rules that formulate illegality on the national level because they are brought into the scope of the EU law by the DSA’s enforcement layer.⁶⁹ Content rules are thus made part of the EU law thanks to the DSA, but they are not pre-empted by its rules because the DSA only exceptionally says what content should be illegal.⁷⁰

However, even the mostly procedural rules of the DSA can potentially challenge extreme substantive rules. Consider *must-carry mandates*—laws that we have seen in Florida and Texas.⁷¹ They are often politically marketed by conservatives as ‘anti-censorship rules’ trying to prevent social media from engaging in ‘cancel culture’. Their goal is usually to impose obligations on social media to carry all content that is not illegal under the law.⁷² In Europe, must-carry rules were, for instance, proposed by the Polish government in 2021.⁷³

The DSA does not have explicit rules stopping such national rules. It leaves it to the Member States to formulate what they consider illegal and, in principle, to the providers to formulate what they consider against their contractual terms. The difference

⁶⁸ For instance, in 2020, Germany adopted its ‘State Treaty on the modernisation of media legislation in Germany’, which obliges certain online platforms to have a legal representative in Germany, despite comments sent by the European Commission pointing at its incompatibility with art 3 ECD (Marc Liesching, ‘EU Kommission: Medienstaatsvertrag verstößt gegen EU-Recht’ (*beck-community*, 29 April 2020) <<https://community.beck.de/2020/04/29/eu-kommission-mediensstaatsvertrag-verstoest-gegen-eu-recht>> accessed 19 September 2023). German NetzDG also imposed an obligation to have a legal representative in Germany (art 5). Such rules now collide with arts 11–12 DSA.

⁶⁹ Case C-617/10 *Åkerberg Fransson* ECLI:EU:C:2013:105; C-648/20 *PI* ECLI:EU:C:2021:187.

⁷⁰ The only real conduct prohibition rules are art 25 (dark patterns), art 26(3) (on profiling in advertising using sensitive personal data), and art 28(2) (on profiling of minors in advertising using their personal data).

⁷¹ Valerie C Brannon, ‘Free Speech Challenges to Florida and Texas Social Media Laws’ (Congressional Research Service 2022) <<https://crsreports.congress.gov/product/pdf/LSB/LSB10748>> accessed 30 August 2023.

⁷² Tech Against Terrorism, ‘The Online Regulation Series: Poland’ (16 November 2021) <<https://www.techagainstterrorism.org/2021/11/16/the-online-regulation-series-poland/>> accessed 30 August 2023.

⁷³ *ibid.*

between the US and EU debate on must-carry mandates is that much more content seen as objectionable is also illegal in the EU Member States. Due to the experience with the Holocaust, the states in Europe are less willing to leave the regulation of speech issues to the rules of communities and private actors. Thus, the typical US examples, such as non-violent hate speech or extremist content,⁷⁴ would qualify as illegal content in many of the Member States.⁷⁵ As such, the content that is ‘awful but lawful’ in the US, is often simply unlawful in the EU. Must-carry mandates thus effectively require much less content to be ‘up’ in Europe than they would require in the US. However, even in Europe, such laws could still require vulgar content, spam, nude content, self-harm content, or other borderline content to never be moderated by the targeted providers.

From the pre-emption standpoint, a big question is whether such must-carry mandates could violate any of the provisions of the DSA. In my view, they could violate the spirit of Article 14 DSA which envisages that the providers keep contractual freedom to formulate content moderation rules but be obliged to engage in a balancing of fundamental rights. Because must-carry rules are a blanket ban on many private content moderation rules, they will likely have problems surviving the scrutiny of Article 14 DSA. Must-carry mandates do not enable any moderation of lawful content by the provider according to its preferences because they ban it entirely. Thus, they undermine the idea of balancing by imposing the government’s view on all content moderation policies.⁷⁶

Finally, any content rules still need to potentially face the country-of-origin principle and notification rules. However, the specificity of content rules is that they usually do *not* regulate information society services providers. They regulate the *users* of such services. Users are not subject to the country-of-origin or transparency rules unless they implicate the freedom of their providers to provide a service.⁷⁷ This is clear from *Airbnb Ireland*,⁷⁸ under which regulation of users can also indirectly mean regulation of the provider and their services. Thus, many content rules will not be slowed down by the country-of-origin principle or notification rules.

As an ultimate backstop, any rules concerning illegality are still subject to the TFEU’s free movement of services and the EU Charter. For example, bans on advertising of abortion-related services, sugary drinks to children, or videos depicting animal cruelty can be reviewed from the perspective of the primary EU law.

⁷⁴ Daphne Keller, ‘Lawful but Awful? Control over Legal Speech by Platforms, Governments, and Internet Users’ (*The University of Chicago Law Review Online*, 28 June 2022) <<https://lawreviewblog.uchicago.edu/2022/06/28/keller-control-over-speech/>> accessed 30 August 2023.

⁷⁵ For the latest consensus understanding of hate speech, the Council of Europe, ‘Recommendation CM/Rec(2022)16 of the Committee of Ministers to member States on combating hate speech (Adopted by the Committee of Ministers on 20 May 2022 at the 132nd Session of the Committee of Ministers)’.

⁷⁶ See on must carry in the DSA, the Court of Amsterdam, *Baudet/Google (YouTube)*, Case No ECLI:NL:RBAMS:2021:5117, para 4.8 ([‘must-carry’] an obligation is also not included in the (European) proposal for the Digital Services Act (the Digital Service Act)).

⁷⁷ If the rules applicable to users are used to indirectly restrict the provision of services (eg imposing liability for failure to remove), such rules would fall under the country-of-origin and notification rules.

⁷⁸ *Airbnb Ireland* (n 8).

17.4.4 Other gaps in the DSA

Apart from *content* rules, national regulation is most feasible after the DSA in the following areas:

- regulation of services that are *outside* the DSA's scope;
- regulation of *super-users*, such as influencers, politicians, and news organisations; and
- regulation of *orders*, including those requested by individuals, such as account-blocking or disclosure orders.

Despite its horizontal nature and comprehensiveness, the DSA has some blind spots. Activities that do not qualify as intermediary services (Chapters 2 and 9) can be exposed to more national experimentation, even if they are crucial for the digital ecosystem. This includes the regulation of goods or services that are not information society services, such as smartphones or computers, and services that are information society services but not intermediary services, such as payment services.

Another gap is the regulation of *super-users*, such as influencers, and trusted content creators, such as journalists, academics, and others, who are not offered stronger protections, although they might need them. While they are indirectly regulated by provisions on advertising, and misleading and abusive practices, this is only to a limited degree. It is, therefore, not surprising that the French legislature adopted a new law on influencers only several months after the DSA.⁷⁹ As of writing, the EU's European Media Freedom of Act is trying to address the situation of news organisations as a type of trusted content creators.⁸⁰ Such rules are generally compatible with the DSA. However, if such rules veer into obligations that influence the freedom of providers to provide services (eg an obligation to only use platforms that conform to certain qualities), they could be scrutinised as rules targeting digital services.

By far, the biggest and most obvious gaping holes of the DSA are *individual orders* issued by national authorities. The DSA, as the ECD before, only foresees such power of national authorities, but the only limit it imposes on them is the prohibition of general monitoring. The safeguards and contestation process for such orders remain entirely up to the national law. Except for Articles 9 and 10, there are no mandatory minimum requirements for such processes. While the underlying content rules being enforced could probably be scrutinised for their compatibility with the EU Charter, the orders are mostly given free rein.

The Member States thus largely preserve their competence to issue individual orders against conduits, caching, and hosting providers. This means that a wide range of

⁷⁹ Simone Shah, 'France is Cracking Down on the Influencer Industry' (*Time*, 8 May 2023) <<https://time.com/6277524/france-influencer-marketing-regulation-social/>> accessed 30 August 2023.

⁸⁰ Martin Husovec, 'Trusted Content Creators' [2022] LSE Law School Policy Briefing Paper No 52 <<https://ssrn.com/abstract=4290917>> accessed 30 August 2023.

orders is potentially permitted: content removal orders, evidence-preservation orders, blocking orders, identification orders, decryption orders, detection orders, and so on. These measures are, however, importantly regulated by liability exemptions, prohibition of the general monitoring obligations, and the ECD's country-of-origin principle.

If the Member States comply with these requirements, they can set up their own authorities and empower them to issue blocking or other orders in the national law. This has been a practice in intellectual property law where some Member States, such as Italy, granted powers to their national authorities to issue such orders.⁸¹ In Germany, for instance, there is a proposal on the ability to create a new type of account-blocking order in hate speech.⁸²

The attentive national legislatures will surely try to find other DSA gaps. For this reason alone, the DSA should be understood as a baseline standard, not as the only exhaustive standard of protection. In the coming years, we can expect a flurry of sectorial legislation building on top of the DSA from the EU legislatures, experiments by national legislatures, and new co-regulatory schemes developed based on the DSA's main framework. It is my expectation that co-regulatory schemes under the DSA are more likely to become the blueprints for legislative proposals on the EU level than national experiments.

17.6 Conclusion

The DSA will not be the last word on the regulation of digital services. If anything, it is rather the beginning. In the coming years, one of the challenges will be to keep national and European legislation coherent.

The parliaments of the Member States will not have it easy. In recent years, national attempts to legislate on digital services in the EU started looking very much like racing through an obstacle course. The participants, in our case, national legislatures, are presented with barriers of increasing difficulty, such as crawling in the mud (notification requirements) and barbed wire (pre-emption). The only winners are those who successfully overcome them thanks to the necessary training, those who are not worn down by the arduous course.

A positive side-effect of this architecture is that it acts as a specific check on the extremist politics of the Member States. By regulating actors in the digital ecosystem, the Union law also protects against misuse of power on the national level. The DSA partly binds the hands of extremist governments that want to engage in politically motivated attacks on providers or users. It allows providers to switch countries (and thus

⁸¹ EUIPO and CEIPI, *Study on Dynamic Blocking Injunctions in the European Union* (EUIPO 2021) <<https://op.europa.eu/s/yX4r>> accessed 21 August 2023.

⁸² Gesellschaft für Freiheitsrechte eV (GFF), 'Accountsperren als Hebel gegen Hass im Netz – Gesellschaft für Freiheitsrechte stellt Eckpunkte für Digitales Gewaltschutzgesetz vor' (13 December 2022) <<https://freiheitsrechte.org/ueber-die-gff/presse/pressemitteilungen-der-gesellschaft-fur-freiheitsrechte/pm-eckpunkte-gewaltschutzgesetz>> accessed 30 August 2023.

regulators), out-of-court dispute settlement bodies or trusted flaggers to choose the place of their certification, and consumer groups the forum for their enforcement actions. Thus, the geographical and institutional spread of the DSA institutions adds to the system's resilience. However, because the orders of authorities were left largely outside the DSA's scope, and content rules were not explicitly regulated either, the DSA's protection against extremist governments is far from complete.

The DSA as a Digital Rights Charter

18.1 Introduction	391	18.4.2 Right to be delisted	405
18.2 Piecing Together the Big Picture	392	18.5 Audiovisual Media Regulation	407
18.3 Copyright Law	396	18.6 Platform to Business Regulation	410
18.3.1 Article 17 CDSMD and hosting	397	18.7 Terrorist Content Regulation	413
18.4 Data Protection Law	401	18.8 Conclusion and Outlook	415
18.4.1 Controllers and hosting service providers	402		

18.1 Introduction

The Digital Services Act (DSA) has an integrating character. Due to its horizontal approach and broad applicability, its effects potentially ripple through many other parts of the legal system. In this chapter, I show how the DSA *lifts* the standards of protection of fundamental rights, especially of due process and freedom of expression, across the various sectorial laws, sometimes in unexpected ways. I discuss five examples of sectorial rules whose protection of the rights of individuals ranges from ‘DSA-suboptimal’ to ‘DSA-exceeding.’ With concrete examples, I show that the ‘DSA-suboptimal’ rules—such as special liability of online content-sharing services in copyright law and the right to be delisted under the General Data Protection Regulation (GDPR)—can have their standards of fundamental rights lifted to the DSA levels. I will also show that ‘DSA-exceeding’ rules—such as the Terrorist Content Regulation (TCR)—remain untouched in their special set of higher mandatory safeguards.

The uplifting effect of the DSA is a result of standard interpretative methods being applied to the question of how the DSA relates to other pre-existing laws. For the future European Union (EU) laws, the effect is more political because the DSA creates horizontal expectations of the minimum level of rights. Since the Member States cannot deviate from these rights, why should the EU legislature? Thus, although the EU legislature can, in theory, suspend the rights acquired by the DSA, doing so requires extra-political justification. Politically and legally, the DSA is likely to become an *EU digital rights charter*. As pointed out in Chapter 17, this charter is not without gaps that the Member States might exploit. However, it is a start. The effect of the DSA as the EU digital rights charter can be depicted as shown in Figure 18.1.

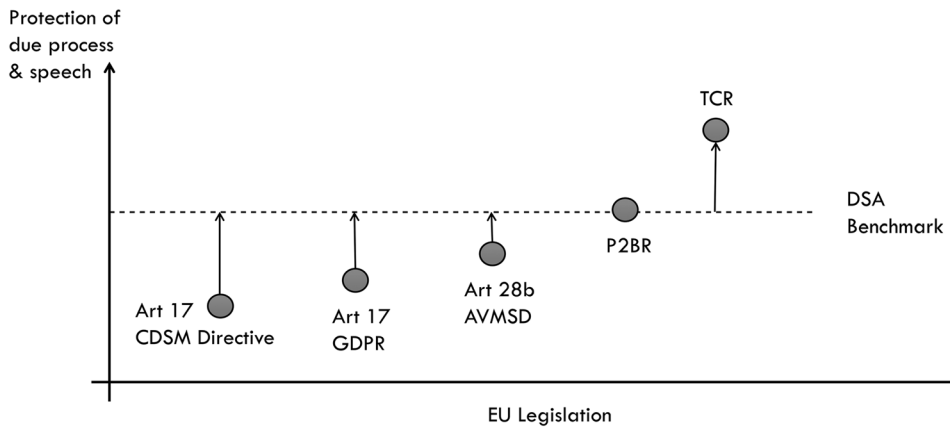


Figure 18.1 The DSA as a Digital Rights Charter

18.2 Piecing Together the Big Picture

The legal system is a curious creature of human architecture. It is so complex that no one usually understands how all the pieces fit together when designed in the fervour of the legislative debate. Thus legislative drafters, and especially those of very broad pieces of legislation, rarely foresee how their laws will interact with the pre-existing rules.

During the fast-paced legislative process, the EU Member States posed countless questions on the relationship of the DSA with the other EU or national laws.¹ Many wondered about unforeseen effects. The European Parliament even wanted an amendment requiring the Commission to publish guidelines about the relationship between the DSA and the other legal acts.² However, as attractive as this idea may seem at first, this would have been inappropriate. An executive-powers body cannot ex post construe how the new piece of legislation affects other existing legislation. Ultimately, only the Court of Justice of the European Union (CJEU) can provide such guidance. And even the CJEU can really only provide such an interpretation when concrete problems come before it for adjudication—some of which we can foresee but many we cannot.

Article 2(4) DSA includes a *non-exhaustive list* of instruments of the EU law which could conflict with the rules under the DSA. It states that: '[t]his Regulation is without prejudice to the rules laid down by other Union legal acts regulating other aspects of

¹ Presidency of the Council of the European Union, 'Digital Services Act: Presidency Selection of Questions Sent by Member-States on Chapter I and II' (2021) Document WK 2289/2021 INIT <<https://councildsa.reset.tech/pdf/wk02289.en21.pdf>> accessed 6 September 2023.

² European Parliament, 'Amendments Adopted by the European Parliament on 20 January 2022 on the Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and Amending Directive 2000/31/EC (COM(2020)0825 — C9-0418/2020 — 2020/0361(COD))' [2022] OJ C336/48, art 1a(4) ('By [12 months after the entry into force of this Regulation] the Commission shall publish guidelines with regard to the relationship between this Regulation and the legal acts referred to in Article 1a [3]').

the provision of intermediary services in the internal market or specifying and complementing this Regulation’ and sets out a long illustrative list of such instruments.

But what does the ‘without prejudice’ clause mean in practice?

The EU’s interinstitutional style guide³ describes the meaning of ‘sans que soit affecté’ (French for ‘without prejudice’) as ‘indépendamment de’. The clause ‘without prejudice’ thus tries to ensure no incidental or unintended amendment of the existing legal acts, which are left intact and unaffected by the new legislation. It does *not* mean the listed instruments ‘always prevail’ or are ‘carved out’ from the new legislation. Where two instruments apply because they overlap, they both potentially apply to the same actors under their own autonomous conditions.

The DSA generally uses the clause to communicate the relationship with other subject matter areas. On the most fundamental level, the clause states that those other areas of law remain *unaffected* and should be *interpreted in harmony* with the new piece of law. The without prejudice clause is not strictly a conflict of norms rule; it merely means that both sources should coexist and are not affected. The clause usually serves the Court as a way to avoid conflict and synchronise interpretation across various legal instruments.

An interpretative problem only arises if two provisions conflict. In such cases, it needs to be determined which one is the *lex specialis*—the more specific and detailed law, and which is *lex generalis*—the law backed by less specific legislative intent. If there is no conflict, both laws will apply in a complementary manner.

Recital 10 explains what ‘without prejudice’ actually means in the context of the DSA:

This Regulation should be without prejudice to other acts of Union law regulating the provision of information society services in general, regulating other aspects of the provision of intermediary services in the internal market or specifying and complementing the harmonised rules set out in this Regulation ... However, to the extent that those Union legal acts pursue the same objectives as those laid down in this Regulation, the rules of this Regulation should apply *in respect of issues that are not addressed or not fully addressed by those other legal acts* ...⁴

The DSA thus leaves untouched other EU acts that do not follow the same objectives, even if they regulate the same actors. For instance, the NIS2 Directive⁵ includes rules for the cybersecurity of digital services that operate ‘essential services’, such as online marketplaces, search engines or cloud computing spaces, but only to achieve ‘a high common level of security of network and information systems’ and keep users informed when there are cybersecurity incidents. The GDPR applies to any intermediary

³ The EU Interinstitutional Guide, Annex C: Miscellaneous, but only in its French version: European Union, ‘Code de Rédaction Interinstitutionnel—Annexe C—Divers’ (*Office des publications*) <<https://publications.europa.eu/code/fr/fr-5020100.htm#prejudice>> accessed 17 September 2023.

⁴ DSA, Rec 10 (emphasis mine).

⁵ European Parliament and Council Directive (EU) 2022/2555 on measures for a high standard level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 [2022] OJ L333/80 (NIS2 Directive).

when it acts as a data controller, not as an intermediary that merely enables data control by others. However, just because these two areas do not touch does not mean that the DSA's effect of lifting the standard of protection will not take place. On the contrary, as argued below, such effects are likely.

Article 89 DSA 'transplants'⁶ the liability regime from the E-Commerce Directive (ECD) to the DSA by deleting Articles 12–15 from the ECD and reintroducing them in the DSA (Chapter 6). Any reference to those articles must be understood as a reference to the corresponding provisions of the DSA.⁷ However, while the ECD is a Directive which requires transposition into national law with certain variations, the DSA is a directly applicable and fully harmonising Regulation. Some of the instruments of EU law that contain the phrase 'without prejudice to Articles 12–15 ECD' are also included by the DSA in its 'without prejudice' clause under Article 2(4). Together, they create what Roche Laguna calls a 'without prejudice loop'⁸ whereby the DSA applies 'without prejudice' to them, and they apply without prejudice to the ECD or the DSA.

An example of this can be seen with respect to the Audiovisual Media Directive (AVMSD):

- 1) the DSA applies without prejudice to AVMSD (Article 2(4)(a) DSA);
- 2) the AVMSD applies as *lex specialis* to the rules under the ECD (Article 4(7) AVMSD);⁹
- 3) Article 28b AVMSD applies 'without prejudice' to Articles 12–15 ECD (Article 28b(1) AVMSD).¹⁰

The first provision (1) sends the message that the DSA will not affect the AVMSD and will continue to apply to the extent that the AVMSD does not specify or complement the DSA. Where the AVMSD goes beyond the DSA or establishes more specific rules, the latter will apply. Under the second provision (2), the AVMSD intends to send the

⁶ Interview with Irene Roche Laguna, Deputy Head of Unit for Coordination and Regulatory Compliance, European Commission (2021–23).

⁷ Many other instruments of Union law, the case law of the CJEU, and national laws and court decisions make reference to arts 12–15 ECD. Art 89(2) DSA makes it clear that such cross-references now have to be construed as referring to arts 4–6, and 8 DSA. Examples include: Data Governance Act (Rec 3); TCR (arts 1(5) and 5(8), Recs 7 and 25); Terrorism Directive (Rec 23); Proposal for Regulation (EU) 2019/1148 on marketing and use of Explosives precursors (Rec 12); the Market Surveillance Regulation (art 2(4) and Recs 16, 41, and 42); GDPR (art 2(4) and Rec 21); AVMSD (art 4(7) and Rec 25); Regulation 2020/740 on tyres (art 8); Directive (EU) 2018/1972 establishing EECC (art 12 ECD applies to radio local area networks (RLANs)); in the field of copyright and IP rights, both the InfoSoc Directive 2001/29/EC and IP Enforcement Directive 2004/48/EC, apply 'without prejudice' to the liability provisions under the ECD; however, the CDSM Directive carves out certain services, under certain conditions, from the protection under art 14 ECD; Omnibus Directive (EU) 2019/2161 for modernisation of consumer protection rules; Delegated Regulations 2019/2013, 2019/2014, 2019/2015, 2019/2016, 2019/2018, and 2019/945 on labelling of products (supplementing Regulation (EU) 2017/1369 setting a framework for energy labelling).

⁸ Interview with Irene Roche Laguna (n 6).

⁹ European Parliament and Council Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services [2010] OJ L 95/1, as amended by Directive (EU) 2018/1808 (AVMSD), art 4(7): 'Directive 2000/31/EC shall apply unless otherwise provided for in this Directive. In the event of a conflict between Directive 2000/31/EC and this Directive, this Directive shall prevail, unless otherwise provided for in this Directive.'

¹⁰ *ibid.*

same message as regards the ECD, including the substantive rules (rules on commercial communications, country of origin principle, information requirements, etc). The AVMSD is the *lex specialis*, and the ECD is the *lex generalis*. This also covers the new rules introduced by the 2018 amendment to the AVMSD on ‘video-sharing platforms’ in Articles 28a and 28b.¹¹ The amendment introduces specific jurisdictional rules and material obligations for video-sharing platforms, which were clearly meant to be more specific than the very general rules under the ECD. Finally, the third provision (3) explains that some specific material obligations cannot deviate from the liability exemption that protects video-sharing platforms, which can benefit from the hosting liability exemption.

The outcome of this complicated web of cross-references is ultimately the same as if there were no without prejudice clauses. That is, the AVMSD cannot amend the ECD, the DSA cannot amend the AVMSD, and the AVMSD cannot deviate from the DSA. Each legislative act and its provisions are a piece of jigsaw that must fit together undistorted, producing a coherent picture.

Because only the EU legislature can deviate from secondary EU law, to ensure legal certainty, the Union legislator is expected to be explicit as regards any real amendments. Otherwise, difficulties will arise when two colliding instruments must be interpreted in a consistent and harmonious manner. EU law already knows explicit derogation from some of the provisions of the DSA (eg Article 17 Copyright in the Digital Single Market (CDSM) Directive).¹² But without the legislature’s explicit will, secondary EU legislation cannot deviate from the standard of fundamental rights protection envisaged by the DSA, including its principles.

To interpret the DSA and its relationship with the other EU acts, the regular tools of statutory interpretation apply, such as grammatical, historical, systemic, and teleological arguments.¹³ This chapter does not offer any new methodology. Instead, it tries to typify the situations the DSA will likely encounter in practice. In practice, there are the following main scenarios:

- *Parallel application*: the rules of the DSA and the other instruments *do not overlap* and apply in parallel. The DSA applies in its area of application without any changes; the same is true for the other instruments of EU law. For instance, much of the GDPR applies parallel to the DSA when regulating digital services because it regulates very different aspects of services.
- *Complementary application*: the rules of the DSA and the rules of the other instrument *overlap* but also *do not collide* in substance. The DSA then applies as *lex generalis* because it offers horizontal solutions to an area and issue not signalled

¹¹ European Parliament and Council Directive (EU) 2018/1808 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (AVMSD) in view of changing market realities [2018] OJ L 303/69.

¹² DSA, art 89(2).

¹³ Koen Lenaerts and José A Gutiérrez-Fons, ‘To Say What the Law of the EU is: Methods of Interpretation and the European Court of Justice’ (2013) Working Paper EUI AEL 2013/09, Distinguished Lectures of the Academy <<https://cadmus.eui.eu/handle/1814/28339>> accessed 17 September 2023.

for special treatment by the EU legislature. For instance, for all hosting services except those which qualify as ‘online content-sharing services’, the DSA complements copyright liability under EU copyright law.

- *Deviant application*: the rules of the DSA and the other instruments *overlap* and *collide* on substance. The DSA, in such cases, cedes to the other (often sectorial) EU law instruments insofar as they are more specific or contain a different answer to the same question. For instance, the Platform to Business Regulation (P2BR) includes special rules for some online platforms and search engines.

Most rules applicable to digital services will be in the camp of parallel application. Some important subsets will benefit from the DSA’s complementary application. Only a very small group of specific rules is likely to be singled out for deviant application by sector-specific rules. In the following sections, the most illustrative overlaps will be identified and explained.

18.3 Copyright Law

No area has such an intense relationship with the DSA as copyright law. This was already obvious during the making of the ECD and its copyright companion, the Information Society (InfoSoc) Directive.¹⁴ The three crucial points of interaction are: a) the right to communication to the public (Article 3 InfoSoc Directive), injunctions against intermediaries (Article 8(3) InfoSoc Directive),¹⁵ and the reform from 2019 which decided to suspend the application of the hosting liability exemption to certain online content-sharing service providers (Article 17 Copyright in the Digital Single Market (CDS Directive), such as video-sharing platforms.¹⁶ Through discussion of these examples, I hope to show how the DSA continues to frame and influence the copyright framework and generally lifts the standard of fundamental rights protection.

The CJEU has so far managed to navigate and synchronise these various pieces of EU law. In its case law, the Court meticulously tries to fit parts of the jigsaw together. In terms of liability, the case law concerning communication to the public was brought in line with the hosting liability exemption criteria. The CJEU’s interpretation of the InfoSoc Directive in *YouTube and Cyando*¹⁷ does not conflict with a horizontal reading of liability exclusion and tries to model the liability around it (Chapter 7). This ensures that platforms hosting third-party content involving copyrighted material are liable *only* when liability exemptions do not apply or are subsequently lost (eg due to an effective notification).

¹⁴ European Parliament and Council Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society [2001] OJ L167/10 (InfoSoc Directive)

¹⁵ InfoSoc Directive, Rec 16.

¹⁶ European Parliament and Council Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC [2019] OJ L130/92 (CDSM Directive), art 17.

¹⁷ Joined Cases C-682/18 and C-683/18 *Frank Peterson v Google LLC and others and Elsevier Inc v Cyando AG* ECLI:EU:C:2021:503.

The more interesting question concerns how the DSA's due diligence obligations will continue to shape future case law. The Court in *YouTube and Cyando* came up with an evidentiary standard to outline when a provider is a rogue player that acts in concert with infringers (Chapter 7).¹⁸ This case law clearly inspired co-legislators when modifying Recital 20 of the DSA. The DSA's transparency requirements will likely offer additional points of evidence to feed into such evidentiary standards. Similarly, the Court's expansion of communication to the public right will now be surrounded by safeguards to prevent over-blocking or other types of abuse. Thus, the DSA is very likely to inform much of the upcoming copyright case law as a benchmark. This is also stressed by Article 2(4) DSA as explained by Recital 11, which stipulates that: 'It should be clarified that this Regulation is without prejudice to Union law on copyright and related rights, including Directives 2001/29/EC, 2004/48/EC, and (EU) 2019/790 of the European Parliament and of the Council, *which establish specific rules and procedures* that should remain unaffected'.¹⁹

The same can be said about injunctions. Injunctions against intermediaries based on the Enforcement²⁰ and InfoSoc Directives are continuously brought in line with the prohibition of general monitoring and injunction clauses (Chapter 8). Arguably, the CJEU broadly managed to navigate the complicated legal landscape by fitting these pieces of the puzzle together.²¹ Thus, website blocking or other measures were scrutinised for compatibility, and sometimes shaped into a form in which they can be granted by national courts. The DSA will now sometimes offer safeguards against potential abuse of such measures, thus giving the Court an opportunity to highlight how to achieve better enforcement and maintain effective safeguards against its abuse.

18.3.1 Article 17 CDSMD and hosting

By far, the most controversial interface between the DSA and copyright is regulating online content-sharing services. Article 17 CDSMD Directive represents the only, and so far the most drastic, divergence from the horizontal liability exemption system. The regime, introduced by the EU legislature in 2019 in response to remuneration concerns arising from certain online video-sharing services, imposes strict liability to encourage licensing for the content posted by users.

All 'online content-sharing service providers' are, by definition, hosting services and online platforms. These services, unlike others in the ecosystem, cannot avoid seeking licenses for the content that users can upload. In case they fail to obtain a licence from a typical set of actors, they bear the liability for users' content unless they can show that

¹⁸ *ibid* para 44.

¹⁹ Emphasis mine.

²⁰ European Parliament and Council Directive 2004/48/EC on the enforcement of intellectual property rights [2004] OJ L 157/45

²¹ Martin Husovec, *Injunctions against Intermediaries in the European Union: Accountable but Not Liable?* (CUP 2017).

they also took best efforts to mitigate the presence of unauthorised content on its platform, including through automated means, following a request to do so.²²

This obligation under Article 17 CDSM Directive would not have been otherwise possible under the DSA because the input for automated recognition comes from private actors and is not overseen by authorities (Chapter 8.3). The DSA, unless its rules are suspended and overridden by the specific EU legislation, allows only ‘order and staydown’ regimes as opposed to ‘notice and staydown’ regimes.²³ In both cases, the expectation is that the same content is prevented from reappearing; however, in the former case, the obligation to do so can be only triggered by a decision of an authority, while in the latter can also be done by a private request.

Article 17 CDSM Directive is a clear case of a *lex specialis* liability regime. Its importance is hard to overstate. In the 22 years since the ECD, it has been the *only* permissible liability regime for platforms that takes a form of strict liability for users’ non-editorial content. By virtue of Article 6 DSA, none of the Member States is allowed to introduce anything similar. The EU legislature itself would have to explicitly derogate from Article 6 of the DSA again (and thus modify it) to do the same again.

Despite its specific position, Article 17 CDSM Directive regime is not immune to due diligence obligations legislated in the DSA.²⁴ These provisions are horizontal and often complement sectorial law. The DSA thus complements and thereby reinforces the mechanisms under the CDSM Directive while not affecting their special status. Below, I offer some examples.

As regards *notice requirements*, notifications are much less relevant in the special regime of Article 17 CDSM Directive. Article 16 DSA will not directly apply to copyright notices envisaged by Article 17(4)(c) CDSM Directive for scenarios where no licence is given and the right holder did not ask for preventive measures. Article 16 DSA will, however, continue to apply to hosting services providers not covered by Article 17 CDSM Directive or those covered by its *de minimis* clause under Article 17(6) CDSM Directive.²⁵ Nevertheless, the differences in language are not dramatic. Article 17 CDSM Directive requires the notice to be ‘sufficiently substantiated’, while the DSA refers to ‘sufficiently precise and adequately substantiated notices’. The language in Article 17(4)(c) of the CDSM Directive is borrowed from the existing case law of the CJEU that interprets the hosting liability exemption. In the Guidance on Article 17 CDSM Directive, ‘the Commission recommends the Member States to follow in their implementation the Commission Recommendation on Measures to Effectively

²² Martin Husovec and João Pedro Quintais, ‘How to License Article 17? Exploring the Implementation Options for the New EU Rules on Content-Sharing Platforms under the Copyright in the Digital Single Market Directive’ (2021) 70(4) *German Association for the Protection of Intellectual Property International* 325.

²³ They must be, however, compliant with other provisions of the DSA, such as the prohibition of general monitoring, see ch 5.

²⁴ João Pedro Quintais and Sebastian Felix Schwemer, ‘The Interplay between the Digital Services Act and Sector Regulation: How Special is Copyright?’ (2022) 13(2) *European Journal of Risk Regulation* 191.

²⁵ Art 17(6) of the CDSM Directive provides a specific liability regime with different conditions for ‘new’ companies, which have been active in the EU for less than three years and have an annual turnover of less than €10 million.

Tackle Illegal Content Online²⁶—a recommendation that acted as a blueprint for the DSA. Thus, while Article 16 DSA is not applicable, the interpretation of Article 16 DSA and Article 17(4)(c) CDSM Directive is unlikely to differ.

The DSA equally harmonises *other aspects of content moderation*, which are not addressed or not fully addressed by Article 17 CDSM Directive. These rules will contribute to ensuring the appropriate use and efficient processing of notices and greater transparency for users.

The obligation for hosting services is to provide a *statement of reasons* to recipients of the services in the case of removal or disabling access to content, among others (Article 17 DSA). As the CDSM Directive remains silent in this regard, one can safely conclude that Article 17 DSA also applies within this special regime and will enhance user rights, due process, and transparency around removals, regardless of whether they are based on notices or automated tools. For instance, all these statements of reasons, including those based on automated filtering decisions, would be publicly available under a database managed by the Commission (Article 24(5) DSA), and the precision of algorithmic systems must be reported even by providers that are not ‘very large on-line platforms’ (VLOPs) (Article 15(1)(e) DSA).

The *internal redress mechanism* will be greatly upgraded too. Article 17(9) CDSM Directive mandates Member States to ‘provide that online content-sharing service providers put in place an effective and expeditious complaint and redress mechanism that is available to users of their services in the event of disputes over the disabling of access to, or the removal of, works or other subject matter uploaded by them.’ It further requires such complaint mechanism to allow for rightsholders to ‘duly justify the reasons for their requests’ (Recital 70 CDSM Directive). Finally, complaints need to be processed ‘without undue delay’, and the removal decisions need to be subject to ‘human review’ (Article 17(9) CDSM Directive).

The (non-binding) Guidance of the European Commission further considers that ‘the content should stay down during the human review performed under the redress mechanism,’ except for content which is not manifestly infringing.²⁷ The DSA, instead, lays down more detailed procedural rules in Article 20, asking for a timely, non-discriminatory, diligent, and non-arbitration decision. It requests for the content to be *reinstated* in case of a successful complaint against a removal. It obliges platforms to inform complainants about their decision and about any redress avenue, and finally requires complaints to be dealt with by humans, and appropriately qualified staff. These provisions do not conflict with the CDSM Directive and are likely to only strengthen the Court’s call for fundamental rights compliant transpositions.

The *out-of-court dispute settlements* in the two instruments also have overlapping and mutually reinforcing rules. The CDSM Directive mandates the Member States to ‘ensure that out-of-court redress mechanisms are available for the settlement of

²⁶ Commission, ‘Guidance on Article 17 of Directive 2019/790 on Copyright in the Digital Single Market’ (Communication) COM(2021) 288 final.

²⁷ *ibid* 24.

disputes. Such mechanisms shall enable disputes to be settled impartially and shall not deprive the user of the legal protection afforded by national law, without prejudice to the rights of users to have recourse to efficient judicial remedies' (Article 17(9) CDSM Directive). Article 21 DSA, on the other hand, establishes a fully-fledged mechanism with many more details than the CDSM Directive: a time limit for settlement, specific requirements for out-of-court bodies (that will be enforced by the country of origin of the body), the possibility to revoke a body if it does not act independently, fee structures for the decisions, and follow-up after their decisions are made.

The obligation under the DSA is more specific and a more single-market-friendly solution. However, the DSA does *not* require the Member States to set up out-of-court dispute settlement bodies, unlike the CDSM Directive. If Article 21 DSA is understood as the full harmonisation of Article 17(9) CDSM Directive, then the Member States would be required to fund one of such bodies if there is no provider on the market for disputes within the scope of Article 17 CDSM Directive.

The CDSM Directive remains silent on the concept of *trusted flaggers*. However, rightsholders can also benefit from the status of trusted flaggers under the DSA if they meet the envisaged requirements, and hence from the priority treatment of their notices, provided that they meet the relevant requirements. However, this has limited usefulness for Article 17 CDSM Directive, as its main goal is to move away from the notice and takedown regime. The only situation where trusted flaggers can add value is under scenarios of Article 17(4)(c) CDSM Directive. In my view, this remains possible, and it also supports the point that Article 16 DSA and Article 17(4)(c) CDSM Directive should be interpreted in harmony.

The CDSM Directive does not contain any specific *rules to protect against misuse*, such as safeguards to avoid misuse by rightsholders who repeatedly use the mechanism to report lawful content. It merely prohibits any cooperation between online content-sharing service providers and rightsholders which results in the prevention of the availability of lawful works, for instance where a copyright exception or limitation covers them (Article 17(7) CDSM Directive). The Court has interpreted this prohibition as an obligation of result.²⁸ Hence, the obligation under Article 23(2) DSA, where online platforms must suspend the processing of notices from notifiers who repeatedly submit manifestly unfounded notices, will only reinforce the purpose of Article 17(7) CDSM Directive. Furthermore, Article 23(1) DSA also contributes to the goal of Article 17 CDSM Directive to impede access to unauthorised works by obliging platforms to suspend users who repeatedly upload manifestly infringing content. It is clear that Article 23 DSA will apply on top of Article 17 CDSM Directive and will reinforce its goals. A notifier who repeatedly submits rogue notices and is suspended on the basis of the DSA should not be able to submit notices under Article 17 CDSM Directive.

Finally, the CDSM Directive imposes limited *transparency obligations* to online content-sharing service providers and only vis-à-vis rightsholders. Article 17(8)

²⁸ Case C-401/19 *Republic of Poland v European Parliament and Council of the European Union* ECLI:EU:C:2022:297, para 78.

CDSM Directive applies only at the request of right holders and concerns the practical application of Article 17 CDSM Directive. The Guidance on Article 17 CDSM Directive further encourages, in a non-binding manner, regular reports on the content blocked as a result of the application of automated tools. It considers that such reports would provide public oversight on the application of Article 17 and will allow user organisations to ‘monitor and contest the application of parameters defined by service providers in cooperation with rightsholders to detect systematic abuses.’²⁹ To do so, it cross-refers to the DSA as the right approach.³⁰

The DSA will impose several *transparency reporting obligations* that will lead to more transparency on using automated tools, notices and the treatment of complaints by online platforms, including those covered by Article 17 CDSM Directive. More transparency will also be required from intermediary services regarding the actions taken in relation to copyright-protected content (eg information on notices and orders received, including the median time for taking action). These obligations are much more specific than the CDSM Directive. Therefore, they should be seen as complementary. The same applies to the DSA obligation under Article 24(5) to send the statements of reasons for Online Content Sharing Service Providers (OCSSP) decisions made under Article 17 CDSM Directive to the public database managed by the Commission. The rule’s application once again mutually reinforces the goals of the two regimes. Such enhanced transparency requirements will benefit rights holders, who gain more transparency on how their rights are enforced, and users, who gain information about using automated tools for content moderation.

For VLOPs and very large online search engines (VLOSEs), Article 34 DSA includes assessing the risk of disseminating of illegal content, including copyright infringements and implementing mitigation measures to avoid such risks. This obligation is clearly complementary and not contradictory to Article 17 CDSM Directive.³¹ This means auditing filtering tools for their compliance with Article 17’s goals and for potential over-blocking effects. However, the obligation cannot have the effect of extending Article 17 beyond its reach due to the CDSM Directive’s *lex specialis* status.

In conclusion, the above discussion of the interplay between the CDSM Directive supports the thesis that the DSA is likely to have an uplifting effect on the protection of fundamental rights online.

18.4 Data Protection Law

The ECD originally included a separate provision excluding the application of the ECD to questions relating to InfoSoc services governed by data protection rules.³² This

²⁹ Commission, ‘COM(2021) 288 Final’ (n 26) 23.

³⁰ *ibid* 23, fn 36.

³¹ On the other hand, the notice and stay-down effect of notices under art 17 CDSM Directive should not be taken as a mitigation measure by analogy, as this regime has special authorisation from the statute.

³² ECD, art 1(5).

provision was accompanied by a recital stating that ‘the processing of personal data is solely governed’ by the former respective EU directives and that they remain ‘fully applicable to information society services’.³³ However, the GDPR in 2016 established that ‘this Regulation shall be without prejudice to the application of [the ECD], in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.’

The DSA simplifies this web of rules as it does *not* overtake the above data protection confusing *limitation* clause from its scope but rather states that the DSA is ‘without prejudice’ to data protection rules. Per Article 89(2) DSA, the references to Articles 12–15 ECD are meant now to refer to Articles 3–7 DSA. Therefore, data protection law is *not* excluded from the scope of the DSA, including the scope of its liability exemptions. DSA is certainly not ‘entirely subsidiary to the protections for personal data’ as David Erdos argued in relation to the Platform to Business Regulation (P2BR) and the DSA’s predecessor, Commission Recommendation (EU) 2018/334.³⁴ The relationship is quite clearly that of parallel application in mutual respect and thus harmonious interpretation without any superiority. The real question, however, is whether this changes anything substantial in the day-to-day relationship between the two areas of law.

The DSA has been designed in compliance with existing rules on data protection, including the GDPR and ePrivacy Directive, and does not modify the rules and safeguards set out in these laws.³⁵ For example, the measures concerning advertising on online platforms complement but do not amend existing rules on consent and the right to object to the processing of personal data. They impose transparency obligations towards users of online platforms, and this information will also enable them to use their rights as data subjects under the GDPR. The GDPR overlaps only partially with the DSA, as it addresses broader questions of data flows and personal data protection.

There are two particular areas where the GDPR and DSA are likely to be read and litigated side by side: (a) the interrelationship between obligations that apply to data controllers and the hosting liability exemption, and (b) the applicability of the DSA’s safeguards to the GDPR’s right to be delisted from search engines.

18.4.1 Controllers and hosting service providers

The concept of a controller is a key concept of the EU’s data protection legislation, which determines who has what responsibilities.³⁶ The Court has continuously

³³ ECD, Rec 14; Miquel Peguera, ‘The Shaky Ground of the Right to be Delisted’ (2016) 18(3) *Vanderbilt Journal of Entertainment & Technology Law* 507.

³⁴ Commission Recommendation (EU) 2018/334 on measures to effectively tackle illegal content online [2018] OJ L63/50; David Erdos, ‘Disclosure, Exposure and the ‘Right to be Forgotten’ after Google Spain: Interrogating Google Search’s Webmaster, End User and Lumen Notification Practices’ (2020) 38 *Computer Law & Security Review* 105437, 5.

³⁵ On an interesting note, it is worth stressing that the DSA refers explicitly to the GDPR up to 17 times, mainly to make clear that the GDPR remains unaffected.

³⁶ Michèle Finck, ‘Cobwebs of Control: The Two Imaginations of the Data Controller in EU Law’ (2021) 11(4) *International Data Privacy Law* 333.

broadened the idea to include actors such as search engines (regarding its search results),³⁷ and social media (regarding their fan pages).³⁸ The Court would include them among ‘controllers’ even if third parties, such as registered users or owners of indexed websites, provided the information in question. Potentially, this means attributing data protection responsibility over harms created by third-party content, similar to imposing liability on hosting services for an illegal video on a video-sharing platform.³⁹ Such outcomes can collide with the DSA’s horizontal rules.

In the *Vividown* case,⁴⁰ the Italian Supreme Court ruled in 2014 that the ECD’s data protection clause does *not* render the ECD and its liability exemptions inoperative regarding data protection. Instead, the clause would only emphasise the applicability of data protection rules in this area.⁴¹ Liability exemptions thus continue to apply. Similarly, in *CG v Facebook Ireland Ltd & Anor*, the Court of Appeal in Northern Ireland held that the liability exemptions *do* apply in data protection law and that the ECD covers a specific question that was not dealt with explicitly under existing data protection rules.⁴²

Two issues merit more discussion when comparing data protection and the hosting liability exemption.

Firstly, as explained in Chapter 6, the liability exemptions cover any civil or criminal liability. Thus, for hosting service providers, the liability exemption can collide with any data protection obligations that would exist prior to acquiring actual knowledge about the illegality of specific information or behaviour. Any attempts to impose sanctions for failure to act before the acquisition of actual knowledge, such as through fines or damages, would directly collide with the hosting liability exemption. As long as the CJEU interprets all third-party content-related obligations as requiring notification, there is no collision. In this way, the data protection laws harmoniously complement the DSA’s liability exemptions by providing a layer of liability-establishing norms which it lacks.⁴³

Secondly, it is not inconceivable that the data protection law might want to impose obligations that would be otherwise understood as general monitoring. For instance, if a hosting provider was asked to broadly prevent the recurrence of some behaviour that violates data protection rules or to manually review large amounts of user-generated content to uncover violations, such obligations could collide again with the hosting liability exemption or the prohibition of general monitoring obligations. Thus, the conflict can occur more easily than it seems at first.

³⁷ Case 131/12 *Google Spain SL and Google Inc v AEPD and Mario Costeja González* ECLI:EU:C:2014:317.

³⁸ C-210/16 *Wirtschaftsakademie Schleswig-Holstein* ECLI:EU:C:2018:388.

³⁹ Italian Supreme Court of Cassation, Cass, 3 Feb 2014, n 5107 (*Vividown*).

⁴⁰ *ibid.*

⁴¹ Peguera (n 33) 543, fn 183.

⁴² *CG v Facebook Ireland Ltd & Anor* [2016] NICA 54; the Court acknowledged the existence of art 1(5) ECD, paras 93–95.

⁴³ Two decisions found liability of Facebook for failure to take swift enough steps after being put on notice: *CG v Facebook Ireland & McCloskey* [2016] NICA 54 (in the Court of Appeal of Northern Ireland); *J20 v Facebook Ireland* [2016] NIQB 98 (in the High Court of Northern Ireland).

According to the CJEU's recent case law, the concept of control under data protection law does not require that a controller has access to data or can distinguish personal and non-personal data.⁴⁴ The CJEU expanded the notion of the controller to cases where intermediaries have only marginal influence over data.⁴⁵ When Facebook hosts its pages, or when Google creates its index, both qualify as data controllers. How liability is distributed among several joint controllers can differ from case to case (eg among Google and publishers, compared to Facebook and page owners).⁴⁶ In fact, the right to be delisted is based explicitly on the fact that Google's processing needs to be distinguished from that of publishers, as it 'affects data subject's rights additionally'.⁴⁷

As a result, the Court sometimes has to adjust the core data protection obligations,⁴⁸ such as when a search engine must verify the lawfulness of its processing of sensitive data only *ex post*—upon receiving a request to dereference.⁴⁹ In the end, the obligations created by data protection law, such as the right to be delisted from the search engines, therefore do not actually modify the basic hosting liability exemptions when they request an action only upon proper notification (which would be assimilated to the knowledge standard under the ECD and the DSA). In such cases, the broad notion of co-controllership and liability exemptions, such as hosting, seems mostly harmonious. In fact, the Court's recent Grand Chamber decision in *TU and RE v Google* (2022)⁵⁰ suggests that only 'manifest inaccuracies' must be delisted following a request to avoid burdening and implicitly deputising the search engine operator to find out the truth.⁵¹ This further synchronises the application of right to be delisted with the hosting liability exemption, which links actual knowledge of hosting service providers only with notifications that 'allow the provider to establish that infringement without conducting a detailed legal or factual examination'.⁵²

After the adoption of the DSA, the relationship between the GDPR and DSA changed to a typical 'without prejudice' loop.⁵³ I think that this does not signal any material change to a relationship that was always meant to be harmonious but is also inherently complicated by two self-standing regimes based on different rationales. In my view, the Court should always strive to achieve harmonious interpretation by keeping in mind the liability exemptions and the prohibition of general monitoring concerning

⁴⁴ *Google Spain* (n 37) paras 28 and 41. See *Google Spain SL and Google Inc v AEPP and Mario Costeja González* ECLI:EU:C:2013:424, Opinion of AG Jääskinen, para 82 (where AG Jääskinen notes Google is not aware of data on the referenced pages, unlike searcher's preferences) and para 101 (where he proposed that the search engine should be only deemed controller if they ignored instructions set out in robots.txt). Before *Google Spain* it was assumed, even by art 29 Working Party, that removal from the index might depend on national tort law—Peguera (n 33) 538. For a discussion of this, Finck (n 36) 335.

⁴⁵ Finck (n 36) 335.

⁴⁶ Art 82(3) GDPR; *ibid* 337.

⁴⁷ *Google Spain* (n 37), paras 35, 38.

⁴⁸ The CJEU found that Google is a data controller not only for links and snippets but also for data in the linked-to pages, see para 41; Google is unable to comply with most of the obligations, eg data quality: see *ibid* para 38 (with the framework of its responsibilities, powers and capabilities). On history, Peguera (n 33) 537ff.

⁴⁹ C-136/17 *GC and others v Commission nationale de l'informatique et des libertés (CNIL)* ECLI:EU:C:2019:773.

⁵⁰ Case C-460/20 *TU and RE v Google LLC* ECLI:EU:C:2022:962.

⁵¹ *ibid* paras 68, 71.

⁵² *YouTube and Cyando* (n 17), para 35.

⁵³ Rec 10 and art 2(5) DSA

third-party content whenever it is interpreting GDPR, as it similarly does under the EU copyright.⁵⁴ Arguably, the latest case law of the Court suggests that this is the approach the Court is taking.

The key to their interaction is how broad we understand the DSA's scope of the term 'is not *liable for the information* stored at the request of a recipient of the service' to be (Chapter 6). Clearly, if the information itself is unlawful (eg hate speech), any liability of its host and the user is covered. Similarly, if the information is unlawful because of the person who is requesting storage or communicating it (eg copyright infringement or defamation), then any liability together with the user is covered too. Data protection's argues that, unlike the DSA, it does not concern the contents of information but its collection and processing. For instance, search engines have an obligation to delist hyperlinks and other information despite the fact that the information is lawful at the source websites.

However, the DSA equally covers situations where the content of the information as such is not unlawful, but its purpose is. Most typically, a discussion between a perpetrator and victim can be lawful on its face but also be part of broader criminal behaviour. The same can be said about spam or phishing messages whose contents can be lawful, but the broader activity of systematic or targeted sending with malicious intention can be unlawful, or a perfectly legally offered apartment available for short-term rental without the prior registration in its municipality. Imposing civil or criminal liability on a platform for such information (eg for not preventing spam or fraudulent conduct) would be pre-empted by the DSA as any other type of liability.

The DSA speaks of being 'liable for the information stored at the request'. The prevailing reading of the day is that any regulation that is enforceable by sanctions of any kind is a liability (Chapter 6). The provision does not require that 'liability' applies only to unlawful information but also to unlawful conduct. The exact contours of the term 'liability for a third-party information', therefore, remain hard to spell out. Data protection law remains at the forefront of these difficulties. But arguably, as long as data protection law is adjusted to the special situation of some controllers who might enjoy liability exemptions, such as the concessions in the context of search engines (assuming they are partly covered, Chapter 7), the problems are more theoretical than practical as delisting is triggered upon request (via a notification).

18.4.2 Right to be delisted

In 2014, in its seminal ruling *de facto*, the Court created a new right to be delisted from search engines by classifying search engines as a special type of data controller. Search engines could be requested to remove information from search results on their name if they are 'inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes'.⁵⁵ This resulted in a major shift in how these services are provided and led to

⁵⁴ *YouTube and Cyando* (n 17).

⁵⁵ *Google Spain* (n 37), para 93.

an immense flood of requests. Some companies like Google created a voluntary safeguard, such as transparency reports, and published studies about how they internalised the judgment.⁵⁶ The GDPR, adopted in 2016, did not change much in this regard. The updated data protection framework did not develop any explicit procedural safeguards concerning this form of delegated enforcement. The guidance regarding substantive balancing was left to practice and the courts.

The DSA now arguably creates some of the much-needed safeguards to the right to be delisted.

Firstly, for VLOSEs, the DSA doubles down on the obligation stipulated by the CJEU in *TU and RE v Google* (2022)⁵⁷ that ‘when the operator of a search engine receives a request for de-referencing ... it *must* ascertain whether [the information] in question is necessary for exercising the right to freedom of information of internet users who are potentially interested in accessing [it]’.⁵⁸ As a result, they ‘*must*, in order to determine whether content may continue to be included in the list of search results carried out using its search engine following a request for de-referencing, take into account *all the rights and interests involved* and all the circumstances of the case’.⁵⁹ The Commission will be exclusively in charge of evaluating risk mitigation measures as regards both data protection and freedom of expression interests;⁶⁰ it will also be able to examine search engines’ practices regarding the right to be delisted against the DSA standards. External auditors will audit, on an annual basis, the compliance by VLOSEs to assess and mitigate risks related to data protection.⁶¹ Vetted researchers will also have access to data to contribute to the detection, identification and understanding of systemic risks.⁶² The public should be able to read about those practices and internal measures in the audit reports to be made public, starting in 2024 (Chapter 16).

Secondly, for VLOSEs, the transparency obligations will now mandate some reporting. VLOSEs are explicitly subject to all DSA’s reporting obligations (Articles 15, 24, and 42), except for the sharing of the statement of reasons with the European Commission’s database (Article 24(5)). These reporting obligations complement Article 17 GDPR. Moreover, if natural links and images included in the search results are understood as a hosting service in some cases (Chapter 7), they would be subject even to the obligation to share statements of reason with the European Commission through a public database—obviously, anonymised and stripped of any personal data.⁶³

The GDPR here does not stand in the way of applying such safeguards, although the search engines sharing the statements of reasons with the European Commission

⁵⁶ Michee Smith, ‘Updating our “Right to be Forgotten” Transparency Report’ (*Google*, 26 February 2018) <<https://blog.google/around-the-globe/google-europe/updating-our-right-be-forgotten-transparency-report/>> accessed 17 September 2023.

⁵⁷ *TU and RE v Google* (n 50).

⁵⁸ *ibid* para 96 (emphasis mine). See also paras 98 and 69 for similar phrasing of obligations.

⁵⁹ *ibid* para 69 (emphasis mine).

⁶⁰ DSA, arts 56 and 34.

⁶¹ DSA, art 37.

⁶² DSA, art 40(4).

⁶³ DSA, art 24(5).

would clearly need to properly de-risk the potential re-identification of the concerned individuals.

A separate sensitive issue concerns the procedural aspects of how search engines make decisions.⁶⁴ The GDPR does not require any issuance of a statement of reasons by search engine operators when they comply with or deny the delisting requests. At the moment, some national Data Protection Authorities seem to even dispute the ability of search engines to notify website owners, such as newspapers whose content is delisted from the search engines. This is highly dubious because the P2BR explicitly requires these notifications whenever the affected website is a business. Moreover, if natural search results qualify as hosting, they could be subject to the even broader obligation under Article 17 DSA to issue a statement of reasons that can be further reviewed internally and externally (Articles 20–21 DSA). This would entirely change how the system operates now on major services whose decisions are not subject to review and often are kept secret. The CJEU will have to clarify this issue in the coming years.

If the Court considers natural search results to be a hosting service (Chapter 7), the DSA is capable of further improving the delegated enforcement system around the right to be delisted by providing further safeguards. It is capable of delivering the safeguards which could have accompanied the GDPR in the first place, according to the Court's own case law.⁶⁵ Since the GDPR does not oppose such safeguards, the DSA now complements the data protection law and offers them up on a golden platter. In *TU and RE v Google*, the Court, for instance, suggests that whenever there is a pending dispute about the accuracy of a particular search result, the search engine operator must append that result temporarily with a public 'warning concerning the existence of such proceedings'.⁶⁶ It is thus clear that the Court does not expect, as some have argued,⁶⁷ that the entire process must take place in utmost secrecy, unbeknownst to the affected parties due to worries about re-amplification by the original publishers.

Thus, analysing the right to be delisted confirms the same trend as copyright law. The DSA is likely to increase the protection of individuals' due process rights without undermining the cause of data protection law.

18.5 Audiovisual Media Regulation

Audiovisual media regulation is one of the early companions of the ECD's regulation of digital services. The first directive, the 'Television without Frontiers' Directive, from

⁶⁴ The CJEU recently said that a search engine operator cannot be expected 'to play an active role in trying to find facts which are not substantiated by the request for de-referencing' as this would place on them a 'burden in excess of what can be reasonably be expected of it': *TU and RE v Google* (n 50) paras 70–71. The same logic obviously does not apply the same to the handling of the dispute process.

⁶⁵ *Poland* (n 28); Martin Husovec, 'Mandatory Filtering Does not Always Violate Freedom of Expression: Important Lessons from *Poland v Council and European Parliament*' (2023) 60(1) Common Law Market Review 173.

⁶⁶ *TU and RE v Google* (n 50) para 76.

⁶⁷ *Erdos* (n 34) 5 ('any disclosure of identity may lead to the content provider subjecting a data subject to inappropriate forms of publicity or exposure').

1989⁶⁸ concerned traditional media. It regulates issues such as television advertising and protection of minors, and facilitated the free movement of broadcasting and distribution of television programmes. The latest directive from 2010, the Audiovisual Media Services Directive (AVMSD),⁶⁹ was once again updated in 2018 to also include video-sharing platforms in its scope.⁷⁰ Thus, for many of the areas covered by the AVMSD, there is no parallel application with the DSA because the two laws regulate different players. However, with respect to video-sharing platforms, the application is often complementary.

The AVMSD's obligations for video-sharing platforms interact, detail, or complement the accountability obligations and safeguards under the DSA.

The Commission's proposal for the DSA in the explanatory memorandum quotes the AVMSD as an example explaining the relationship between the DSA and other EU law instruments. It clarifies that 'the obligations set out in [the AVMSD] as regards audiovisual content and audiovisual commercial communications will continue to apply. However, this Regulation applies to those providers to the extent that the AVMSD ... *do not contain more specific provisions applicable to them*'.⁷¹

Article 28b AVMSD harmonises several obligations for video-sharing platforms. By its definition, all video-sharing platforms are also likely to constitute online platforms, and some of them will even qualify as VLOPs under the DSA. Article 28b thus overlaps fully with the DSA. In terms of substance, Article 28b AVMSD provides for an obligation on the Member States to ensure that video-sharing platform providers under their jurisdiction take '*appropriate measures*' to protect:

- (i) minors from harmful content⁷² in 'user-generated videos' and 'advertising' (Article 28b(1)(a));
- (ii) the general public from incitement to violence or hatred and activities criminalised by Union law, such as terrorist content, child sexual abuse or illegal hate speech in 'user-generated videos' and 'advertising' (Article 28b(1)(b) and (c));
- (iii) the general public from the advertising that they do not 'market', 'sell' or 'arrange', such as those carried by its users, if it does not comply with advertising restrictions (Article 28b(2));

⁶⁸ Council Directive 89/552/EEC on the coordination of certain provisions laid down by Law, Regulation or Administrative Action in Member States concerning the pursuit of television broadcasting activities [1989] OJ L 298/23.

⁶⁹ European Parliament and Council Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (AVMSD) [2010] OJ L95/1.

⁷⁰ European Parliament and Council Directive (EU) 2018/1808 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (AVMSD) in view of changing market realities [2018] OJ L303/69.

⁷¹ Commission, 'Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (DSA) and Amending Directive 2000/31/EC' COM(2020) 825 final (emphasis mine).

⁷² The term is indirectly defined as 'communications which may impair their physical, mental or moral development' (28b(1)(a) AVMSD). It is also mentioned in similar terms in Rec 20 AVMSD and art 6a(1) AVMSD, which also adds that 'The most harmful content, such as gratuitous violence and pornography, shall be subject to the strictest measures.'

All three measures are a form of sector-specific due diligence obligations. They constitute, in fact, a precursor to the DSA in the imposition of due diligence obligations for online platforms. Article 28b(2) AVMSD even emphasises that ‘the limited control exercised by those video-sharing platforms over those audiovisual commercial communications’ must be considered. With these obligations, which mostly target illegal content, there is a clear overlap in the personal and material scope of Article 28b AVMSD and many provisions of the DSA. Obligations (ii) and (iii) clearly cover illegal content, which is the DSA’s core concern.

Obligation (i) concerns content that is not necessarily illegal per se but can be harmful to minors. Minor-related provisions can still overlap with the DSA’s protection of minors (Article 28 DSA) and risk assessment and mitigation measures by VLOPS (Articles 34–35 DSA). The AVMSD’s due diligence measures provided illustratively in Article 28b(3) AVMSD take the form of minimum harmonisation that allows ‘more detailed or stricter measures’ by the Member States (Article 4(1) AVMSD).

Article 28b(3) AVMSD establishes that the ‘appropriate measures’ should be ‘practicable and proportionate, taking into account the size of the video-sharing platform service and the nature of the service that is provided’, and ‘shall be determined in light of the nature of the content in question, the harm it may cause, the characteristics of the category of persons to be protected as well as the rights and legitimate interests at stake’. Thus, it leaves relatively open which measures could be eligible. The DSA could be said to narrow down those choices, previously left to providers or national legislature by a measure of minimum harmonisation. Among the AVMSD’s ‘appropriate measures’, several measures now clearly overlap with explicitly legislated due diligence obligations under the DSA.

The AVMSD obliges the providers to *modify and apply their terms and conditions* to reject relevant illegal content (Article 28b(3)(a)). As far as most of the relevant illegal content is concerned, this rather forces the providers to mirror illegality in legislation into their contracts with users. Hence, it does not contain rules that are different or more specific than Article 14 DSA, which will apply without modifications. The DSA will apply without modification also for related content moderation transparency provisions, as well as for advertising related measures that concern illegal advertising served by third parties (Article 28b(3)(b) AVMSD). Those advertisements will be considered illegal content because the AVMSD bans them. Hence, the AVMSD does not contain rules that are different or more specific than Article 16 DSA or transparency obligations on content moderation restrictions or provisions on advertising transparency, which will apply fully. As those advertisements will be illegal content, Article 16 DSA will also apply.

The AVMSD also obliges video-sharing platforms to establish and operate *transparent and user-friendly mechanisms* for users to report or flag to the provider relevant illegal or harmful content (Article 28b(3)(d)). This obligation overlaps partially with Article 16 of the DSA, which only covers illegal content, not contractually restricted

content. However, even for the overlapping elements, the AVMSD is less specific than Article 16 DSA, which is very prescriptive about what a notice should include. Arguably, Article 16 DSA should thus prevail over 28b(3)(d) AVMSD as a top-up of minimum harmonisation rules.

The AVMSD also obliges video-sharing platforms to establish and operate systems to *explain to its users what effect has been given* to the reporting and flagging (Article 28b(3)(e) AVMSD). Hence, the provision overlaps, in relation to illegal content, with Article 16(4) DSA, which mandates acknowledgement of receipt of the notice. But, as the provision does not specify which user should be informed, it can also overlap with Article 17 DSA, which includes an obligation to issue a statement of reasons for any content moderation decision, regardless of whether its basis is grounded in illegality or terms of services violation. Again, both Articles 16(4) and 17 DSA are more specific and detailed than 28b(3)(e) AVMSD, so the DSA should prevail over minimum harmonisation, including otherwise available provider's discretion.

Finally, the AVMSD obliges video-sharing platforms to establish and operate 'transparent, easy-to-use and effective procedures for the handling and resolution of users' complaints' in relation to the implementation of the measures referred to above (reporting mechanisms, feedback obligation). This obligation leaves the details of internal complaint-handling mechanisms completely open and is much less specific than Article 20 DSA, which establishes deadlines, content retention, human-in-the-loop, and put-back obligations. Hence, it is difficult to justify why the AVMSD should prevail in this regard because the DSA clearly fills its gaps.

To conclude, the analysis of the AVMSD shows an area that is closely intertwined with the DSA, and most of its standards are not far from the DSA. However, the DSA still has some uplifting positive effects on sectorial rules. In terms of substance, the interaction is unlikely to cause significant problems. However, the competence questions can be more complicated depending on the national law.

18.6 Platform to Business Regulation

In many respects, the P2BR⁷³ adopted in 2019 is a forerunner of the DSA. It therefore does not come as a surprise that its rules mostly offer equivalent level of protection of fundamental rights as the DSA. Written by the same team in the European Commission, it largely addresses the same problems from a much more limited business-oriented perspective. The P2BR aims to promote fairness and transparency in

⁷³ European Parliament and Council Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services [2019] OJ L 186/57 (P2BR).

online intermediation services. The Regulation can also be seen as a forerunner of the Digital Markets Act (DMA),⁷⁴ as it addresses some problems that are thematised more in-depth by the DMA today.

As explained above, the DSA applies unless there is sector-specific regulation that is more detailed or specific. The P2BR is one of such related sector regulations and often overlaps with the rules of the DSA. It applies to providers of 'online intermediation services',⁷⁵ to the extent that they offer those services to business users, and to some limited extent to 'online search engines'.⁷⁶ The former set of services often qualifies as online platforms according to the DSA. The latter set of services can qualify as VLOSEs where it meets the threshold.

Typical examples of online intermediation services are online marketplaces, short-term rental services,⁷⁷ or app stores, but also potentially social networks (as regards their advertising, or marketplaces) or other online platforms. Online intermediation services are subject to obligations concerning their terms and conditions (Article 3), fairness standards in the context of suspension, termination, and restriction of their services (Article 4), ranking on their services (Article 5) and related stipulations (Article 8), transparency rules as to differential treatment (Article 7), rules on access to data (Article 9), complaint handling (Article 11) and mediation (Article 12).

Under the P2BR, obligations concerning ranking (Article 5) and differentiated treatment (Article 7) also apply to online search engines. The Regulation only covers *generalist* search engines that 'perform searches of, in principle, all websites, or all websites in a particular language, on the basis of a query on any subject' (Article 2(5)). Thus, specialised meta-search engines are notably excluded. However, if specialised search engines operate *de facto* as marketplaces, they can qualify as 'online intermediation services'. The DSA takes over the same definition of search engines, hence the same applies to the DSA.

The P2BR deviates from the DSA's horizontal rules in the context of *content moderation* in several ways. As regards content moderation of business users' content, Article 4 P2BR imposes a specific obligation for online intermediation services to send a statement of reasons to the business user whenever it decides to restrict or suspend the provision of its online intermediation services to that business user in relation to individual goods or services. This predates Article 17 DSA but overlaps to a great extent with it. Article 4 P2BR has clearly inspired Article 17 DSA in the Commission's proposal.

⁷⁴ European Parliament and Council Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 [2022] OJ L265/1 (Digital Markets Act).

⁷⁵ P2BR, art 2(2). This definition puts them very close to the status of online marketplaces.

⁷⁶ Defined in art 2(5) of the P2BR. This definition was replicated verbatim under the DSA.

⁷⁷ Airbnb was classified as an InfoSoc service in Case C-390/18 *Airbnb Ireland* ECLI:EU:C:2019:1112. Uber was interpreted to be a transport service (Case C-434/15 *Asociación Profesional Elite Taxi v Uber Systems Spain* ECLI:EU:C:2017:9811). But other Uber-like services, which retain less control over the process, could still qualify as InfoSoc service providers, and online intermediation services under the P2BR, Case C-62/19 *Star Taxi App* ECLI:EU:C:2020:980.

The P2BR foresees that statement of reasons are issued *prior to* or at the *same time* of the implementation of the restriction. The same timeframe is given in the DSA, according to which '[i]t shall apply at the latest from the date that the restriction is imposed' (Article 17 DSA). However, the content of the statement of reasons prescribed by the P2BR is more minimalistic (Article 4(5) P2BR) than the detailed requirements of minimum content prescribed by Article 17(3)(a) DSA. The DSA thus extends the statement of reasons because Article 17 DSA complements and further specifies the requirements of Article 4(5) P2BR. The open question is whether the P2BR's statement of reasons will also feed the database managed by the Commission, following Article 24(5) DSA.

The P2BR has a special provision for the termination of accounts. In this context, the P2BR is a clear *lex specialis* to the DSA because it mandates a prior warning. As a rule, it requires that the statement of reasons is issued at least 30 days prior (Article 4(2) P2BR). There are only three exceptions (Article 4(4) P2BR) to this rule—when the provider:

- (a) is subject to a legal or regulatory obligation which requires it to terminate the provision of the whole of its online intermediation services to a given business user in a manner which does not allow it to respect that notice period;
- (b) exercises a right of termination under an imperative reason pursuant to national law which is in compliance with Union law; or
- (c) can demonstrate that the business user concerned has repeatedly infringed the applicable terms and conditions, resulting in the termination of the provision of the whole of the online intermediation services in question.

The first two options are not up to the discretion of the provider. However, the third option allows them some discretion. Arguably, this provision is now further specified by Article 23 DSA. Thus, in cases of repeat infringers, it is not merely that the providers *can* terminate the account; under the DSA, they *must* do so. However, Article 23 DSA only applies when a person 'frequently provide(s) manifestly illegal content' or 'manifestly unfounded' complaints. Thus, the discretion under Article 4(4) (c) P2BR is much broader. Only in some cases, this discretion is limited by Article 23 DSA.

First of all, Article 23 applies only when illegal content is concerned. Thus, any repeated terms of services violations continue to be regulated only by Article 4(4) (c) P2BR. Moreover, Article 23 also will not apply if the provider is a small business. In such scenarios, providers are not obligated to suspend service provisions to repeated infringers. In practice, if it is likely that the providers tend to over-use Article 4(4)(c) P2BR, it is something that Article 14 DSA can now potentially address by requiring any act of termination to be proportionate to the violations in question.

However, even in cases when Article 23 DSA limits discretion under Article 4(4) (c) P2BR, the providers might well give 30 days' notice as a rule to businesses, as

such practice would not generally be incompatible with the DSA, which also requires ‘prior warnings’. This is sensible given that business users often have their business and thus livelihoods on the line. Naturally, this does not mean that the providers could not act swiftly against accounts set up to distribute spam or bots. In such cases, nothing in the P2BR and the DSA prevents them from exceptionally acting quickly.

The P2BR also includes its own *out-of-court dispute settlement* system that takes the form of *mediation*. It works as follows. Each online intermediation service must preselect in its terms and conditions two mediators whose services it is willing to use in case its business users are not happy with the result of the internal complaint procedure. These mediators must meet some requirements, such as independence, impartiality, and affordability (Article 12(2) P2BR). Participation, however, remains voluntary (Article 12(3) P2BR). If the provider agrees to participate, it must pay ‘a reasonable proportion of the total costs of mediation in each individual case’ (Article 12(4)). The outcome of the procedure is an agreement of two parties (Article 12(5)).

The DSA, on the other hand, creates a mandatory system of out-of-court settlement under Article 21, where platforms cannot refuse to participate. They have leeway not to accept the outcome, but they must reimburse the complainant’s fee if they lose. However, they also do not get to choose the dispute resolution provider; the complainant does. The outcome of the procedure is not an agreement but a decision. Arguably, therefore, these two are different out-of-court settlement systems. The P2BR system initially introduces a much more cautious approach based purely on voluntary participation. The DSA mandates a more elaborate system. The reason is simple: the P2BR still comes from a business-to-business perspective, while the DSA covers potentially all types of relationships, be it B2B or B2C.

While Article 21 DSA does not displace Article 12 P2BR, it will probably make it less interesting. However, given the differences, Article 12 P2BR also does not pre-empt the application of Article 21 DSA to B2B disputes. This outcome is also evident from the fact the state authorities cannot be pre-empted by P2BR to introduce or fund more elaborate systems to facilitate the resolution of disputes (Article 15 P2BR).

Thus, the analysis of the P2BR shows that while the DSA’s uplifting effect is much more limited, as rules contained largely equivalent levels of safeguards, the horizontal nature of the DSA extends the rules substantially.

18.7 Terrorist Content Regulation

In 2021, the EU legislature adopted the TCR.⁷⁸ The TCR aims to limit terrorist content online by harmonising the rules concerning orders issued by national authorities.

⁷⁸ European Parliament and Council Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online [2021] OJ L 172/79.

Controversially, it requires that hosting service providers remove terrorist content or disable access to it in all Member States ‘as soon as possible and in any event within one hour of receipt of the removal order’ (Article 3(3) TCR). It includes a template for authorities to communicate removal orders, and templates for providers to respond to them. The TCR facilitates cross-border removal and retention of relevant data. Finally, it requires that authorities and providers engage in some level of transparency and co-operation, and respect some essential due process safeguards. The TCR safeguards partly⁷⁹ exceed the DSA’s level of protection because the DSA generally lacks complex safeguards for the orders of authorities.

Among the points of interaction, the crucial points concern orders, transparency, and safeguards.

Firstly, the TCR has its own specific rules concerning removal orders and the speed of removal. The whole point of the TCR is to establish templates to communicate more easily between the providers and competent authorities. The DSA does not change any of these rules. Once the decision is made, although the DSA is overridden on the issue of communication with the competent national authorities, the communication with the affected content creators continues in the DSA’s trajectory. While the provider does not have to issue a statement of reasons, the TCR obliges the provider that removes or disables access to terrorist content to ‘make available to the content provider information on such removal or disabling’ (Article 11(1) TCR). However, the TCR does allow the authority issuing the removal order to prohibit the disclosure for reasons of public security, such as the prevention, investigation, detection and prosecution of terrorist offences, for as long as necessary, but not exceeding six weeks from that decision (Article 11(3) TCR). These rules will apply as *lex specialis* to the general optional rules regarding orders (Article 9(5) DSA).

Secondly, the transparency requirements under Article 7 TCR are a special reporting obligation that complements the general reporting obligations under the DSA (Article 15 DSA). Article 7(3) information is more elaborate than expected from orders falling under Article 15(1)(a) DSA. Under Article 7(3) TCR, for instance, information must be published ‘about the hosting service provider’s measures to address the reappearance online of material which has previously been removed or to which access has been disabled because it was considered to be terrorist content, in particular where automated tools have been used’. This obligation is further complemented by Article 15(1)(e) DSA. Moreover, under the TCR, the authorities also have an obligation to issue transparency reports of their own (Article 8 TCR).

Third, the TCR grants hosting service providers a right to challenge orders before courts (Article 9 TCR). The internal dispute resolution process (Article 10 TCR) only offers a framework, which the DSA builds upon with many explicit

⁷⁹ In other respects (eg time limits for takedown), one could say that the TCR lowers the protections afforded by the DSA.

requirements. However, the period of a maximum of two weeks within which the provider has to inform the complainant of the outcome continues to apply (Article 10(2) TCR).

18.8 Conclusion and Outlook

Based on the sectorial analysis, the uplifting effect of the DSA is a fact. While it might take years to clarify in practice, it seems clear that the DSA's rules create strong horizontal expectations of the minimum level of rights. Legally speaking, the DSA is likely to become an *EU digital rights charter*.

As pointed out in the introduction, this might also impact future European politics. The increasing reliance on the 'without prejudice' clause only increases the application of the DSA's charter of rights. Despite being adopted only in 2022, there are already several new instruments that are likely to build on top of the DSA. The Commission and co-legislators seem ready to tackle any sector-specific problem, sometimes without even waiting to see whether the proposed and recently agreed rules show effect.

To mention some: the Regulation on general product safety (GPSR)⁸⁰, the Proposal for a Regulation establishing a common framework for media services in the internal market (EMFA)⁸¹ and the Proposal for a Regulation on transparency and targeting of political advertising⁸² all build upon the institutions established by the DSA.⁸³ They 'do not affect' the DSA (Article 1(2) EMFA) and apply 'without prejudice' to the DSA's liability provisions,⁸⁴ although they continue to impact the due diligence obligations under the DSA.

The most controversial of these is the Proposal for a Regulation laying down rules to prevent and combat child sexual abuse (CSA)⁸⁵ that exploits one of the bigger gaps of the DSA—its weak application to the infrastructure layer. The proposal says it applies 'without prejudice to the rules resulting from' the ECD and the DSA but at the same time it 'should be considered *lex specialis* in relation to the generally applicable framework set out in' the DSA.

⁸⁰ European Parliament and Council Regulation (EU) 2023/988 on general product safety, amending Regulation (EU) No 1025/2012 and Directive (EU) 2020/1828, and repealing Directive 2001/95/EC and Council Directive 87/357/EEC [2023] OJ L 135/1 (General Product Safety Regulation (GPSR)).

⁸¹ Commission, 'Proposal for a Regulation of the European Parliament and of the Council Establishing a Common Framework for Media Services in the Internal Market (European Media Freedom Act) and Amending Directive 2010/13/EU' COM(2022) 457 final (EMFA).

⁸² Commission, 'Proposal for a Regulation Of The European Parliament And Of The Council on the Transparency and Targeting of Political Advertising' COM(2021) 731 final.

⁸³ Rec 57 GPSR.

⁸⁴ GPSR, art 20(1); Commission, 'COM(2021) 731 Final' (n 82), Rec 70.

⁸⁵ Commission, 'Proposal for a Regulation of the European Parliament and of the Council Laying down Rules to Prevent and Combat Child Sexual Abuse' COM(2022) 209 final (CSA).

Regardless of the political outcomes, these proposals already show that the DSA has integrating effects for pre-existing and future legislation. It frames the debate and forces legislatures to think about compatibility with the institutions and protections offered by the DSA. While this does not guarantee immunity against change, it contributes toward certain consistency of the rules and potentially helps to preserve a horizontal set of individual rights and freedoms across the digital ecosystem.

The DSA as a Mixed Enforcement System

19.1 Introduction	417	19.3.3 Compensatory damages	434
19.2 Public Enforcement	420	19.3.4 Injunctions by consumer bodies	436
19.2.1 European Commission	422	19.3.5 IP injunctions against intermediaries	437
19.2.2 National DSCs	426	19.3.6 Cross-border jurisdiction and enforcement	438
19.2.3 Board	427	19.3.7 Non-judicial enforcement	439
19.3 Private Enforcement	428	19.4 Conclusion	442
19.3.1 Of rights and obligations	429		
19.3.2 What constitutes an infringement?	433		

19.1 Introduction

The Digital Services Act (DSA)’s direct predecessor, the E-Commerce Directive (ECD), had little to no experience in the enforcement area. The ECD’s main goal was to create markets, not regulate them. The DSA, in contrast, is a regulatory moment for the technology industry. It brings command-and-control-style due process regulation for content moderation activities for mid-sized online platforms. These rules are largely borrowed from pre-existing industry practices. For very large online platforms and search engines (VLOPs/VLOSEs), collectively referred to as Big Tech, the DSA creates an elaborate system of regulatory dialogue about risks complemented by co-regulation through Codes of Conduct.

On the global stage, the European Union (EU) is not alone in trying to regulate the risks of Big Tech. Other countries have also started regulating the space, but their approach has varied. The closest regulatory twin—the UK’s Online Safety Bill—is public enforcement focused.¹ Meanwhile, countries such as Australia rely more on supervised self-regulation.² Noticeably, both regulate the space without creating the rights of individuals. The DSA is not much different, but only specifically with respect to Big Tech and in the sphere of public enforcement. However, the uniqueness of the European approach lies, among other things, in its reliance on combined public *and* private enforcement of rules. For the latter, it has created a binding catalogue of due process rights and obligations applicable in content moderation that are also privately enforceable.

The DSA and similar regimes worldwide face several unique enforcement challenges.

¹ Online Safety HC Bill (2021–22, 2022–23).

² Online Safety Act 2021 (Cth).

Large transnational companies often provide popular digital services that offer the same user experience worldwide. Sometimes, the uniform design is a cost-saving strategy, but in many cases, it is dictated by the nature of the global service. Nowhere is this more visible than in debates about weakening encryption, where companies often argue that they are not willing to remake their global products specifically for one country if that means weakening a product for all its customers.³ Physical goods can be easily adjusted for the local context; global services inherently less so. Thus, the first challenge is understanding when companies are raising global objections legitimately and when they are raising them only as a matter of commercial convenience. If the objection is genuine, the global nature of the network means that national or regional regulators are inevitably making decisions with trade-offs that exceed the boundaries of their jurisdiction. For instance, a liberal democracy's decision to require the filtering of extremist material on a global platform would inadvertently facilitate the demands of a dictatorship in another country to do the same, though for very different content.

Different jurisdictions can legitimately have *different ideas about individual freedoms*. Europeans might never understand why American laws permit relatively free trade in guns but prohibit the sale of Kinder Surprise chocolate eggs⁴ on the grounds of safety. Americans, in turn, might scoff at European laws giving individuals a right to be erased from search engines or criminalise non-violent hate speech. It is, therefore, important to always remind ourselves that even within the Union of like-minded countries that share the same human rights charters, the notions of what is illegal might differ considerably. Because the DSA's definition of *illegality* relies on national law, it imports all the potential conflicts into its ambit. The DSA expects providers to enforce the Maltese ban on abortion advertising,⁵ Spanish criminal rules on religious blasphemy,⁶ the German total ban on the use of Nazi and similar symbols,⁷ or the Hungarian ban on the depiction of gays in content for minors,⁸ even though this content is not illegal in most of the other EU countries. The difficulties of navigating global and intra-European legal and cultural differences will only be amplified by the

³ See, for instance, Hartley Charlton, 'Apple Threatens to Pull FaceTime and iMessage in the UK over Proposed Surveillance Law Changes' (*MacRumors*, 20 July 2023) <<https://www.macrumors.com/2023/07/20/apple-threat-ens-to-pull-facetime-and-imessage-uk/>> accessed 18 September 2023.

⁴ US FDA, 'Import Alert 34-02' <https://www.accessdata.fda.gov/cms_ia/importalert_107.html> accessed 18 September 2023.

⁵ Sub-title VII of the Maltese Criminal Code: *Legiżlazzjoni Malta*, 'Chapter 9: Criminal Code' <<https://legislat.ion.mt/eli/cap/9/eng>> accessed 18 September 2023.

⁶ Art 525 of the Spanish Criminal Code 2016: (1) Whoever, in order to offend the feelings of the members of a religious confession, publicly disparages the dogmas, beliefs, rites or public ceremonies thereof, verbally or in writing, or insult, also publicly, those who profess or practice these, shall incur the punishment of a fine from eight to twelve months. (2) The same penalties shall be incurred by those who publicly disparage, verbally or in writing, those who do not profess any religion or belief whatsoever. See *Criminal Code* (Ministerio de Justicia 2016) <https://www.mjusticia.gob.es/es/AreaTematica/DocumentacionPublicaciones/Documents/Criminal_Code_2016.pdf> accessed 18 September 2023.

⁷ Art 86a of the German Criminal Code: Bundesministerium der Justiz, 'Strafgesetzbuch (StGB): § 86a Verwenden von Kennzeichen Verfassungswidriger Und Terroristischer Organisationen' <https://www.gesetz-im-internet.de/stgb/_86a.html> accessed 18 September 2023.

⁸ Kati Cseres, 'Instrumentalization of Consumer Law in Central and Eastern Europe for Populist Politics: A Citizen-Consumer Perspective' [2022] Amsterdam Law School Research Paper No 19 (2022), 17 <<https://papers.ssrn.com/abstract=4162963>> accessed 18 September 2023.

DSA and its numerous tools because of the intrinsic temptation to impose one's own solutions on others.

Coupled with this are several legal coordination problems.

To enforce means to agree on *which country* can *enforce* the rules. To facilitate the emergence of digital services, the DSA and many other EU laws, such as the General Data Protection Regulation (GDPR), try to answer that question by vesting public enforcement almost exclusively with the Member State where the company decides to settle. In the context of digital services, any rule-making power of states besides EU harmonisation, is constrained by the country-of-origin principle. Where public enforcement is a dominant paradigm, this effectively means putting a lot of the responsibility on one Member State. The risk is that this becomes a forum shopping opportunity for companies that can try to curry favours with specific countries in exchange for local investment. However, if the policy area is strongly complemented by private enforcement, the effect of concentrated public enforcement can be diluted. Private enforcement foresees many instances where the courts other than those of the company's seat are competent to hear the case and grant reliefs. As Recital 126 DSA emphasised, these private enforcement routes remain untouched by the DSA's distribution of public enforcement powers.

The second coordination problem exists within each country. As illustrated in Chapter 18, the DSA overlaps with many other legal instruments. This also means that it overlaps with enforcement structures for all these instruments, such as the GDPR, the Audiovisual Media Services Directive (AVMSD), Platform to Business Regulation (P2BR), or Terrorist Content Regulation (TCR). All these items of legislation try to tackle the problem of cross-border enforcement and potential deadlocks at the national level in their own ways. It is one thing to infer what rules apply and quite another to agree on who oversees enforcing them in case of overlaps.

The DSA relies on a mixture of public and private enforcement to give life to the legal instrument. For many European policies, there is a tendency to employ administrative agencies subsidised by the taxpayers.⁹ But upon closer look, the DSA rather asks public enforcement to oversee that providers diligently operate the expected cycle of *private machinery* of content moderation. In this sense, the DSA subsidises the resolution of individual disputes through administrative oversight of private systems. This is especially visible with the oversight of content moderation procedures, explanations, out-of-court dispute settlement (ODS) bodies, trusted flaggers, and access to data, where the public regulators control the cogs of the system but are not involved in daily operations. The taxpayer thus does not pay for the resolution of private skirmishes.¹⁰

⁹ Melanie Smith, 'Challenges in the Implementation of EU Law at National Level' (Briefing requested by the JURI committee, PE 608841, 2018) <[https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/608841/IPOL_BRI\(2018\)608841_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/608841/IPOL_BRI(2018)608841_EN.pdf)> accessed 18 September 2023.

¹⁰ To be sure, there are parts of the DSA, such as obligations to provide a statement of reasons or decide in a timely fashion, that can still give rise to individual-level public enforcement through complaints (art 53 DSA).

19.2 Public Enforcement

It was hoped that the public administrative enforcement structure of the DSA would solve and improve two parallel and conflicting issues. On the one hand, to protect the internal market, it must respect the country-of-origin rule, which limits the number of EU regulators of the EU-established providers to one. On the other hand, the DSA tries to address the (GDPR-linked) fears¹¹ of other destination countries relating to the potential underenforcement by the regulator of the country of origin. However, allowing all destination countries to regulate all companies could endanger the internal market because even if the underlying rules were to be fully harmonised, providers would have to constantly engage in dialogue with potentially hundreds of authorities from 27 countries speaking 24 different languages.

The DSA tries to learn from its older sister, the GDPR,¹² in addressing the key concern that new ambitious rules might become hostage to ineffective enforcement structures. Thierry Breton, during the hearing before the European Parliament,¹³ committed vehemently to respect the country of origin as part of the three main *red lines* signalled by the Parliament on the DSA.¹⁴ The Commission's DSA proposal aimed to *strengthen* the country-of-origin principle.¹⁵ Under the rule, in the harmonised field, the authorities of the country of destination cannot act directly against a provider established elsewhere; only the Member State of establishment is competent in the first place. In the legislative process, one exception was introduced: the Commission can act with concurrent powers, and only in the case of designated VLOPs.¹⁶ As explained by Roche Laguna, the logic behind this was that 'for Big Tech, the country of origin is

¹¹ For an example of the criticism, Daniel Holznagel, 'Ireland Cannot Do It Alone: All Member States Should Contribute to the Supervision of Very Large Online Platforms Under the Digital Services Act' (*Verfassungsblog*, 27 April 2021) <<https://verfassungsblog.de/dsa-ireland/>> accessed 18 September 2023.

¹² For the overview of the administrative enforcement systems of the GDPR and their deficiencies, Giulia Gentile and Orla Lynskey, 'Deficient by Design? The Transnational Enforcement of the GDPR' (2022) 71(4) *International and Comparative Law Quarterly* 799. The European Commission recently proposed a new regulation to overcome some of these issues, European Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679' COM(2023) 348 final

¹³ European Parliament, 'Hearing of Commissioner-Designate Thierry Breton' (14 November 2019) <<https://www.europarl.europa.eu/news/en/press-room/20191112IPR66319/hearing-of-commissioner-designate-thierry-breton>> accessed 18 September 2023.

¹⁴ The three red lines were: the liability exemptions, the prohibition of general monitoring obligations and the country-of-origin principle. These were singled out and raised by ministers from the so-called D9 + group (comprising Belgium, Czech Republic, Denmark, Estonia, Finland, Ireland, Luxembourg, Netherlands, Poland, and Sweden): D9+, 'D9+ Non-Paper on the Creation of a Modern Regulatory Framework for the Provision of Online Services in the EU' <https://euractiv.cz/wp-content/uploads/sites/7/2020/08/D9_NON-PAPER-1.pdf> accessed 18 September 2023.

¹⁵ There are two meanings of the country-of-origin principle. The first speaks to the ability to make rules, and the second to the ability to enforce rules. The DSA, like any harmonisation legislation, limits the ability to make domestic rules by harmonising them. In the context of this chapter, I mostly refer to country of origin as a principle designating the authorities that can enforce the rules. Orders according to arts 9–10 typically do not touch the principle, however. See Rec 38 DSA.

¹⁶ Art 50 of the Commission's proposal foresaw an 'enhanced supervision for very large online platforms', see Commission, 'Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (DSA) and Amending Directive 2000/31/EC' COM(2020) 825 final.

Europe.¹⁷ Thus, any failure of the Member State of establishment does not have to be resolved by infringement actions against that state, but also by direct enforcement capabilities of the European Commission.

This outcome was a product of an interesting dynamic during the legislative process. The Council was quickly divided into two opposing groups on the enforcement issues: those seeking more powers of enforcement for the Member States of destination (eg France, Germany, Denmark, Poland), and those, typically smaller countries, that defended the country-of-origin principle. France, which eventually presided over the Council during the last parts of the negotiations, failed in its initial attempt to increase the enforcement power of every country of destination.¹⁸ It immediately faced the opposition of the smaller single-market-friendly countries which managed to form a blocking minority.¹⁹ As a result, a compromise was necessary.

The agreed solution was that if the country of origin is strengthened, the control of the country of establishment is weakened through new supranational powers of the European Commission. In order to avoid VLOPs ‘hiding’ behind weaker enforcers, the Council eventually pushed for a new role of the Commission as an *exclusive enforcer* of some special obligations (Section 5 of Chapter III DSA). It, moreover, installed the Commission as a *concurrent enforcer* in case of breaches of other (standard) obligations by VLOPs and VLOSEs. Thus, eventually, the tension between the two positions led to a stronger European Commission. The countries of establishment, however, preserved their control over more local champions who are not sufficiently big to qualify as VLOPs.²⁰ They are important eyes and ears for problems of SMEs with the application of the DSA.

During the negotiations, some Member States that were afraid of underenforcement by the country of establishment expressed their preference to give exclusive powers to the Commission for *all* obligations applicable to VLOPs/VLOSE. The final text, however, did not adopt this approach for a simple reason. Underenforcement would be almost guaranteed under such an approach because the European Commission would have minimal resources available. As expressed by Roche Laguna, it could have led to a ‘paradox situation where people using VLOPs would be less protected than users of smaller platforms if the Commission decided to focus only on widespread issues.’²¹ For this reason, the final text gives the European Commission only concurrent powers. The expectation is that the supranational body should act against VLOPs for their standard due diligence violations only when things get really serious.

¹⁷ Interview with Irene Roche Laguna, Deputy Head of Unit for Coordination and Regulatory Compliance, European Commission (2021–23).

¹⁸ Ilaria Buri, ‘The DSA Proposal and France’ (*DSA Observatory*, 12 November 2021) <<https://dsa-observatory.eu/2021/11/12/france-and-the-dsa-proposal/>> accessed 18 September 2023.

¹⁹ IE delegation and others, ‘Joint Non-Paper of Croatia, Czech Republic, Estonia, Finland, Malta, Ireland, Latvia, Lithuania, Luxembourg, Romania, Slovakia, and Sweden on the Effective Supervision under the Digital Services Act’ (2021) Document WK 11144/2021 REV 2 <<https://councildsa.reset.tech/pdf/wk11144-re02.en21.pdf>> accessed 18 September 2023.

²⁰ This agreed solution was the French Presidency’s main red line. Interview with Irene Roche Laguna (n 17).

²¹ *ibid.*

Table 19.1 Competence for national regulators

Competence	Standard Enforcement		Reinforced Enforcement
Type of obligations	Standard due diligence obligations (Articles 11–32 DSA)		Special due diligence obligations (Articles 33–43 DSA)
Who violates what obligations?	Any infringement by providers that are <i>not</i> VLOPs or VLOSEs	Any infringements by VLOPs or VLOSEs	Any infringements by VLOPs or VLOSEs
Which public authority is competent?	Digital Services Coordinator of the Country of Origin (DSC-COO)	DSC-COO and COM share the enforcement powers; COM uses it for ‘systemic infringements’ and has priority to act (Article 56(3), Recital 125 DSA)	European Commission (COM) has exclusive enforcement powers (Article 56(2) DSA)

19.2.1 European Commission

The final text of the DSA encompasses two different schemes of enforcement: the *standard* one for all intermediaries in scope and a *reinforced* one for designated VLOPs and VLOSEs. The thinking behind this is that very large players are more likely to impact the whole of the EU because of their broad European user base. From that perspective, their non-compliance even with standard due diligence obligations—ie *universal*,²² *basic*²³ or *advanced*²⁴ obligations—is more likely to become time-sensitive and large-scale. As a result, the task could well overwhelm even the more experienced national regulators. Thus, the enforcement is layered depending on the importance of infringement and its perpetrator, based on the following criteria:

- a) Who is the infringer (VLOP/VLOSE or others).
- b) What obligations are violated (special obligations or standard obligations).
- c) What is the significance of the violation (systemic or non-systemic).

Table 19.1 shows how the Digital Services Coordinator of the country of establishment of the provider (DSC-COO) shares the responsibility with the Commission (COM). The DSC-COO is the DSC which belongs to the country where the provider is established in the EU²⁵ or, if it is not established in the EU, the country where its legal representative is established (Article 56(6)). If the provider of regulated digital

²² DSA, ch III, s 1.

²³ DSA, ch III, s 2.

²⁴ DSA, ch III, ss 3–4.

²⁵ Rec 123 DSA specifies that ‘the main establishment of the provider of intermediary services is located, that is, where the provider has its head office or registered office within which the principal financial functions and operational control are exercised’.

services provides offers services in the EU markets²⁶ but does not have an establishment or a legal representative in the EU, the competence is shared by all the DSCs and Commission but subject to a mutual notification requirement (Article 56(7)).²⁷

However, one should note that legally speaking, the ‘systemic infringements’ criterion delineating the sharing of powers between the COM and DSC-COO is rather one of self-constraint than a real hard limit.²⁸ In the competence rule of Article 56(3) of the DSA, the condition of ‘systemic infringements’ does not appear. It is only mentioned in Recital 125, which also suggests very broad discretion on the side of the Commission:

... the Commission could in many instances be better placed to address *systemic infringements* committed by those providers, such as those affecting multiple Member States or serious repeated infringements or concerning a failure to establish effective mechanisms required by this Regulation. On the other hand, the competent authorities in the Member State where the main establishment of a provider of very large online platform or of very large online search engine is located could be better placed to address individual infringements committed by those providers, that do not raise any systemic or cross-border issues. In the interest of efficiency, to avoid duplication and to ensure compliance with the principle of *ne bis in idem*, *it should be for the Commission to assess whether it deems it appropriate to exercise those shared competences in a given case and, once it has initiated proceedings, Member States should no longer have the ability to do so.*²⁹

An example of a ‘systemic infringement affecting multiple Member States’ could be the failure of a very large online marketplace to identify any trader operating from another Member State for the purposes of Article 30 of the DSA. An example of a ‘serious repeated infringement’ could be a recurrent failure, by a VLOP, to send any statement of reasons in compliance with Article 17 of the DSA to users in some countries. However, usually, these two grounds for systemic infringement will overlap as anything systemic is likely to affect multiple EU Member States.

Arguably both powers of the European Commission are about violations with large European impact and follow the same logic: whatever big players do matters for the whole EU. As Recital 125 explains, the Commission has the discretion to decide whether to exercise those concurrent competencies for systemic breaches in each case. But once the European Commission has initiated proceedings, the Member States should no longer proceed with enforcement. This rule is meant to avoid breaches of the

²⁶ DSA, arts 2(1), 3(e), and (d).

²⁷ Those countries that share a language with other non-European countries (eg Portugal and Brazil) might de facto gain a special role as enforcers of rules against providers that serve the EU market but have no EU representatives or establishment.

²⁸ A similar argument is made by Saulius Kaleda, Paul-John Loewenthal, and Folkert Wilman, *Digital Services Act: Commentary* (forthcoming, OUP 2024) § 56.

²⁹ DSA, Rec 125 (emphasis mine).

ne bis in idem principle.³⁰ It basically gives the European Commission priority in exercising the shared competencies. The situation is more complex in situations when providers change establishment, or their legal representatives during the investigations. In those cases, the DSA has no special rules about whether the competence remains with the original DSC for existing investigations, or has to be ceded to the new DSC of establishment. If providers are VLOPs or VLOSEs, it is clear that the Commission can take over, however. To avoid forum-shopping, the review of the DSA should introduce explicit rules for such situations.

The resulting distribution of competences for public enforcement over providers that are either established in the EU or at least have an EU legal representative is as shown in Table 19.1.

Only practice will tell how the European Commission will exercise its competence in cases when VLOPs or VLOSEs violate standard due diligence obligations. It is likely that the resource-limited Commission will prioritise cases based on their importance. The priorities might resemble what we have seen in competition law, where the Commission routinely has its main priorities³¹ and is unwilling to investigate cases that do not pass muster.

According to the existing EU rules,³² the Commission must prepare a public forecast of its income and budget every June. For 2024,³³ the Commission budgeted €19.4 million for 123 full-time equivalent (FTE) employees for all its activities, ranging from staff working on designation, case handling, supervision, coordination, and IT infrastructure. Another €25.8 million is planned for material support and the cost of external experts. If one compares these numbers with costs forecasted in other newly proposed areas, such as control of subsidies,³⁴ and considers the fact that the Commission must always supervise all the 19 VLOPs and VLOSEs (as of July 2023) at least concerning

³⁰ DSA, Rec 125. EU competition law is an example of application of the principle, Case C-117/20 *bpost SA v Autorité belge de la concurrence* ECLI:EU:C:2021:680; Case C-151/20 *Nordzucker AG and others* ECLI:EU:C:2022:203.

³¹ See, for instance, European Commission, 'Guidance on the Commission's Enforcement Priorities in Applying Article 82 of the EC Treaty to Abusive Exclusionary Conduct by Dominant Undertakings' (Communication) [2009] OJ C45/7 <[https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52009XC0224\(01\)](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52009XC0224(01))> accessed 18 September 2023; European Commission, 'Amendments to the Communication from the Commission Guidance on the Commission's Enforcement Priorities in Applying Article 82 of the EC Treaty to Abusive Exclusionary Conduct by Dominant Undertakings' (2023) (Communication) C(2023) 1923 final <https://competition-policy.ec.europa.eu/system/files/2023-03/20230327_amending_communication_art_102_0.pdf> accessed 18 September 2023.

³² Art 6(1), second subparagraph of Commission Delegated Regulation (EU) 2023/1127 supplementing Regulation (EU) 2022/2065 of the European Parliament and the Council with the detailed methodologies and procedures regarding the supervisory fees charged by the Commission on providers of VLOPs and VLOSEs [2023] OJ L149/16.

³³ Commission, 'Overview of Elements Accounted for the Estimation of the Amount of External Assigned Revenues Stemming from the Supervisory Fee Pursuant to Article 6(1) of Commission Delegated Regulation (EU) 2023/1127' (Commission Staff Working Document) SWD(2023) 242 final.

³⁴ Commission, "Impact Assessment" (Commission Staff Working Document) Accompanying the "Proposal for a Regulation of the European Parliament and of the Council on Foreign Subsidies Distorting the Internal Market" SWD(2021) 99 final 60 <<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021SC0099>> accessed 18 September 2023 (discussing various regulatory options, all of which are in the range of one to two FTEs per investigation per year).

their special obligations, it becomes clear that it will have only very limited space to conduct extra investigations.³⁵

Due to the enormous scope of the potential DSA investigations, there will always be too few Commission officials chasing down too many problems. To foot the bill, the DSA adopts the ‘polluter-pays’ principle, under which companies are specifically taxed to pay for their public supervision. The supervisory fee is to be paid by designated very large players as externally assigned revenue.³⁶ In addition, the DSA relies on the Member States to increase the European enforcement capacity by funding its national DSCs. The European public enforcement of the DSA is thus powered by the staff of the Commission *and* national DSCs. However, national authorities are funded by national budgets, and thus their funding depends on the national parliaments. The DSA’s only check on any potential under-funding is the independence requirement for national DSCs, which demands that the ‘Digital Services Coordinators have all necessary resources to carry out their tasks, including sufficient technical, financial and human resources to adequately supervise all providers of intermediary services falling within their competence’ (Article 50 DSA).

In the legislative process, there were also some more ambitious options proposed, such as creating a dedicated EU Agency. As noted by Roche Laguna, ‘the banking sector was often mentioned as a model to justify the need to act in front of a crisis that was compared to the financial crisis.’³⁷ While a new Agency had some support in academia³⁸ and among political groups,³⁹ its creation would probably slow down the legislative process. According to Roche Laguna, ‘while looking into the existing models in the field of data protection (the EDPB), the banking sector or medicines, the Commission preferred not to accelerate too quickly from 0 to 100.’⁴⁰ Thus, while a separate agency could have eased the suspicions surrounding the relative independence of the Commission as a political body, it stood in the way of the expediency of the legislative process. The idea of a new Agency was thus left for another day. In the coming years, the extent to which the European Commission will be susceptible to politicisation of the oversight of Big Tech should determine how quickly the transformation to an independent agency model is required.

³⁵ But because the special obligation to mitigate risks is so all-encompassing, any extra investigations of violations of standard due diligence obligations can sometimes be integrated into bigger annual monitoring, which could somewhat reduce the investigation cost per employee.

³⁶ Following the Commission Delegated Regulation (EU) 2023/1127, supervisory fees will constitute externally assigned revenue in accordance with art 21(5) of the Financial Regulation (EU, Euratom) 2018/1046. European Parliament and Council Regulation (EU, Euratom) 2018/1046 on the financial rules applicable to the general budget of the Union, amending Regulations (EU) No 1296/2013, (EU) No 1301/2013, (EU) No 1303/2013, (EU) No 1304/2013, (EU) No 1309/2013, (EU) No 1316/2013, (EU) No 223/2014, (EU) No 283/2014, and Decision No 541/2014/EU and repealing Regulation (EU, Euratom) No 966/2012 [2012] OJ L 193/1

³⁷ *Interview with Irene Roche Laguna* (n 17).

³⁸ Ben Wagner and Carolina Ferro, ‘Governance of Digitalization in Europe: A Contribution to the Exploration Shaping Digital Policy - Towards a Fair Digital Society?’ (Bertelsmann Stiftung 2020) <<https://www.bertelsmann-stiftung.de/doi/10.11586/2020018>> accessed 18 September 2023.

³⁹ The Greens/EFA, opposing the proposal to put the Commission in charge of VLOPs supervision because the Commission is an executive body under political leadership and not an independent expert regulator as is needed to oversee platforms, had proposed the introduction of a new independent EU Agency. This proposal was not adopted.

⁴⁰ *Interview with Irene Roche Laguna* (n 17).

19.2.2 National DSCs

The DSA leaves an important role to the national regulators and parliaments. National parliaments decide to structure and fund their national DSCs. Given that the DSA covers so many areas, it will inevitably be a tool for many authorities with different types of expertise. This requires a good regulatory design, and building of local competencies, such as in research.⁴¹ The strengths, weaknesses, and capabilities of national regulators will either be a liability or help for the European Commission, tasked with the biggest of actions. At the time of writing, the national regulators are not designated yet, and the public information about plans suggests a future mixture of new and old authorities across the continent. According to Euractive,⁴² the Member States are planning to designate a mixture of former media regulators (eg Ireland and Slovakia), competition and consumer authorities (eg the Netherlands), and telecommunication regulators (eg Italy and Germany).

The initial VLOP and VLOSE designations (Chapter 9) show that Ireland will be responsible for many of the largest players. In the context of the GDPR, Ireland has been repeatedly blamed for soft enforcement to lure investment from technology companies and protect the country's competitive advantage. In the first five years of the GDPR, as reported by the Irish Council for Civil Liberties, '67% of the Irish Data Protection Commission's GDPR investigation decisions in EU cases were overruled by majority vote of its European peers at the European Data Protection Board, who demand tougher enforcement action. Only one other country, in one single case, has ever been overruled in this manner.'⁴³ For the DSA, Ireland chose a different authority and restructured its media regulator, Coimisiún na Meán, which already announced a plan to hire 80 staff members for the platform supervision.⁴⁴

Arguably, with the DSA's concurrent and exclusive competencies, the incentive and ability to replicate the GDPR problems is weakened. Ireland, as the country that established the largest players, does not have competence over the risk management obligations that are overseen exclusively by the European Commission. Moreover, even for standard due diligence obligations of these companies, the European Commission can often take over the investigations. At the same time, national DSCs that host VLOPs and VLOSEs, like Ireland, Luxembourg, Germany, and the Netherlands, will still remain crucial. Besides the residual enforcement powers, they retain responsibility over

⁴¹ Julian Jaurisch, 'Here is Why Digital Services Coordinators Should Establish Strong Research and Data Units' (*DSA Observatory*, 10 March 2023) <<https://dsa-observatory.eu/2023/03/10/here-is-why-digital-services-coordinators-should-establish-strong-research-and-data-units/>> accessed 18 September 2023.

⁴² Luca Bertuzzi, 'National Regulators Face an Uphill Battle in Enforcing EU Digital Rulebook' (*Euractiv*, 28 June 2023) <<https://www.euractiv.com/section/platforms/news/national-regulators-face-an-uphill-battle-in-enforcing-eu-digital-rulebook/>> accessed 18 September 2023.

⁴³ Irish Council for Civil Liberties, '5 Years: GDPR's Crisis Point' (ICCL report on EEA data protection authorities 2023) <<https://www.iccl.ie/wp-content/uploads/2023/05/5-years-GDPR-crisis.pdf>> accessed 18 September 2023.

⁴⁴ Bertuzzi (n 42).

administrative tasks, such as granting the researchers access to data held by VLOPs and VLOSEs.

For countries that do not host VLOPs or VLOSEs, the key responsibility will be to administer the system of certification and oversight of the DSA players, such as trusted flaggers and ODS bodies, and monitor the transparency of providers. The DSCs will retain investigatory competence over local providers of digital services, such as providers of various hosting services and infrastructure services. They can also enforce stricter rules against local platforms that exceed the size of small companies (Chapter 9). Looking at the most visited websites in the Member States, it appears that the number of platforms per country will be relatively manageable.⁴⁵

Finally, although the DSA foresees the DSCs to be mainly reactive to the complaints received (Article 53), the national law can endow them with more proactive monitoring duties, such as monitoring the services, sending notifications, issuing of orders in specific cases, or conducting market investigations.

19.2.3 Board

The European Board for Digital Services does not exist at the time of writing. The reason for that is simple: the DSCs in the Member States, who are supposed to be its members, have not come into existence either. As a result, the Commission cannot adopt several acts requiring consultation with the Board (eg delegated acts on user-counting for VLOPs). The Board is envisaged to be an ‘independent advisory group of Digital Services Coordinators’ (Article 61(1)) composed of the DSCs ‘represented by high-level officials’ (Article 62). Under some conditions, other authorities can join the group. The Board may also invite external experts and observers to attend its meetings and cooperate with other bodies. The Board is chaired by the Commission. Whenever the Board votes, a simple majority decides (Article 62(3)). The Commission does not have a vote.

The Board has a crucial role in coordinating the activity of DSCs. It supports general risk management, joint investigations, and standardisation, and gives input for the Commission’s rule-making powers (eg delegated acts). What is key is also its competence to ‘issue opinions, recommendations or advice to Digital Services Coordinators in accordance with this Regulation’ (Article 61(3)(c)) and to ‘support and promote the development and implementation of European standards, guidelines, reports, templates and code of conducts’ (Article 61(3)(e)). Thus, while the Commission has powers to investigate VLOP/VLOSEs and to issue delegated acts or Guidance, the Board takes the lead in orchestrating various ancillary ‘soft-law’ instruments, such as Codes of Conduct. The adoption does not always have a particular prescribed form. Thus, for instance, there is no prescribed adoption act for finalising the Codes of

⁴⁵ ‘Similarweb Rank—Top Websites by Country and Category’ (*Similarweb*) <<https://www.similarweb.com/country/>> accessed 18 September 2023.

Conduct, even though they produce legal effects. However, this defect does not prevent their potential legal review (Chapter 20.2.4).

19.3 Private Enforcement

The DSA's main enforcement focus is on public enforcement and distribution of powers between administrative authorities across the EU.⁴⁶ Its entire Chapter IV deals with enforcement by national public authorities and the European Commission. With two notable exceptions, the DSA's text largely ignores the question of private enforcement. By private enforcement, I mean the legal ability of individuals or their representatives to defend their rights in courts when those rights are violated. However, at a closer look, even though many private claims for violations of the DSA are not foreseen by the DSA, they are not pre-empted by its rules either.⁴⁷ Furthermore, as this chapter will explain, the Court of Justice of the European Union (CJEU) is likely to expect comprehensive mandatory private enforcement to safeguard the DSA's effectiveness.

Private enforcement is most relevant in the context of due diligence obligations. Most due diligence obligations are formulated as *passive regulatory expectations* without explicitly framing them as corresponding rights of affected individuals. If regulatory expectations create any *individual* expectations, they mostly make promises to 'recipients of the services'. These can be consumers, businesses, or non-profit organisations that uploaded information or were otherwise exposed to the service (Article 3(p)).

While the DSA does not regulate most private claims, it explicitly prescribes the availability of damages for individuals (Article 54), and collective redress, including injunctions, for consumer bodies (Article 90). Other private remedies, such as injunctions, are not explicitly foreseen; however, as explained below, they can be inferred as equally mandatory from the DSA's broader framework and Court's pre-existing case law. The DSA further includes a special regime of representation which allows any recipients of the services, including businesses, 'to mandate a body, organisation or association to exercise the rights conferred by this Regulation on their behalf' (Article 86).

In practice, private enforcement will take two main forms: contractual and non-contractual.

Often, 'recipients of the service' are in a *contractual relationship* with the providers of digital services. Where a contractual relationship exists, the private enforcement of due diligence obligations is arguably easier from the legal perspective. In such cases, there is no need to create a new cause of action, and contractual remedies can sometimes be relied upon to enforce what the DSA now prescribes as mandatory rules in legal relationships. For instance, due diligence obligations in content moderation owed to content creators can be potentially litigated by them based on their contractual agreements

⁴⁶ DSA, Recs 124 and 153.

⁴⁷ Franz Hofmann and Benjamin Raue (eds), *Digital Services Act: Gesetz über digitale Dienste* (Nomos 2023) 805 (arguing that art 54 shows clearly that private enforcement is possible).

with providers. The DSA's due diligence obligations in content moderation could be incorporated into user agreements as statutory rights of the users. For this reason, I have called the DSA's rights the creators' charter.⁴⁸

For instance, an influencer using a video-sharing platform relies on a contract to gain access to the platform's distribution service. The DSA's due process provisions that regulate content moderation will modify the rights of content creators against termination, reinstatement, explanation, remedies to such decisions, and arrangements about the publicity of those decisions. For instance, if her content is suddenly demonetised, she can seek explanations and have them reviewed internally by the company; if the provider fails to do so, she can seek damages and reinstatement of the content.⁴⁹

When the contractual relationship between the provider and the recipient of the service is missing, such as in cases of affected parties who suffered privacy invasions, defamation, or the sale of counterfeit products, the private enforcement structure can be provided by *tort law*, such as unfair competition, consumer, and intellectual property law. Enforcement in these cases can be less straightforward.

19.3.1 Of rights and obligations

In its seminal judgment from 1963, *van Gend & Loos*,⁵⁰ the Court held that European law that appears to impose only obligations could implicitly grant corresponding rights to individuals. The Court held that:

Independently of the legislation of member states, community law not only imposes obligations on individuals but is also intended to *confer upon them rights* which become part of their legal heritage. *These rights arise not only where they are expressly granted by the treaty but also by reason of obligations which the treaty imposes in a clearly defined way upon individuals as well as upon the member states and upon the institutions of the community.*⁵¹

In the case law that followed, it was established that:

It follows that only a breach of a rule of EU law which is intended to confer rights on individuals is, in accordance with the first of the three conditions mentioned above, capable of giving rise to State liability. According to well-established case-law those rights arise not only where they are expressly granted by provisions of EU law, but also by reason of positive or negative obligations which those provisions impose in a

⁴⁸ Martin Husovec, 'The DSA as a Creator's Charter?' (2023) 18(2) *Journal of Intellectual Property Law & Practice* 71.

⁴⁹ DSA, arts 17, 20(1), and 20(4) ('it shall reverse its decision referred to in paragraph 1 without undue delay').

⁵⁰ Case C-26/62 *Van Gend & Loos* ECLI:EU:C:1962:42.

⁵¹ *ibid* (emphasis mine).

clearly defined manner, whether on individuals, on the Member States or on the EU institutions...⁵²

Article 54 is the first indication that the DSA imposes not only regulatory obligations upon companies but also confers corresponding rights upon individuals, whose violations might need to be compensated. The second hint of the rights conferral can be found in Article 86, which speaks of ‘exercise the *rights* conferred by this Regulation.’⁵³ Taken together, both provisions provide ‘visible’ parts of the private enforcement architecture.⁵⁴ Admittedly, these two building blocks hardly explicitly state whether national law must provide for injunctions, or information claims, as other typical remedies. But if these visible parts of the DSA are read together with pre-existing case law, the conclusion is inescapable. Consequently, the entire due diligence chapter confers not only obligations but also rights that *must* be equipped by private remedies.

Under the Platform to Business Regulation (P2BR), the non-articulation of private remedies led to a lot of conflicting national case law⁵⁵ and academic discussion about whether private claims of individuals are required as an enforcement framework.⁵⁶ Under the DSA, the situation is much more straightforward. Not only does Article 54 foresee one type of private claim available to individuals, but the entire framework is built around the idea that individuals gain the agency to take care of their own due process rights on platforms. Denying them the ability to enforce such obligations directly and allowing the Member States to limit the redress only to administrative enforcement, would clearly conflict with the ethos of the DSA.

Thus, for instance, as far as injunctions are concerned, the Court is more likely to follow *Muñoz*.⁵⁷ In this case, the Court invoked the status of the EU regulations in primary law as having general application and direct applicability in all the Member States. Building on this, it held that ‘owing to their very nature and their place in the system of sources of Community law, *regulations operate to confer rights on individuals which the national courts have a duty to protect*’.⁵⁸ In that sense, the Court under the DSA is more likely to conclude, as it did in *Muñoz*, that ‘the full effectiveness of the rules on quality standards ... imply that it must be possible to enforce that obligation by means of civil proceedings’.⁵⁹

Despite this European mandate of private enforcement, national law has a key role in defining the *conditions* under which such remedies are available. However, the EU law imposes some minimum requirements for the sake of the effectiveness of the EU rules. In 1999, the Court held in *Courage* that:

⁵² Case 61/21 *JP v Ministre de la Transition écologique* ECLI:EU:C:2022:1015, paras 45–46.

⁵³ DSA, art 86 (emphasis mine).

⁵⁴ To borrow the term from Franck: Jens-Uwe Franck, ‘Individual Private Rights of Action under the Platform-to-Business Regulation’ (2023) 34(4) *European Business Law Review* 525.

⁵⁵ For more on this debate, *ibid*.

⁵⁶ Some national courts have invoked C-604/11 *Genil* 48 ECLI:EU:C:2013:344 to deny it. For a discussion, *ibid* 527.

⁵⁷ Case C-253/00 *Muñoz and Superior Fruiticola* ECLI:EU:C:2002:497.

⁵⁸ *ibid* para 27 (emphasis mine).

⁵⁹ *ibid* para 30.

in the absence of Community rules governing the matter, it is for the domestic legal system of each Member State to designate the courts and tribunals having jurisdiction and to lay down the detailed procedural rules governing actions for safeguarding rights which individuals derive directly from Community law, provided that such rules are not less favourable than those governing similar domestic actions (principle of equivalence) and that they do not render practically impossible or excessively difficult the exercise of rights conferred by Community law (principle of effectiveness)⁶⁰

This means that existing private remedies to enforce the DSA cannot be less favourable or effective than other comparable remedies in the national law. For instance, national or case law could not condition the DSA enforcement to longer limitation periods or a higher burden of proof. The principle of effectiveness means that remedies must be effective, proportionate, and dissuasive.⁶¹ The Court is increasingly applying the above minimum EU floor to procedural rules and specific remedies.⁶²

Although most provisions in the DSA's due diligence chapter confer rights, some arguably are *not sufficiently unconditional* to be able to immediately confer any directly enforceable rights upon individuals or might not have been intended to have such effect.

Consider the main special obligation that applies only to VLOPs and VLOSEs—the general risk management system laid down in Articles 34–35. The system is a dialogue-based regulatory tool that involves multiple parties and grants broad discretion to the providers and the Commission as an executive body. The Commission's exercise of that discretion is to some extent protected against interferences, including by national courts (Article 82(3)). As a result, prior to the Commission, as an exclusive enforcer of the rule, concretising what risk mitigation measures are appropriate given the practice of the provider, it is hard to infer specifically what an individual can personally expect from such rules. This lack of specificity coupled with broad discretion arguably means that as a rule, Articles 34–35 cannot be enforced through private action by individuals or organisations.

This might seem counterintuitive at first. However, there are three potential problems with direct enforceability of Articles 34–35.

First, in *van Gend & Loos*, the Court said the following about the direct effect:

The wording of [a provision of primary law] contains *a clear and unconditional prohibition* which is not a positive but a negative obligation. This obligation, moreover, is not qualified by any reservation on the part of states which would make its implementation conditional upon a positive legislative measure enacted under national law. The

⁶⁰ Case C-453/99 *Courage and Crehan* ECLI:EU:C:2001:465, para 29.

⁶¹ Case C-68/88 *Commission v Greece* ECLI:EU:C:1989:339. For a discussion of the debate on this with further case law, Franck (n 54) 541.

⁶² Case C-295/04 *Manfredi* ECLI:EU:C:2006:461, para 62; Case C-163/21 *PACCAR and others* ECLI:EU:C:2022:863, para 44.

very nature of this prohibition makes it ideally adapted to produce direct effects in the legal relationship between member states and their subjects.⁶³

The Court has repeatedly clarified that ‘an unconditional provision is one which leaves no discretion to the Member States.’⁶⁴ Applying this to the EU regulations, the Court held in *Azienda Agricola* that:

In this respect, although, by virtue of the very nature of regulations and of their function in the system of sources of Community law, the provisions of those regulations generally have immediate effect in the national legal systems without its being necessary for the national authorities to adopt measures of application, *some of their provisions may none the less necessitate, for their implementation, the adoption of measures of application by the Member States...* In the light of the discretion enjoyed by the Member States in respect of the implementation of those provisions, it cannot be held that individuals may derive rights from those provisions in the absence of measures of application adopted by the Member States.⁶⁵

In the context of Articles 34–35, the discretion is vested with the European Commission and not the legislature or authority of the Member State. Moreover, the discretion is also given to the provider. However, the underlying problem is the same. The legal obligation is not sufficiently unconditional if it grants two-level discretion for us to infer what exactly is owed to an individual under those provisions of the DSA. The second and related problem is that with the system of double discretion as outlined above, it is much harder to argue that the provisions intend to grant rights to individuals. Thus, in my view, Articles 34–35, and potentially others that impose broad regulatory discretion upon the authorities or providers, cannot be immediately enforced by individuals.⁶⁶ This will need to be decided on a case-by-case basis.

The third problem relates to how the DSA protects the Commission’s discretion. According to Article 82(3):

When a national court rules on a matter which is already the subject matter of a decision adopted by the Commission under this Regulation, that national court shall not take any decision which runs counter to that Commission decision. National courts shall also avoid taking decisions which could conflict with a decision contemplated by the Commission in proceedings it has initiated under this Regulation. To that effect, a national court may assess whether it is necessary to stay its proceedings. This is without prejudice to Article 267 TFEU.

⁶³ *Van Gend & Loos* (n 50) (emphasis mine).

⁶⁴ Joined Cases C-100/89 and C-101/89 *Kaefer and Procacci v French State* ECLI:EU:C:1990:456, para 26; Case C-8/81 *Becker v Finanzamt Münster-Innenstadt* ECLI:EU:C:1982:7.

⁶⁵ Case C-403/98 *Azienda Agricola v Sardegna* ECLI:EU:C:2001:6, para 26, 28.

⁶⁶ Hofmann and Raue (n 47) 812 present a different view, although without analysing the reasons.

Given that Article 34–35 are an annual exercise of review of the entire service, the Commission always *decides* at the end of the monitoring cycle. It either decides positively or negatively for the VLOP or VLOSE, but in either case, it is the Commission that decides on the compliance. Since courts are not at liberty to interfere with even ‘contemplated’ decisions, it is not clear *when* the national courts could even intervene as the Commission’s decision regarding Articles 34–35 might be either contemplated or finalised in the annual cycle. Naturally, the Commission’s decisions based on Articles 34–35 remain subject to judicial review under Articles 263, 265, and 267 of the TFEU.⁶⁷

Once the Commission exercises its discretion, such as when it finds a violation of the risk mitigation obligation, the third problem is cleared. That said, the second problem might remain if plaintiffs try to privately enforce the follow-up damages in courts. In this case, the Commission formulated specific regulatory expectations from the regulated providers, and if it is valid as a matter of an act of the European Commission, the DSA does not limit the ability of private parties to enforce it in parallel, such as through claims for damages. However, the plaintiffs still need to show that the provision that is the basis of the illegal act was intended to confer rights upon the affected individuals. And even if it does, the additional limitation is that any parallel enforcement must be in line with the principle of *ne bis in idem*. In other words, the follow-up enforcement after violations of Articles 34–35 will not be easy either, and it will require clarifications from the CJEU or a potential legislative upgrade.

19.3.2 What constitutes an infringement?

After accepting that the DSA, in many cases, grants rights to individuals, the second important question is when these obligations are ‘infringed’. Consider the following three provisions in the context of private enforcement:

- Article 17(1): ‘Providers of hosting services shall provide a clear and specific statement of reasons to any affected recipients of the service for any of the following restrictions.’
- Article 15(1): ‘Providers of intermediary services shall make publicly available, in a machine-readable format and in an easily accessible manner, at least once a year, clear, easily comprehensible reports on any content moderation that they engaged in during the relevant period.’
- Article 20(4): ‘Providers of online platforms shall handle complaints submitted through their internal complaint-handling system in a timely, non-discriminatory, diligent and non-arbitrary manner. Where a complaint [succeeds], it shall reverse its decision referred to in paragraph 1 without undue delay.’

⁶⁷ See the debate in chs 9 (designation) and 20 (codes of conduct).

What constitutes a violation of such obligations? Article 17(1) would seem to be violated every single time a statement of reasons is not given. The same appears to be the case for Article 15(1) whenever a report is not published or lacks prescribed qualities, or for Article 20(4) whenever content is not reinstated following the success in appeals. However, how about the obligation to handle complaints ‘in a timely, non-discriminatory, diligent and non-arbitrary manner’? Can circumstances of a single case be sufficient to substantiate the violation of such a standard, or is the comparison with the typical behaviour of the company or industry required? Moreover, consider the obligation under Article 21(2) to ‘engage, in good faith, with the selected certified ODS body with a view to resolving the dispute’. Such obligation is clearly of a systemic nature, and the violation can only be established after investigating how the provider has behaved *in other cases*.

Thus, while all these rules might impose obligations and rights, the violations might sometimes require contextual assessment of practice in other cases, which means that they must be violated *systemically*.

The majority of DSA’s standard due diligence obligations appear to confer rights which can be violated by a single act of non-compliance. In my view, this is clear from the provision on the statement of reasons (Article 17(1)), transparency reports (Article 15), dark patterns (Article 25), transparency of advertising (Article 26) or rights of researchers to access data (Article 40). However, other DSA due diligence obligations require an assessment of the general practice—ie behaviour on a systemic level—to be able to establish violations. This includes compliance with ODS decisions (Article 21(2)), good behaviour of trusted flaggers (Article 22(2)(c)), compliance with anti-abuse provisions (Article 23), and arguably many open-ended standards of Article 20(4), such as timelines or arbitrariness. In my view, this does not mean that the latter type of provisions are not directly enforceable, but only that the infringement test is broader than the circumstances of a single case. The affected plaintiffs, thus, might need to present broader evidence.

19.3.3 Compensatory damages

Article 54 creates a ‘right to seek compensation’ and added at the request of the European Parliament in the following way:

Recipients of the service shall have the right to seek, in accordance with Union and national law, compensation from providers of intermediary services, in respect of any damage or loss suffered due to an infringement by those providers of their obligations under this Regulation.

The provision mandates the availability of pecuniary compensation by providers ‘due to an infringement’ of an ‘obligations under [the DSA]’. Recital 121 emphasises that

there must be a causal link⁶⁸ between the damages suffered by recipients of the service and an infringement of the DSA obligations by a provider.

While Article 54 does not speak of infringement of *rights*, the damage or loss must be suffered due to a violation of individual interests arising from those obligations. As argued above, in my view, the DSA creates individual rights. However, the mere fact alone that regulatory expectations also confer rights on affected individuals does *not* mean that such rights immediately trigger compensation or other remedies in case of every breach. Any compensation for violation of individual rights derived from the DSA must be reviewed against national law that grants such remedies subject to principles of equivalence and effectiveness. Such law subjects the exercise of such claims by fault, evidentiary standards, and limitation periods. A failure to comply with the DSA might violate the rights of several affected individuals at once, but not necessarily lead to an obligation of providers to compensate all or even most of them (eg absent transparency reports). In some cases, the rights derived from the DSA can be also used defensively against private claims pursued by providers.⁶⁹

The liability for damages triggered by infringement of due diligence obligations is meant to be *distinct* from the liability for third-party content regulated by the DSA's liability chapter, without prejudice to it. This is emphasised by Recital 121. The infringement of due diligence obligations by a given provider is about the provider's own wrongdoing and has nothing to do with the potential damage caused by its users' content to others. The distinction is deliberate (Chapter 9.4) and quite easy to maintain in cases where the DSA violation is only remotely connected with the user-caused damage *while* the provider keeps the liability exemption (eg when the submission system was not designed in full compliance with Article 16). In such cases, any liability for damages is limited to refusing the individual breach of process accountability. The situation is somewhat more complicated in cases where a DSA violation is closely connected with the user-caused damage *while* liability exemptions are no longer available (eg where lack of timely removal leads to actual knowledge and potential joint liability with users). In such cases, the DSA can *indicate* to national law that a component of the duty of care for domestic liability was violated. However, the latter cases are very limited scenarios.

⁶⁸ DSA, Rec 121: '... a provider of intermediary services should be liable for the damages suffered by recipients of the service that are *caused* by an infringement of the obligations set out in this Regulation by that provider ...' (emphasis mine). For instance, if an unsafe toy causes choking, the damage is attributable to the seller and the manufacturer. If a marketplace failed to identify that seller in its platform, the national court still needs to determine that there is a causal link between the infringement of art 30 DSA and the choking.

⁶⁹ For instance, a researcher can rely on due diligence obligations in art 40(12) DSA against VLOPs if they are sued under intellectual property law. The same applies if users or providers are relying on due process obligations, such as the implementation of the ODS (art 21), vis-a-vis third parties who might be harmed by such compliance with the DSA.

19.3.4 Injunctions by consumer bodies

The DSA mandates injunction entitlements of qualified consumer groups. Through Article 90, the DSA introduces a much-needed tool of collective private enforcement. It turns consumer organisations into potential ‘private attorneys general’.⁷⁰ The P2BR already included this option for the business-to-business context.⁷¹ However, based on the official notifications at the time of writing, only Austria, Spain, and Ireland have designated qualified organisations to rely on this option.⁷² The business organisations’ collective redress is not being regulated or anticipated by the DSA, but it remains possible if given support in the national law.

In contrast, in the *business-to-consumer context*, the EU started exploring the collective redress of consumer associations in the 2000s.⁷³ Thus, the list of qualified organisations in this area is longer. Recently, the legislation was reformed by a new Representative Actions Directive from 2020.⁷⁴ The DSA, therefore, did not have to invent new rules concerning collective action.⁷⁵ Article 90 of the DSA submits the DSA under the horizontal regime of consumer laws that can be enforced collectively. The Representative Actions Directive⁷⁶ sets out rules to ensure that mechanisms for the protection of the collective interests of consumers exist on the national level. It applies to infringements of all the provisions of the DSA, and its national implementing rules.⁷⁷ Quite conveniently, it also applies to many overlapping legal rules, such as the GDPR, Unfair Commercial Practices Directive, and many others.⁷⁸ The key condition is that the DSA infringement ‘may harm the collective interests of consumers.’⁷⁹ The concept is defined as ‘the general interest of consumers and, in particular for redress measures, the interests of a group of consumers.’⁸⁰ Consumers, in the EU context, are only natural persons who act outside of a profession, craft or trade.⁸¹

⁷⁰ John Coffee, ‘Rescuing the Private Attorney General: Why the Model of the Lawyer as Bounty Hunter is Not Working’ (1983) 42(2) Maryland Law Review 215.

⁷¹ P2BR, art 14.

⁷² DG Connect (EU Commission), ‘List of Designated Organisations, Associations and Public Entities Drawn up and Published Pursuant to Article 14(6) of Regulation (EU) 2019/1150 of the European Parliament and of the Council on Promoting Fairness and Transparency for Business Users of Online Intermediation Services’ (Notices from Member States) [2021] OJ C402/5 <[https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021XC1005\(01\)](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021XC1005(01))> accessed 18 September 2023.

⁷³ On the European history of collective redress, Alexia Pato, ‘Cross-Border Collective Redress in the European Union and Private International Law Rules on Jurisdiction’ (PhD thesis, Universidad Autónoma de Madrid) 87ff <https://repositorio.uam.es/bitstream/handle/10486/682778/pato_alexia.pdf?sequence=1> accessed 18 September 2023.

⁷⁴ European Parliament and Council Directive (EU) 2020/1828 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC [2020] OJ L 409/1 (Representative Actions Directive).

⁷⁵ The DMA is equally added to that list, following art 52 DMA.

⁷⁶ Representative Actions Directive.

⁷⁷ *ibid* art 2(1).

⁷⁸ *ibid* Annex 1.

⁷⁹ *ibid* art 2(1).

⁸⁰ *ibid* art 3(2).

⁸¹ Unfair Commercial Practices Directive, art 2(a); DSA, art 3(c).

Qualified infringements can be pursued collectively only by qualified entities. These must be designated at a national level, although ad hoc qualification remains possible.⁸² The representative actions must give rise to at least two core remedies: injunctive and redress measures. The Member States might also equip the qualified entities with additional tools, such as information relief.⁸³ As for injunctions,⁸⁴ they must be available as interim or final relief regardless of the infringers' negligence or the existence of damage. As for redress measures,⁸⁵ they should cover a broad range of specific remedies 'such as compensation, repair, replacement, price reduction, contract termination or reimbursement of the price paid'. In the DSA context, this will clearly involve content moderation claims and specific performance arising out of disputes with a contractual basis (eg account terminations, or putback claims).

19.3.5 IP injunctions against intermediaries

All holders of intellectual property rights in the EU are entitled to injunctions against intermediaries. Article 8(3) of the InfoSoc Directive and Article 11 (third sentence) of the IP Enforcement Directive prescribe this remedy to the Member States in intellectual property cases.⁸⁶ The cause of action is extensive. Its goal is to facilitate assistance by providers of services whenever rightsholders face a violation of their intellectual property rights, and providers are in a position to help.⁸⁷ These measures, like due diligence obligations, hold the providers of digital services accountable for the provision of some assistance, without making them liable for the underlying content. Because the measures imposed can ask for assistance with the removal or prevention of infringements, there is a potential overlap with the DSA's due diligence obligations.

In practice, injunctions against intermediaries might become one of the explicit causes of action based on the EU law that mandates the availability of injunctive relief to individuals for violations of the DSA due diligence obligations. For instance, a failure to suspend repeated infringers could be requested by the copyright holder as preventive measures by means of such injunctions if a provider fails to comply with their Article 23 obligations. Similarly, a failure to allow traders to comply with some basic disclosures under Article 31 could be litigated by the trademark holders to help prevent infringement of their trademarks. On the other hand, as explained above, risk mitigation obligations, in my view, cannot be enforced through private remedies unless the Commission already exercised its discretion by finding a violation.

⁸² Representative Actions Directive, art 4(6).

⁸³ *ibid* art 7(4).

⁸⁴ *ibid* art 8.

⁸⁵ *ibid* art 9.

⁸⁶ European Parliament and Council Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society [2001] OJ L167/10, art 8(3) (InfoSoc Directive); European Parliament and Council Directive 2004/48/EC on the enforcement of intellectual property rights [2004] OJ L157/45, art 11 (IP Enforcement Directive).

⁸⁷ Martin Husovec, *Injunctions against Intermediaries in the European Union: Accountable but Not Liable?* (CUP 2017).

19.3.6 Cross-border jurisdiction and enforcement

The system of private enforcement enlarges the pool of enforcers of the DSA. But it is also geographically spread much more widely across the EU. While public enforcement is strictly allocated to one of the Member States (or the European Commission) in most cases, private enforcement is much more diversified. Unlike the GDPR,⁸⁸ the DSA contains no special rules concerning private international law. As a result, the general rules of the Brussels Ia Regulation apply.⁸⁹ The general jurisdiction of civil or commercial courts (Article 4 Brussels Ia) will mostly coincide with that of the country of the provider's establishment as a defendant. However, the regulation offers numerous special types of jurisdictions where plaintiffs might be able to seek redress against providers of digital services elsewhere.

For tortious obligations, this includes 'the courts for the place where the harmful event occurred or may occur' (Article 7(2) Brussels Ia). According to established case law,⁹⁰ this potentially includes two jurisdictions: the place of the event giving rise to damage and the place where the damage occurred. The first alternative is not territorially limited, but following *Wintersteiger*, it will often coincide with the providers' place of establishment.⁹¹ In the second alternative, special jurisdiction is available wherever the service is accessible,⁹² but any claims are territorially limited.⁹³ Personality rights cases are a special category under Article 7(2) Brussels Ia, allowing legal and natural persons to pursue geographically unlimited claims in the place of their centre of interest.⁹⁴

In theory, territorial limitation of claims is workable for damages but is hard to apply to injunctions. The usefulness of Article 7(2) Brussels Ia thus seems clearer for the place giving the right to damage than where the damage occurred. In the latter case, the latest case law of the CJEU suggests that an injunction seeking rectification and removal is 'a single and indivisible application' and hence cannot be based on territorially limited jurisdiction but only on the jurisdiction that can rule on the entirety of an application for compensation for damage under existing case law.⁹⁵

⁸⁸ GDPR, art 79(2) ('such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers').

⁸⁹ European Parliament and Council Regulation (EU) No 1215/2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast) [2012] OJ L351/1 (Brussels Ia).

⁹⁰ This was first developed in Case C-21/76 *Handelskwekerij Bier v Mines de Potasse d'Alsace* ECLI:EU:C:1976:166.

⁹¹ Case C-523/10 *Wintersteiger* ECLI:EU:C:2012:220, paras 36–39.

⁹² Case C-251/20 *Gtflifx TV v DR* ECLI:EU:C:2021:1036, para 41 (directing is not a requirement, and thus the scope is very broad). See the debate in Dan Jerker B Svantesson, 'European Union Claims of Jurisdiction over the Internet – an Analysis of Three Recent Key Developments' (2018) 9(2) *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 113.

⁹³ The so-called mosaic approach: Case C-68/93 *Shevill and Others v Presse Alliance* ECLI:EU:C:1995:61; and more recently defended in *Gtflifx TV v DR* (n 92).

⁹⁴ Joined Cases C-509/09 and C-161/10 *eDate Advertising GmbH and Others v X and Société MGN Limited* ECLI:EU:C:2011:685; Case C-194/16 *Bolagsupplysningen and Ilsjan* ECLI:EU:C:2017:766; *Gtflifx TV v DR* (n 92).

⁹⁵ *Bolagsupplysningen and Ilsjan* (n 94) para 48; *Gtflifx TV v DR* (n 92) para 35.

To illustrate the potential problems with this, consider an example of the enforcement of the obligation to publish content moderation reports by a consumer organisation that relies on Article 90 DSA. It is not clear that such an injunction can be granted by the court in whose jurisdiction the service is only being used by consumers, but it is not established. This is because if such an injunction is granted, the content moderation report in its entirety must be inevitably produced and published. Thus, no half-solution to satisfy only one jurisdiction is possible. The same is true for many DSA obligations. Although one can think of account restorations or content put backs that would be localised only for the said jurisdiction, the practicality of such orders is questionable.

On the other hand, the benefit of Article 7(2) Brussels Ia is that it is available to any private plaintiff, including associations for the purposes of collective action.⁹⁶ This is important because the Brussels Ia Regulation also includes special rules for the benefit of consumers (Articles 17–18 Brussels Ia) that are interpreted very strictly by the CJEU. Consumers who were targeted⁹⁷ in their home jurisdiction can also sue in the courts of their domicile in relation to some of their contracts, such as platform-to-user contracts.⁹⁸ But this special consumer jurisdiction is not available to consumer organisations.⁹⁹ Similarly, if a consumer assigns a claim to another consumer in a different jurisdiction, the acquirer of assigned claims cannot use their jurisdiction for the assigned claims.¹⁰⁰ Thus, Article 18 Brussels Ia remains only useful if consumers as natural persons directly try to enforce their DSA rights from their user agreements. If they assign the claims to consumers in other jurisdictions or let consumer associations advance their interests pursuant to Article 86 or 90 DSA, such actions outside the providers' country of establishment must usually rely on Article 7(2) Brussels Ia.

Finally, concerning providers subject to the DSA, but do not have their establishment in the EU, the jurisdiction rules continue to be mostly derived from national law (Article 6(1) Brussels Ia). This is particularly relevant for providers subject to the DSA who only have a legal representative in the EU according to Article 13 DSA or have failed to appoint a legal representative.

19.3.7 Non-judicial enforcement

Collective enforcement also has a non-judicial dimension. The day-to-day life of the DSA rules has nothing to do with the world of authorities and courts. The DSA creates structures that the law can only foresee and incentivise but cannot build; only people

⁹⁶ Case C-167/00 *Verein für Konsumenteninformation v Karl Heinz Henkel* ECLI:EU:C:2002:555 (for consumer associations).

⁹⁷ Joined Cases C-585/08 and C-144/09 *Pammer and Hotel Alpenhof* ECLI:EU:C:2010:740.

⁹⁸ Brussels Ia, art 17(1)(c).

⁹⁹ Case C-89/91 *Shearson Lehman Hutton* ECLI:EU:C:1993:15 ('a legal person which acts as assignee of the rights of a private final consumer, without itself being party to a contract between a professional and a private individual, cannot be regarded as a consumer').

¹⁰⁰ C-498/16 *Schrems v Facebook* ECLI:EU:C:2018:37, para 48 ('an assignment of claims such as that at issue in the main proceedings cannot provide the basis for a new specific forum for a consumer to whom those claims have been assigned').

on the ground can. These structures, such as local organisations analysing threats, consumer groups helping content creators, and communities of researchers, are the only ones to give life to the DSA's tools. They need to be built bottom-up and sometimes locally in each Member State. If their creation fails, the regulatory promises might turn out to be a glorious aspiration.

The DSA's special rule on representation allows businesses, non-profits, and individuals, including consumers, to 'mandate' a body, organisation, or association to 'exercise' their rights conferred by the DSA (Article 86). This includes all the due diligence in the content moderation process, as well as fair design and transparency due diligence obligations that benefit the recipients of the services.

According to Article 86, the representation 'on their behalf' of businesses, non-profits or individuals is possible if 'the body, organisation or association' meets all of the following conditions:

- (a) it operates on a not-for-profit basis;
- (b) it has been properly constituted in accordance with the law of a Member State;
- (c) its statutory objectives include a legitimate interest in ensuring that this Regulation is complied with.

These are extremely broad criteria that allow consumer groups and trade associations to support their members or the wider public. For instance, a trade association or consumer group could represent members in internal dispute resolution or before the ODS bodies. The providers have an obligation to facilitate this, especially in the internal complaint process, where they must 'take the necessary technical and organisational measures' to ensure their complaints are 'processed and decided upon with priority and without undue delay' (Article 86(2)).

Outside of content moderation, the relevant bodies according to Article 86 could step in to help researchers with their data access requests. One can imagine that the universities, for instance, or specialised consortia, would step in to represent their researchers in the data requests procedure.

The unique European challenge for the DSA is that such organisations must almost always be local. Excellent German consumer organisations are unlikely to help Spanish-speaking consumers. Devoted Dutch anti-hate speech groups will not have the skills to find and notify Romanian content. Skilled Estonian groups fighting against hybrid threats will not help in Slovakia. Thus, the capacity needs to be built up across all the Member States to fight all today's unique challenges, ranging across various forms of extremism, terrorism, war propaganda, hate speech, and beyond.

Table 19.2 summarises conditions for five such collective structures which the DSA and related acts envisage but require individuals to build. The important takeaway is that sometimes, these structures can be embedded into the same organisations. They are not mutually exclusive. In fact, the only incompatible matches are: (a) between the ODS bodies and other bodies and (b) between business and consumer collective redress bodies. All other bodies are mutually compatible. Trusted flaggers can also represent users in the DSA processes and seek collective redress in the courts.

Table 19.2 Other enforcement actors

	Representation (Article 68)	Collective redress for consumers (Directive 2020/1828)	Collective redress for businesses (Regulation 2019/1150)	Trusted flaggers (Article 22)	ODS bodies (Article 21)
Character	Non-profit character	Non-profit character	Non-profit character	N/A	N/A
Personhood	An entity with legal personhood	An entity with legal personhood	An entity with legal personhood	N/A	N/A
Objectives	DSA compliance is one of its statutory objectives	DSA compliance and consumer protection is one of its statutory objectives	Pursue collective interests of business users or corporate website users	Expertise in 'detecting, identifying and notifying illegal content'	Expertise in 'an area of illegal content', or 'enforcement of terms and conditions' of one type of platform
Experience	N/A	12 months of actual public policy activity in the area	Pursues its goals on a 'sustained basis'	Submits notices diligently, accurately and objectively	Capable of settling disputes in a swift, efficient and cost- effective manner and in at least one of the official EU languages
Independence	N/A	Independence from influence, except for consumers	Their decision- making is not 'unduly influenced' by third- party financing, such from providers	Independence from online platforms	(a) Independent from platforms and recipients of services, including notifiers (b) Impartiality of staff, whose pay cannot be linked to the outcome of disputes
Disclosure	N/A	Publicly discloses the above requirements, and funding, organisational, management and membership structure	Publicly discloses information on their membership and source of financing	Publicly discloses its functioning and draws reports on its activities	Publicly discloses its functioning, and fair rules of procedure, and draws reports on its activities; the system must function electronically

The above structures offer tools that various organisations can seize and use when representing private interests. For instance, journalists can create communities that help them push against account restrictions and content removals when it concerns their profession. The same organisations can help journalists by representing them

professionally in content disputes with providers before the ODS settlement bodies and, if necessary, seeking redress before courts. Such an organisation could also seize the opportunity and qualify as trusted flaggers and protect their members from hate speech and other illegal behaviour against journalists. Finally, after the organisation is formed and running, it could start negotiating with the platforms on how to further protect journalists on their platforms. They could join the conversations about risk assessments and mitigation, and offer to self-police the quality of the content of its members in exchange for stronger privileges, such as more protection against account suspensions. These can be formalised through the DSA's official Codes of Conduct, making them subject to the Commission's own monitoring.

19.4 Conclusion

This brief chapter could not do justice to all potential issues related to enforcement. At this point, it is hard to say much about public enforcement because the system is only in the making, especially on the national level and before the European Commission. I, therefore, leave closer scrutiny of it to another day. The supranational set-up with the European Commission as the main enforcer offers many opportunities, but also challenges, given the novelty of issues, resource constraints, and risks of politicisation of the oversight.

My conclusion is that while the DSA spends a lot of effort in creating public administrative enforcement, the private enforcement through the courts and also outside of them might do a lot of heavy lifting to give the DSA teeth. Regulators, regardless of how well-staffed and resourced they are, can only follow several cases, and their priorities do not always align with those of individuals. While European strategic litigation culture is still only in its infancy, the DSA gives it a boost by offering a lot of tools to build better digital regulation.

From the US perspective, in which many platforms are steeped, it might sound scary to read about all the possibilities of how individuals and collectives can enforce the DSA. However, as noted by Wilman, European private enforcement is different because we do not have the 'toxic cocktail' of pro-plaintiff procedural rules and punitive damages.¹⁰¹ That is not to say that abuse will not take place and that we should not keep an eye on how individuals might make use of the DSA before the courts. I only mean to give this chapter a big footnote for non-European readers who might a priori assume the environment of high litigation costs, no cost-shifting rules, extensive discovery procedures, and sky-high punitive damages. European private enforcement is much softer. It still hurts, but usually less. And in some Member States, it still takes too long.

¹⁰¹ Folkert Wilman, *Private Enforcement of EU Law Before National Courts* (Edward Elgar Publishing 2015) 11.26.

The DSA as a Co-regulatory System

20.1 Introduction	443	20.2.4 Judicial review of the Codes	453
20.2 Codes of Conduct as European Benchmarks (Articles 45–48)	445	20.3 A Theory of the DSA's Regulatory Design	456
20.2.1 Creation of the Codes	446	20.4 DSA's Global Spillover Effects	459
20.2.2 How binding are the Codes?	447	20.5 Conclusion	461
20.2.3 What can be in the Codes?	450		

20.1 Introduction

The headline story behind the Digital Services Act (DSA) is that it ushers an unregulated industry into a new regulatory reality. This story is undoubtedly true. Many mid-sized companies will face compliance costs that they did not have before. As of August 2024, Big Tech (comprising very large online platforms and search engines (VLOPs/VLOSEs)) has become subject to a seemingly never-ending regulatory dialogue with the European Commission about risk management on their platforms.

However, the DSA creates only a regulatory baseline. Its full harmonisation does not imply that the DSA rules impose the only golden standard of due diligence that cannot be exceeded in practice. The 'DSA-plus' measures are almost by definition expected to accompany the DSA in the years to come. To complement Big Tech's open-ended risk management tasks, the DSA builds a separate co-regulatory arm to inform its scrutiny.

For a regulator in such a dynamic and quickly changing landscape as digital services, there is little choice but to give some agency to providers to satisfy public policy goals. Different societal challenges have different levels of regulatory maturity, and regulators usually know less about potential solutions than the industry. The DSA architecture de facto reroutes society's effort to co-regulation through a mixture of experimentation, industry-consensus building, and, eventually, standardisation.

The story of the internet is largely a story of self-regulation. The global network is based on open standards, such as TCP/IP, HTML, URL or HTTP, produced by non-profit Standard Developing Organisations (SDOs). IETF and W3C, the two most important internet SDOs, evolved out of the original community of academic and governmental developers of the internet.¹ As explained

¹ For more about their governance, Justus Baron and others, *Making the Rules: The Governance of Standard Development Organizations and Their Policies on Intellectual Property Rights* (Nikolaus Thumm ed, EU Publications Office 2019) 60 <<https://data.europa.eu/doi/10.2760/48536>> accessed 17 September 2023.

by Marsden, the internet has always been regulated in a polycentric regulatory model.² He explains that:

The route to this intermingled co-regulatory environment has also been somewhat novel in that it owes as much to bottom-up as top-down co-regulation. Bottom-up can be seen in many standards organizations, content (especially print journalism) and technical regulatory bodies, and top-down in other more traditional standards bodies, and regulatory arrangements inherited from telecoms and broadcasting inheritances. The direction of travel is in almost all cases towards co-regulation, no matter what the basis from which each arrangement starts.³

Technical standards have always been seen as a key component in building the European Union (EU) internal market.⁴ In 1985, shortly before the adoption of the Single European Act (1986), the Council adopted a resolution starting a new approach to standardisation.⁵ The New Approach created opportunities for companies to join in the standards development activities of the European Standard Organisations (ESOs), such as CEN/CENELEC and ETSI, with the help of traditional national standards bodies. In 2012, the EU consolidated the rules through an EU Regulation.⁶ The Standardisation Regulation imposes obligations upon the ESOs and national standard bodies with respect to their governance, including transparency (Articles 3–4), stakeholder participation (Articles 5–6, and 16), and participation of public authorities (Article 7). The Regulation also creates an elaborate system for standardisation agenda setting (Articles 8, 10) and financing European standard development (Article 15).

The DSA thus does not enter an entirely new space. The EU law has several legal instruments that include typical ‘encouragements’⁷ that result in self-regulation.⁸ For instance, in the context of consumer law, traders are encouraged to develop codes to comply with prohibitions of misleading and aggressive practices.⁹ Under Article 40 General Data Protection Regulation (GDPR), associations, and other representative

² Christopher T Marsden, *Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace* (CUP 2011) ch 8.

³ *ibid.*

⁴ Baron and others (n 1).

⁵ Council Resolution of 7 May 1985 on a new approach to technical harmonisation and standards [1985] OJ C 136/1.

⁶ European Parliament and Council Regulation (EU) No 1025/2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC, and 2009/105/EC and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC [2012] OJ L316/12 (Standardisation Regulation).

⁷ These include art 40 GDPR and arts 40 (standards) and 69 (Codes of Conduct) of the Proposed AI Act (Commission, ‘Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (AI Act) and Amending Certain Union Legislative Acts’ COM(2021) 206 final).

⁸ LAJ Senden, ‘Soft Law, Self-Regulation and Co-Regulation in European Law: Where do They Meet?’ (2005) 9(1) *Electronic Journal of Comparative Law* 1.

⁹ European Parliament and Council Directive 2005/29/EC concerning unfair business-to-consumer commercial practices in the internal market [2005] OJ L149/22 as amended by Directive (EU) 2019/2161, art 2(f) (Unfair Commercial Practices Directive).

bodies can initiate the creation of codes ‘to contribute to the proper application’ of data protection law. The DSA goes a step further by embedding some of the Codes of Conduct into its enforcement system, creating clear expectations for Big Tech to join and participate. The result is a clear push toward co-regulation.

The DSA’s mechanism for Codes of Conduct improves the pre-DSA situation. Prior to the DSA, the EU law had a framework for standardisation outlined above, but not for other private ordering. The process was entirely political and the chances of public participation depended on how loudly one could scream. The previous initiatives of the European Commission include the Memorandum of Understanding on Counterfeiting (2011),¹⁰ and Hate Speech Code of Conduct (2016; 2022),¹¹ the Code of Conduct on Disinformation (2018; 2022),¹² and initiatives to protect minors (2022).¹³

The DSA gives the process more structure. Although the framework is still far from ideal, it gives the stakeholders more predictability. At the time of writing, the Commission started convening the first Code of Conduct that might become an official DSA Code of Conduct—the Age-Appropriate Design Code.¹⁴ Another candidate is the existing Disinformation Code of Conduct.¹⁵ The DSA Codes of Conduct, along with standards, represent the new generation of technology regulation in Europe.¹⁶ In this new age, the EU does not shy away from steering and funding private ordering, including through SDOs, such as CEN/CENELEC. The most prominent (and controversial) example of this trajectory is the proposed Artificial Intelligence Act (AI Act), which relies heavily on harmonised standards.¹⁷

20.2 Codes of Conduct as European Benchmarks (Articles 45–48)

The DSA invites stakeholders to formulate more detailed and specific rules through Codes of Conduct. Next to a general provision in Article 45, it also singles out

¹⁰ European Commission, ‘Memorandum of Understanding on the Sale of Counterfeit Goods on the Internet’ <https://single-market-economy.ec.europa.eu/industry/strategy/intellectual-property/enforcement-intellectual-property-rights/memorandum-understanding-sale-counterfeit-goods-internet_en> accessed 6 September 2023.

¹¹ European Commission, ‘The EU Code of Conduct on Countering Illegal Hate Speech Online’ <https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combating-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en> accessed 6 September 2023.

¹² European Commission, ‘The 2022 Code of Practice on Disinformation’ (*Shaping Europe’s digital future*, 31 July 2023) <<https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation>> accessed 18 September 2023.

¹³ For the Better Internet for Kids + strategy, see: European Commission, ‘Special Group on the EU Code of Conduct on Age-Appropriate Design’ (*Shaping Europe’s digital future*) <<https://digital-strategy.ec.europa.eu/en/policies/group-age-appropriate-design>> accessed 18 September 2023.

¹⁴ *ibid.*

¹⁵ European Commission, ‘2022 Strengthened Code of Practice on Disinformation’ (n 15) 2 (‘This Code of Practice aims to become a Code of Conduct under Article 35 of the DSA, after entry into force, regarding Very Large Online Platforms that sign up to its Commitments and Measures.’).

¹⁶ See a comprehensive report by Hans-W Micklitz, ‘The Role of Standards in Future EU Digital Policy Legislation’ (Report commissioned by ANEC and BEUC, 2023) <https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-096_The_Role_of_Standards_in_Future_EU_Digital_Policy_Legislation.pdf> accessed 18 September 2023.

¹⁷ Commission, ‘COM(2021) 206 Final’ (n 7) art 40.

advertising (Article 46), accessibility codes (Article 47), and crisis protocols (Article 48). While many other private ordering schemes will exist, the benefit of official ‘DSA-recognised’ Codes of Conduct is the regulatory structure into which they are embedded. Most of the DSA references to Codes are sprinkled around the special obligations of VLOPs and VLOSEs, which shows that the focus is on the regulation of Big Tech.¹⁸

20.2.1 Creation of the Codes

The creation of Codes begins with the DSA’s mandate in Article 45(1) that the European Commission and the Board ‘shall encourage and facilitate the drawing up of voluntary codes of conduct at Union level to contribute to the proper application of this Regulation.’ Such documents shall take into account ‘the specific challenges of tackling different types of illegal content and systemic risks.’ An official DSA Code of Conduct benefits from the brokering undertaken by the European Commission (Article 45(2)), as well as regular monitoring and evaluation, including publication of the results of such exercises (Article 45(4)). Thus, any new DSA Code of Conduct is a new responsibility for the European Commission and the Board. The European Commission *can* initiate a DSA Code of Conduct where significant systemic risks emerge and concern ‘several’ VLOPs or VLOSEs (Article 45(2)).

If it decides to initiate the process, the Commission invites the concerned VLOPs, VLOSEs, other providers of intermediary services, relevant stakeholders, civil society organisations, and competent authorities to join the process (Article 45(2)). Thus, in the absence of VLOPs or VLOSEs in the sector, the DSA Codes arguably cannot be initiated. The only exceptions are advertising and accessibility codes (Articles 46 and 47) that do not require the presence of VLOPs/VLOSEs. The logic behind this is probably that since the Codes have their primary regulatory relevance directed towards very large players, initiating such Codes in their absence makes no sense. Similarly, if there are not at least two such players, there is no point in discussing what constitutes the best ‘industry’ practice. The Codes of Conduct are thus clearly conceived as industry-wide tools and not only tools for interested players. While the DSA does not specify the threshold for comparability of services that should be included in each Code, arguably, they usually need to constitute somewhat *similar* types of services.

Thus, for instance, if the age-appropriate design code is set up for marketplaces, social media, or app stores, it can hardly apply also to online maps or encyclopaedias, as the latter two only have one VLOP each (Google Maps, and Wikipedia). While the Commission could argue that these platforms are equally ‘concerned’ by rules for social media, based on the unique nature of maps or encyclopaedias, I would argue that the

¹⁸ For an overview, Rachel Griffin and Carl Vander Maelen, ‘Codes of Conduct in the Digital Services Act: Exploring the Opportunities and Challenges’ [2023] Draft paper, Law, AI & Regulation Conference, Erasmus University, Rotterdam <<https://papers.ssrn.com/abstract=4463874>> accessed 18 September 2023.

respective risk profiles differ substantially to be comparable. Thus, the unique position of Wikipedia, for instance, gives it a reasonable excuse to stay out of many Codes of Conduct.

Naturally, *other* private commitments of companies remain possible even after the DSA. All non-EU-specific codes or purely national codes will fall into this category. Such commitments do not qualify as ‘official’ DSA Codes of Conduct under Article 45 with all the oversight structures. This makes sense given that the monitoring of the official Codes is entrusted to the European Commission and Board, which have limited resources, and often no interest in monitoring purely local matters.

Recitals of the DSA mention five relevant initiatives that could be brought into the scope of Article 45 in the coming years: (i) a Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+),¹⁹ (ii) the Product Safety Pledge,²⁰ (iii) the Memorandum of understanding on the sale of counterfeit goods on the internet,²¹ (iv) the Code of conduct on countering illegal hate speech online,²² and (v) the Code of Practice on Disinformation.²³ In Recital 104, it also mentions that another potential area for such initiatives concerns computational propaganda.

20.2.2 How binding are the Codes?

Companies will not usually be able to afford to refuse to join the Codes, and once they do, they gain extra explicit obligations for their risk management cycles. While failing to meet Codes of Conduct obligations does not constitute a direct violation of the DSA, it will reflect badly on their overall compliance for the next assessment cycle. Auditors, for instance, will have to note that providers are not fully compliant.

According to Recital 104, ‘[t]he refusal without proper explanations by a provider of an online platform or of an online search engine of the Commission’s invitation to participate in the application of such a code of conduct could be taken into account, where relevant, when determining whether the online platform or the online search engine has infringed the obligations laid down by this Regulation.’ At the same time, according to Recital 103, ‘[w]hile the implementation of codes of conduct should be measurable and subject to public oversight, this should not impair the voluntary nature of such codes and the freedom of interested parties to decide whether to participate.’ The ‘initiating or adjusting cooperation with other providers’ is part of the expected risk mitigation measures (Article 35(1)(h)), which means that the provider would have to keep justifying why it is not participating even years later.

¹⁹ Commission, ‘A Digital Decade for Children and Youth: The New European Strategy for a Better Internet for Kids (BIK+)’ (Communication) COM(2022) 212 final.

²⁰ Commission, ‘Product Safety Pledge’ <https://commission.europa.eu/business-economy-euro/product-safety-and-requirements/product-safety/product-safety-pledge_en> accessed 19 September 2023.

²¹ European Commission, ‘Memorandum of Understanding on the Sale of Counterfeit Goods on the Internet’ (n 10).

²² European Commission, ‘The EU Code of Conduct on Countering Illegal Hate Speech Online’ (n 11).

²³ European Commission, ‘2022 Strengthened Code of Practice on Disinformation’ (n 15).

What does this back and forth actually mean in practice? It is likely akin to one's mother-in-law's 'invitation' to help in the garden over the weekend. In theory, you can turn it down, but if you do not have a good reason to refuse, many things can go south. Despite proclamations about the voluntary nature, the pull to join is powerful. All incentives seem to be lined up against refusal. By refusing, providers look suspicious and uncooperative, have to keep explaining themselves, and even miss the opportunity to influence the wording of such Codes.

For *signatories*, compliance with the DSA Codes of Conduct becomes part of the risk management exercise. VLOP/VLOSE compliance officers even have it in their job description to monitor internal compliance 'with commitments made under the codes of conduct' (Article 41(3)(f)). The obligation, however, only applies to the DSA's general and advertising Codes of Conduct and Crisis Protocols. Thus, once a provider signs a Code of Conduct, the DSA imposes an obligation to monitor compliance. Finally, the auditors are also specifically tasked to review compliance with the DSA's general and advertising Codes of Conduct and Crisis Protocols (Article 37(1)(b)).

If the European Commission and the Board detect a '*systematic* failure to comply with the codes of conduct', they 'may invite the signatories' of such codes 'to take the necessary action' (Article 45(4)). Thus, it is obvious that a single violation in isolation means little. The regulator cannot simply base their findings of incompatibility on mere violation of the relevant Codes of Conduct. However, undeniably, such a situation *indicates* that VLOPS or VLOSEs might be falling short of their general obligation to manage risks according to Articles 34–35. If further instances or similar behaviour arises and is detected, the Codes of Conduct effectively flesh out the DSA's rules of risk management. This is because the general risk management obligations are worded very broadly, potentially accommodating a broad range of risk measures and areas.

The Codes of Conduct thus embed into the enforcement system an obligation on providers to *justify* why they did not join relevant Codes of Conduct, and if they did, why they did not fully comply with them. If they can present good reasons, they might be off the hook. However, in the absence of good reasons, providers refusing to join or comply raise suspicion about the sincerity of their efforts and immediately draw a target on their backs. The Commission should be, however, very cautious in always equating non-compliance with bad faith. As noted above, the key benefit of co-regulation is that it is less 'sticky' and allows stakeholders to renegotiate and swiftly update the outdated. If the Commission adopts a very uncompromising stance when companies can walk away from their commitments, or their parts, they might lose the benefits. To facilitate this, it might be worth outlining in the Codes specific instances where the Commission is willing to accept the justification of the providers, such as inefficiency or the outdated character of previously agreed rules. Obviously, companies could equally be expected to substantiate such claims.

For *everyone* else but VLOPs and VLOSEs, the compelling effects of the Codes of Conduct described above do not exist. This can create a problematic dynamic. Some signatories of Codes can be held accountable for their promises while others cannot, and are not even monitored on their behaviour. For instance, if a particular action of a

VLOP depends heavily on the creation of conditions by other players in the ecosystem (eg to implement a specific labelling system or produce some data sets), the VLOP might legitimately struggle to comply as the conditions for compliance were not created by others.

Online platforms other than VLOPs are in a special situation. They can be invited to become signatories, but they are not subject to special due diligence obligations. Thus, they do not need to worry about the annual regulatory dialogue about risk management. However, the courts can potentially take the Codes of Conduct into account when interpreting more open-ended provisions, such as those about dark patterns (Article 25), protection of minors (Article 28), design of interfaces (Article 16), and fair content moderation (Article 14).

Finally, Codes of Conduct are not binding upon the *European Commission, DSCs or courts*. As noted by Recital 104, compliance with them does not ‘in itself presume compliance with the DSA’. Thus, from the companies’ perspective, they hardly offer safe harbours. From the regulator’s perspective, they serve as a way to increase the benchmarks of the regulatory environment and key performance indicators (KPIs) without changing the law.

That being said, it is clear that establishing violations of Articles 34–35 is much more difficult for the European Commission if it wants to exceed the obligations present in the Codes. In such cases, it must present evidence to substantiate the failures of *appropriate* interventions, which inevitably rely on how a company compares with others in the industry. Thus, for the European Commission, the Codes are a very convenient way to increase the bar without having to produce any factual evidence.

To conclude, Codes of Conduct are hardly ‘voluntary’, although they are certainly not binding in the same way as the typical DSA provisions. My test here is rather simple: if you cannot easily refuse being dragged into an exercise that will load you with extra work to do, and someone with the ability to fine you will even evaluate your work if you are deemed as not doing a good enough job, you are probably not doing it as a choice. Thus, while Recitals 88–89 conceptualise general Codes of Conduct as ‘self-regulatory measures’, the more accurate description would be co-regulatory measures for three main reasons: first, participation is not entirely voluntary for VLOPs and VLOSEs; second, regulators initiate, facilitate, and monitor compliance; and third, the agreed-upon standards of efforts constitute best-practice evidence provided by the industry itself that is likely to serve the regulator when enforcing the general risk mitigation.

Codes of Conduct *expect* companies to join and articulate industry best practices, partly against their own interests. This is why participation is not entirely voluntary. The company’s main prerogative is the ability to form them through dialogue. The public policy goals are set by Article 34 DSA, and the focus is picked by the European Commission. They effectively gather and codify evidence of what constitutes an industry best practice as they are formulated by the companies themselves. The intuition is that if similar providers agree on something as appropriate, it sets a baseline for good risk mitigation practice. That baseline can be moved but will trigger questions to which

the provider will have to be able to respond. Codes of Conduct are *prima facie* evidence of optimal efforts. This, in turn, makes it cheaper for the European Commission to punish providers on the basis of Articles 34–35 as it does not have to establish the baseline through evidence of its own.²⁴

20.2.3 What can be in the Codes?

The secret sauce of the Codes is that the discussions are not happening in an information vacuum. The auditing reports from previous years, along with accompanying documents, allow other stakeholders to target their discussion, and most importantly, to mutually benchmark providers' practices or resources used. The cross-industry comparison allows the Commission to better articulate its demands, and along with transparency reports, allows civil society to meaningfully join the conversation.

20.2.3.1 General Codes of Conduct

The goal of the exercise is to draw up a document which will set out 'commitments to take specific risk mitigation measures,' as well as a 'regular reporting framework on any measures taken and their outcomes' (Article 45(2)). An example in this regard can be the Code of Practice on Disinformation (2022), which includes specific commitments as to how to demonetise disinformation and allow access to relevant data.²⁵ The specific risk management measures should mirror the size and capacity of different signatories (Article 45(3)).

The main content of the general Codes is foreseen by Article 35 DSA which asks companies to 'put in place reasonable, proportionate and effective mitigation measures, tailored to the specific systemic risks identified'. Since the scope of risks is truly broad, the mandate for Codes is also extremely broad. It covers questions, such as: (a) the design of their services, (b) content moderation processes, (c) testing and adapting their algorithmic systems, including their recommender systems, (d) the design of their advertising systems, and (e) the back-end internal processes (eg resources, testing, or training). Thus, the public and non-public faces of digital services can be scrutinised for their handling of various relevant risks (Chapter 15). Very little is off-limits.

In other words, the scope is potentially so broad that it makes more sense to discuss what *cannot* be in the Codes. The DSA itself says little about the limits of such Codes; however, some limits can be inferred. The Codes must be designed in full compliance with law, including competition and data protection law (Article 45(1)). They obviously could not commit companies to task their employees to work in conditions that are against employment law, or demand interventions that would otherwise violate

²⁴ The violation of Codes of Conduct in itself is insufficient to establish DSA violations. The DSA rightly insists on violation of its legal provisions as the key requirement—art 51 ('under this Regulation'), art 52 ('infringements of this Regulation'), art 73(1) ('the relevant provisions of this Regulation'), and art 74 ('provisions of this Regulation').

²⁵ European Commission, 'The 2022 Code of Practice on Disinformation' (n 12).

fundamental rights, such as the freedom of expression. Among the limits, competition and data protection law are likely to be taken the most seriously because they are backed by specific independent agencies that can step into the process. Unfortunately, the situation is more complicated for other fundamental rights, such as freedom of expression, where the key voice will be likely that of NGOs.

20.2.3.2 Advertising Codes of Conduct

Advertising Codes of Conduct (Article 46) open the DSA system to a much broader set of players, such as those who broker the sale of *advertisements*. Those players, such as advertising networks, do not usually constitute hosting services, much less online platforms,²⁶ but they are key elements in ensuring that the information on every single advertisement flows from the advertiser to the publisher to the consumer and getting all the relevant details into the advertisement repositories created under Article 39 DSA.

There is no prerequisite for advertising Codes of Conduct to be created only by the VLOPs/VLOSEs in the market. The European Commission is only tasked to ‘encourage the development’ of such rules before February 2025. The advertising Codes of Conduct should go beyond the DSA’s subject matter by covering ‘online platforms and other relevant service providers, such as providers of online advertising intermediary services, other actors involved in the programmatic advertising value chain, or organisations representing recipients of the service and civil society organisations or relevant authorities’ (Article 46(1)). The idea is clearly to potentially involve the entire advertising supply chain, and for them to be among the signatories, alongside online platforms. The latter is clear from the fact that the provision speaks of ‘transparency for actors in the online advertising value chain beyond’ what the DSA already requires from online platforms or VLOPs.

The Commission must make sure that the advertising Codes of Conduct ‘pursue an effective transmission of information that fully respects the rights and interests of all parties involved, as well as a competitive, transparent and fair environment in online advertising’ (Article 46(2)). The expected minimum content of such Codes of Conduct should relate to how the data about advertising is labelled, disclosed, and presented by online platforms to users, how the advertising repositories work, and sharing information concerning data monetisation. If the advertising Code of Conduct is accepted by a VLOP or VLOSE, they become part of its risk management systems. Compliance officers must take them into account, and auditors must check compliance with them.

20.2.3.3 Accessibility Codes of Conduct

The only type of Code of Conduct with no legal connection to risk mitigation is the Accessibility Code of Conduct according to Article 47. This provision was not in the Commission’s initial proposal or the mandates of any of the co-legislators. Instead, the European Parliament wanted to have hard-law obligations for platforms to be

²⁶ However, the advertising exchanges are more of an open case as they effectively function as public B2B marketplaces for advertising.

accessible to people with disabilities. However, this raised several questions, starting with the clear overlap with the Accessibility Directive,²⁷ at least for what that directive categorises as ‘e-commerce services’.

The mandate of the accessibility Codes of Conduct concerns improving ‘access to online services that, through their initial design or subsequent adaptation, address the particular needs of persons with disabilities’ (Article 47(1)). They should be concerned with at least the following objectives (Article 47(2)):

- (a) designing and adapting services to make them accessible to persons with disabilities by making them perceivable, operable, understandable, and robust;
- (b) explaining how the services meet the applicable accessibility requirements and making this information available to the public in an accessible manner for persons with disabilities;
- (c) making information, forms, and measures provided pursuant to this Regulation available in such a manner that they are easy to find, easy to understand, and accessible to persons with disabilities.

20.2.3.4 Crisis Protocols

The final special type of Code is the so-called Crisis Protocol (Article 48). The idea of crisis protocols was developed in the wake of the Christchurch terrorist attack in New Zealand,²⁸ in which the perpetrator live-streamed the attack on social media to spread his message. Crisis protocols, such as Christchurch Call Crisis Response Protocol, are thus intended to facilitate rapid response in ‘crises’. Its usefulness can be illustrated by an example where it was clear it should have been employed: the 2022 terrorist attack on the gay community in Slovakia showed that a failure of local authorities to use the Christchurch Crisis Response Protocol or tools envisaged by the Terrorist Content Regulation meant that it took weeks for VLOPs to takedown the antisemitic and terrorist manifestos of the attacker.²⁹

A crisis protocol under Article 48(1) can be initiated by the European Commission upon recommendation of the Board. The Protocols should remain voluntary and their use ‘be strictly limited to extraordinary circumstances affecting public security or public health’ (Article 48(1)). This excludes, for instance, their use for commercially sensitive situations that merit a faster response, such as enforcement against illegal streaming of live sports events. One of the prominent examples of principles for such protocols is civil society’s Declaration of Principles for Content and

²⁷ European Parliament and Council Directive (EU) 2019/882 on the accessibility requirements for products and services [2019] OJ L 151/70.

²⁸ ‘Christchurch Mosque Shootings’ (*Wikipedia*, 16 September 2023) <https://en.wikipedia.org/w/index.php?title=Christchurch_mosque_shootings&oldid=1175688216> accessed 18 September 2023.

²⁹ Katarína Drevená, Jakub Rybníkar, and Jakub Rybár, ‘Teroristický Útok Na Zámockej Ulici v Bratislave: Bezprostredné a Preventívne Aktivity Rady Pre Mediálne Služby Na Zamedzenie Šírenia Nelegálneho a Škodlivého Obsahu’ (Slovak Council for Media Services 2022) <https://rpms.sk/sites/default/files/2022-12/Teroristicky_utok_na_Zamockej_ul_Bezprostredna_a_preventivne_aktivity_RpMS_na_zamedzenie_sirenia_nelegalneho_a_skodliveho_obsahu.pdf> accessed 18 September 2023.

Platform Governance in Times of Crisis,³⁰ which partly relates to the Commission's Recommendation on the non-binding guidelines for the identification of conflict-affected and high-risk areas.³¹

The Protocols should be drafted by the providers. The European Commission's drafting role is unclear. The Commission can invite other authorities and civil society groups to participate. The Protocols aim to highlight how regular DSA obligations must be adopted for extraordinary circumstances, such as through staffing and special communication channels. The text of the Protocol should determine the questions of when to activate them, for how long, and what this means in real terms. It should also include provisions on transparency and safeguards once activated (Article 48(4)). The safeguards should address any negative effects on exercising the fundamental rights enshrined in the EU Charter, particularly negative effects on the freedom of expression and information and the right to non-discrimination.

The use of Crisis Protocols, including their negative effects, can be assessed within the risk management framework of VLOPs and VLOSEs. Similarly, as with general Codes of Conduct, compliance with them is embedded in the oversight framework.

20.2.4 Judicial Review of the Codes

Standards and Codes of Conduct should not be seen as an escape path from fundamental rights obligations. As emphasised by the Court in *Elliott*, standards which have legal effects based on EU law remain part of the legal system and are thus subject to fundamental rights.³² The same should be true for co-regulatory Codes of Conduct that rely on the EU's institutional scaffolding and sometimes borrow from its enforcement frameworks.³³

According to the settled case law of the Court, even non-binding rules can be subject to proceedings for a preliminary ruling under Article 267 of the Treaty on the Functioning of the European Union (TFEU).³⁴ The Court retains 'jurisdiction to give preliminary rulings on the interpretation of EU law and the validity of acts adopted by the EU institutions without exception'.³⁵ The Court is thus able to provide interpretation and even examine the validity of such measures, regardless of the fact that they do not have binding effect.³⁶ In *FBF*, for instance, the Grand Chamber reviewed the

³⁰ Access Now, 'Declaration of Principles for Content and Platform Governance in Times of Crisis' (2022) <<https://www.accessnow.org/cms/assets/uploads/2022/11/Declaration-of-principles-for-content-and-platform-governance-in-times-of-crisis.pdf>> accessed 18 September 2023.

³¹ Commission Recommendation (EU) 2018/1149 on non-binding guidelines for the identification of conflict-affected and high-risk areas and other supply chain risks under Regulation (EU) 2017/821 [2016] OJ L208/94.

³² Case C-613/14 *James Elliott Construction v Irish Asphalt* ECLI:EU:C:2016:821; Case C-171/11 *Fra.bo SpA v DVGWECLI*:EU:C:2012:453; Case C-630/16 *Anstar Oy* ECLI:EU:C:2017:971.

³³ Christina Angelopoulos and others, 'Study of Fundamental Rights Limitations for Online Enforcement through Self-Regulation' (Institute for Information Law (IViR) 2015) <<https://hdl.handle.net/11245.1/7317bf21-e50c-4fea-b882-3d819e0da93a>> accessed 10 August 2023.

³⁴ Case C-188/91 *Deutsche Shell* EU:C:1993:24, para 18.

³⁵ Case C-911/19 *Fédération bancaire française (FBF)* ECLI:EU:C:2021:599, para 53.

³⁶ *ibid* paras 54, 56.

validity of non-binding guidelines on retail banking products adopted by the European Banking Authority.³⁷

One complication for the DSA Codes of Conduct is how they are ‘adopted.’ Article 45(1) says that ‘[t]he Commission and the Board shall encourage and facilitate the drawing up of voluntary codes of conduct at Union level to contribute to the proper application of this Regulation.’ Article 63(1)(e) then speaks of the Board’s role to ‘support and promote the development and implementation of ... code of conducts.’ Thus, it would seem that the industry is in charge of agreeing upon the contents and finalising the rules. However, Recital 107 invites the Commission to ‘include evaluation mechanisms in drawing up the codes of conduct,’ and potentially invite the EU Fundamental Rights Agency or the European Data Protection Supervisor to comment on the codes. Article 45(3) then reiterates that the Commission ‘shall aim to ensure that the codes of conduct clearly set out their specific objectives, contain key performance indicators.’ It is not clear how the Commission or Board can assure any contents without having some final say. It is even less clear how the Commission, in its enforcement capacity, would know what is the final text of such documents if there is no formal act that seals the text of particular versions. It seems implicit that the text is adopted by stakeholders and only offered to the Commission.

The Commission initiates, evaluates, and monitors compliance and may issue fines. However, fines are not based on Codes of Conduct but on Articles 34–35 that underlie them, and for which they provide evidence of best practices. Thus, while the Commission does not draw up the documents, it ‘adopts’ them at the latest when it starts using them against companies because this act lends them certain legal consequences (eg Articles 41(3)(f), 45(4), and 75(2)). The situation is similar to harmonised standards because the standard-setting process is not controlled by the authorities. In *Elliott*, a case dealing with harmonised standards, the Court reminded that on the basis of Article 267 TFEU, it has the ‘jurisdiction to interpret acts which, while indeed adopted by bodies which cannot be described as “institutions, bodies, offices or agencies of the Union”, are by their nature measures implementing or applying an act of EU law.’³⁸ Having said that, the legal effects of Codes of Conduct are somewhat weaker as they serve as *prima facie* evidence of industry consensus that ‘only’ feeds into the risk management system.

Thus, in my view, Codes of Conduct based on Article 45 can potentially be subject to interpretation and invalidation by the Court in the preliminary reference procedure (Article 267 TFEU). This also implies that such documents are part of the EU law, and subject to fundamental rights scrutiny as any other acts of the EU institutions. Therefore, the Court can invalidate not only them on the grounds of going beyond the envisaged remit of statutory text but also for violating fundamental rights.

³⁷ *ibid.*

³⁸ *Elliott* (n 32) para 334.

The same is potentially true for other DSA-related guidance or recommendations issued by the Board.³⁹ In *FBF*, the Court issued a strong reminder to regulators who might overstep their mandate when it held the following:

to accept that the [European Banking Authority] may freely issue guidelines, irrespective of the specific framework established by the EU legislature, would be liable to undermine the allocation of powers between the institutions, bodies, offices and agencies of the European Union ... It follows from the foregoing that the EBA has competence to issue guidelines only to the extent expressly provided for by the EU legislature and that it is for the Court of Justice, in order to answer the third question, to ascertain whether the contested guidelines fall within the EBA's powers, as established by that legislature.⁴⁰

In contrast, the possibility of a *direct annulment challenge* to such Codes of Conduct based on Article 263 TFEU is more problematic. The key requirement under the case law is that all measures whose invalidation is sought must have 'binding legal effects'.⁴¹ According to case law, 'only measures producing binding legal effects of such a kind as to affect the applicant's interests by clearly altering his legal position constitute acts or decisions open to challenge by an application for annulment'.⁴² The Court has repeatedly held that 'any provisions adopted by the institutions, *whatever their form*, which are intended to have binding legal effects are regarded as "challengeable acts" for the purposes of Article 263 TFEU'.⁴³ It previously recognised legal effect even for supposedly non-binding acts, such as opinions, recommendations, or even informal measures, such as emails, oral statements, or letters.⁴⁴ However, the Court requires existence of a legitimate legal basis for the adoption of the act.⁴⁵ The DSA, as noted above, only indirectly confers such powers by tasking the Commission and Board to assist with creation of these Codes, and even more indirectly relies on them in then follow-up enforcement as evidence.

At the same time, Codes are also an avenue through which the EU bodies can exert regulatory power.⁴⁶ Depending on their content, they can arguably lay down specific expectations, thus fleshing out pre-existing obligations under Articles 34–35 DSA.⁴⁷ The argument against the direct challengeability would be to point to cases like *Netherlands v Council*⁴⁸ or *FBF*.⁴⁹ In the latter case, the Grand Chamber considered that product guidelines that only try to persuade and are drafted in non-mandatory

³⁹ For guidance, C-16/16 P *Belgium v Commission* EU:C:2018:79, para 30.

⁴⁰ *FBF* (n 35) paras 72 and 75.

⁴¹ *ibid* para 36.

⁴² Case 151/88 *Italian Republic v Commission of the European Communities* ECLI:EU:C:1989:201.

⁴³ *Belgium v Commission* (n 39).

⁴⁴ Viktor Luszcz, *European Court Procedure: A Practical Guide* (Hart Publishing 2020) 112.

⁴⁵ Case T-113/89 *Nefarma* ECLI:EU:T:1990:82, para 69.

⁴⁶ Case T-36/14 *St'art and Others v Commission* ECLI:EU:T:2015:13, para 29.

⁴⁷ Case T-258/06 *Germany v Commission* ECLI:EU:T:2010:214, para 31.

⁴⁸ Case C-58/94 *Kingdom of the Netherlands v Council of the European Union* ECLI:EU:C:1996:171, paras 25–26.

⁴⁹ *FBF* (n 35).

language were considered to not have binding legal effects, even though they clearly influence market behaviour.

Codes of Conduct, however, have a stronger legal framework behind the adopted commitments. The acceptance of obligations and their subsequent violation provides *prima facie* evidence of a violation of Articles 34–35, with all its corresponding consequences. There is not automatism, to be sure, however, the companies will have to justify themselves against such pre-established baselines. In the coming years, it will be crucial to observe how the Commission institutionalises the tasks, what language it adopts, and how it weaves the Codes into its enforcement system. If the Commission and Board assume a strong steering role, the argument against them being challengeable acts for the purposes of Article 263 TFEU becomes weaker. The executive power should not have it both ways. With legal effects and procedural convenience should also come judicial review.

The challenge of Article 263 TFEU is, however, more likely to succeed when it is pursued by VLOPs and VLOSEs. As noted above, other participants are not even indirectly legally bound by such commitments. While non-VLOPs might be subject to spillover effects of such Codes, that is probably too remote to substantiate the necessary legal effects. In any case, all these other participants that cannot rely directly on Article 263 TFEU can seek an invalidation through a preliminary reference arising out of a dispute. For instance, in a dispute about data access under Article 40 before national courts, researchers could argue that the Code of Conduct that limits their access is invalid or wrongly interpreted. In such a case, the court of the Member States could rely on Article 267 TFEU and lodge questions to Luxembourg.

20.3 A Theory of the DSA's Regulatory Design

The DSA's risk management system, along with Codes of Conduct, is probably best described as a form of 'responsive regulation'⁵⁰ that delegates various parts of the regulation to regulated companies and their unregulated competitors (where providers investigate and mitigate risks), and public interest groups (where researchers and NGO investigate risks). As explained by Ayres and Braithwaite, this approach allows states to retain many of the benefits of *laissez-faire* governance without abdicating the responsibility of solving market failures. In their classification, the DSA model is a form of 'enforced self-regulation'.⁵¹ Across the book, I tend to use the term co-regulation instead because it better captures the idea for the general audience in the European setting.⁵² However, the key point is that it is a type of regulation that is adopted as an alternative

⁵⁰ Ian Ayres and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (OUP 1992) 4.

⁵¹ Nicolo Zingales, 'The DSA as a Paradigm Shift for Online Intermediaries' Due Diligence: Hail to Meta-Regulation' [2022] Verfassungsblog <<https://verfassungsblog.de/dsa-meta-regulation/>> accessed 18 September 2023.

⁵² Senden (n 8); Cary Coglianese and Evan Mendelson, 'Meta-Regulation and Self-Regulation' in Robert Baldwin, Martin Cave, and Martin Lodge (eds), *The Oxford Handbook of Regulation* (OUP 2010) <<https://doi.org/10.1093/oxfordhb/9780199560219.003.0008>> accessed 18 September 2023.

to typical command-and-control regulation where the regulator enforces prescriptive rules.

As argued by Ayres and Braithwaite, the crucial question of regulation is when to *punish* and when to *persuade*.⁵³ They argue against consistent reliance on either punishment or persuasion. Drawing on Scholz's game-theoretical work,⁵⁴ they argue for regulators to adopt a mixed tit-for-tat strategy when overseeing regulated firms.⁵⁵ Building on Axelrod's path-breaking work on cooperation, the idea is that the tit-for-tat strategy creates long-term reciprocity, and thus cooperation. The mechanism is simple. Companies that repeatedly interact eventually realise that cooperation with a tit-for-tat-minded regulator may cost companies in the short-term but will make them better off in the long run. As eloquently explained by Ayres and Braithwaite:

Scholz models regulation as a prisoner's dilemma game wherein the motivation of the firm is to minimize regulatory costs and the motivation of the regulator is to maximize compliance outcomes. He shows that a [tit-for-tat (TFT)] enforcement strategy will most likely establish mutually beneficial cooperation, under assumptions he believes will be met in many regulatory contexts. TFT means that the regulator refrains from a deterrent response as long as the firm is cooperating; but when the firm yields to the temptation to exploit the cooperative posture of the regulator and cheats on compliance, then the regulator shifts from a cooperative to a deterrent response. Confronted with the matrix of payoffs typical in the enforcement dilemma, the optimal strategy is for both the firm and the regulator to cooperate until the other defects from cooperation.⁵⁶

Scholz's insights and further elaboration by Ayres and Braithwaite are useful for conceptualising the DSA enforcement and the role of Codes of Conduct. VLOP/VLOSEs and the European Commission are involved in long-term repeated interactions. The annual review cycle epitomises this most clearly. The VLOP/VLOSE's experimentation to meet public policy goals, the industry-wide Codes of Conduct, and their annual monitoring by reports and audits give the European Commission ample opportunity to infer the willingness of companies to cooperate. The Commission can benchmark the enthusiasm and visible steps of VLOPs/VLOSEs. This clear *detectability* of whether persuasion is working supports the emergence of cooperation.

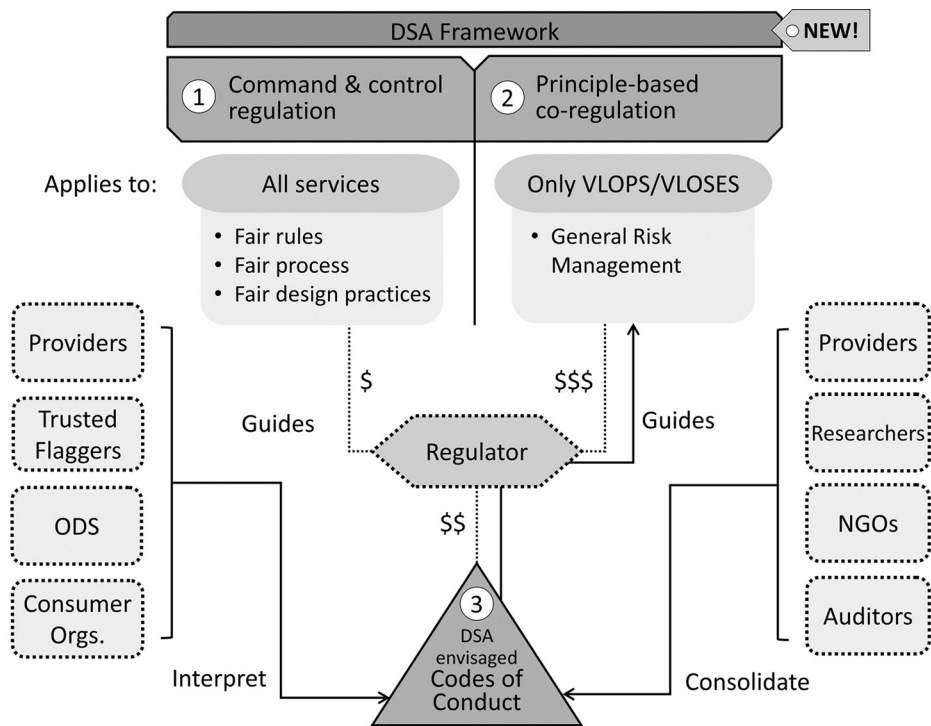
The above dynamic offers many lessons for the interaction between VLOP/VLOSEs and the European Commission in the context of the DSA. If the Commission can credibly retaliate to punish a refusal to cooperate (ie compliance), the companies are likely to respond by cooperation. In my view, this is where the Codes of Conduct play a key role. They constitute a cheaper way for the European Commission to establish

⁵³ Ayres and Braithwaite (n 50) 21.

⁵⁴ John T Scholz, 'Cooperative Regulatory Enforcement and the Politics of Administrative Effectiveness' (1991) 85 *American Political Science Review* 115.

⁵⁵ Ayres and Braithwaite (n 50) 5.

⁵⁶ *ibid* 21.



Number of \$ signs represents relative cost to regulator for meting out punishment for violation of each aspect of DSA

Figure 20.1 The DSA's regulatory architecture

violations of Articles 34–35. Along with prescriptive obligations of due process in content moderation, they are the most likely to be taken up by regulators to mete out punishment. Furthermore, to be an effective tit-for-tat-minded regulator, the European Commission needs fast and cheap reasons under which it can punish non-cooperating companies. The resulting picture is set out in Figure 20.1.

Thus, the existence of Codes has potentially an important practical effect on mutual interactions. It forces companies to not only develop compliance internally but also to articulate industry consensus and be subject to simple detection of its violations. However, it is key that the Commission instead of being slow to anger, always responds quickly to a provocation.⁵⁷ Ayres and Braithwaite offer numerous useful strategies for regulators on how to escalate sanctions (eg to start with formal letters and escalate further).⁵⁸

To conclude, looking at the incentives, it seems that the Member States, stakeholders, and the Commission have all the motivation to push for Codes of Conduct. For the Member States, because the DSA imposes limits on national rule-making, it is likely to channel any *national* frustrations into the European level, especially through Codes of

⁵⁷ Robert M Axelrod, *The Evolution of Cooperation* (Basic Books 1984) 11ff.

⁵⁸ Ayres and Braithwaite (n 50) 35ff.

Conduct (Chapter 17). For the Commission, they offer benefits because it will not have to produce as much factual evidence to fine companies when enforcing Articles 34–35. And finally, for stakeholders, it is the only way their voice can be heard and accepted in the context of risk management due to the limits of private enforcement (Chapter 19).

The DSA's regulatory approach has advantages compared to command-and-control regulation. It is much less '*sticky*' and allows *faster deployment* and *adoption* of the rules. Thus, the regulator must be less worried about path dependence. But co-regulation also poses numerous new challenges as to regulatory capture, legitimacy, and accountability.⁵⁹

Ayres and Braithwaite offer one design feature as an antidote to regulatory capture.⁶⁰ Tripartism is a process in which relevant public interest groups become the fully-fledged third player in the interactions between the regulator and regulated companies.⁶¹ Their role is to prevent regulators from being captured and corrupted by the firms. In the DSA's context, this role is played by civil society, which can participate in the Codes and Conduct, along with researchers who feed into the risk investigation and compliance. The potential weakness of this model is that, as noted in Chapter 19 and this chapter, the NGOs have limited ability to challenge the decisions of the regulator regarding VLOP/VLOSEs. Thus, their ability to step into the interactions remains limited. Going forward, this ability should be strengthened.

20.4 DSA's Global Spillover Effects

Anu Bradford, inspired by David Vogel's work on the California Effect,⁶² famously coined the term 'Brussels Effect' for situations where the EU's rules have spillover effects in other markets.⁶³ She argued that the Brussels Effect will materialise only if the regulator regulates 'inelastic targets' that are not able to flee to less regulated jurisdictions, and when companies' benefits of adhering to a single standard exceed the opportunity costs of laxer standards in other markets.⁶⁴ Her notion of the Brussel Effect focuses more on spillovers than regulatory imitation.

Following the DSA's adoption, many wondered whether other countries are likely to follow suit as with the GDPR, or whether companies are likely to export the implementation of the DSA beyond the EU borders. At the time of writing, some countries, such as Brazil,⁶⁵ are already considering copying parts of the DSA. In my view, there is a reason to be hesitant about whether this is a good idea. The DSA is an untested

⁵⁹ Marian Garcia Martinez, Paul Verbruggen, and Andrew Fearn, 'Risk-Based Approaches to Food Safety Regulation: What Role for Co-Regulation?' (2013) 16(9) *Journal of Risk Research* 1101; Griffin and Vander Maelen (n 18) 8ff.

⁶⁰ Ayres and Braithwaite (n 50) 54ff.

⁶¹ *ibid* 56.

⁶² David Vogel, *Trading Up: Consumer and Environmental Regulation in a Global Economy* (HUP 1997).

⁶³ Anu Bradford, 'The Brussels Effect' (2012) 107 *Northwestern University Law Review* 1.

⁶⁴ Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (OUP 2020) 25ff.

⁶⁵ Beatriz Kira, 'In Brazil, Platform Regulation Takes Center Stage' (*Tech Policy Press*, 24 April 2023) <<https://techpolicy.press/in-brazil-platform-regulation-takes-center-stage/>> accessed 18 September 2023.

regulatory approach, and some of its parts, such as the risk management under Article 34, might require high trust in the regulators. Having said that, it is understandable that other countries would start asking VLOPs why something is possible in Europe and not in their own jurisdiction.

The more compelling question, at this point, is Bradford's original question about whether the companies are likely to export the implementation of the DSA to other markets, most notably the US.

Arguably, such *spillover effects* depend on the type of DSA rules in question. As for content moderation rules that create due process rights (Chapters 10–12), they are the most obvious candidate to go global. Once a company builds one elaborate system for handling things in Europe, why would it design something else for the rest of the world? Thus, if the DSA can produce some Brussels Effect, it will likely occur for due process rights. However, I don't expect this to be the case for all the DSA content moderation features. Out-of-court dispute settlement requires local certification, and costs providers money. They can easily ignore it outside of the European markets. Thus, in the absence of push, there is no obvious answer to why they would voluntarily extend it to other countries.

The same is likely to be true for a risk management system that asks companies to submit to auditing and produce elaborate reports. The complicating aspect here, however, is that many other countries are developing similar schemes, and it might be hard to split consequences per jurisdiction. Australia is steadily adopting Codes of Conduct, such as for social media, app stores, and search engines, that are certified by its eSafety Commissioner,⁶⁶ and the UK's Ofcom is gearing up to preparing a number of Codes of Practice to implement its imminent Online Safety Bill.⁶⁷ Thus, while the US is a crucial holdout on any risk-based regulation for digital services, the spillover effects from the EU, Australia, and the UK might become inevitable at some point.

In addition to direct regulatory spillovers, the DSA is expected to have a standardising effect on the industry. It can do for content moderation on digital services what shipping containers have done for the transport of goods. By creating vocabulary and basic building blocks, one can expect the industry to start developing off-the-shelf tools that serve various content moderation needs by different providers. This *de facto* standardisation is caused by the pull of the EU as a major market deciding to unify its regulatory approach. Next to *de facto* standardisation, the DSA also tries to harness formal voluntary standardisation to support its goals in three areas: content moderation, fair design practices, risk management practices, and transparency rules (Article 44(1)).

Examples of how standardisation can facilitate the DSA's implementation are as follows. Technical standards concerning content moderation notifications facilitate the exchange of notices and thereby increase the speed and quality of

⁶⁶ eSafety Commissioner, 'Industry Codes and Standards' <<https://www.esafety.gov.au/industry/codes>> accessed 18 September 2023.

⁶⁷ Ofcom, 'Online Safety Bill: Ofcom's Roadmap to Regulation' (2022) <https://www.ofcom.org.uk/__data/assets/pdf_file/0016/240442/online-safety-roadmap.pdf> accessed 18 September 2023.

notifications.⁶⁸ The access to application programming interfaces for trusted flaggers can, along with priority assessment, be a true incentive for stakeholders to organise themselves as entities with a great track record of precise enforcement. The standardisation of templates around statements of reasons and other due process communications can improve the clarity and speed of the process across the platforms and the transmission to the database mandated under Article 24(5). The standardisation of advertising labels can improve the user experience and avoid consumer confusion in a fast, vast and rich information environment.

Another use case of standards is to facilitate trust in content. Professionals of various kinds have been joining forces to come up with standards that govern their activities to signal coherence and quality in order to gain external trust. For instance, the European Code of Standards for Independent Fact-Checking Organisations⁶⁹ has been developed by a community of fact-checkers, supported financially by the European Commission, to codify the best practices in the area. Similar standards or codes of conduct can be developed across the ecosystem. I have argued that they are the missing piece in the regulatory mosaic today, where we often lack signals for what constitutes trusted content. One of the ideas of how to bridge this gap is to incentivise self-organised communities to develop and monitor compliance with their practices and for the members of these communities, Trusted Content Creators, to benefit from better treatment from providers.⁷⁰

20.5 Conclusion

The Codes of Conduct will likely push the DSA into a co-regulation frenzy. This chapter has explained why the Member States, stakeholders, and the Commission have all the motivation to push for Codes of Conduct. For the Member States, the Codes of Conduct are a way how to formulate expectations without resorting to formal rule-making pre-empted by the DSA. For the Commission, Codes of Conduct can produce factual evidence of optimal enforcement that helps to fine companies when enforcing Articles 34–35. Together with prescriptive rules about design practices and content moderation, Codes of Conduct offer a simple way to practice tit-for-tat enforcement strategy to motivate companies to cooperate. And finally, for stakeholders, it is the only way their voices can be heard and accepted in the context of risk management due to the limits of private enforcement.

⁶⁸ Martin Husovec, ‘The Promises of Algorithmic Copyright Enforcement’ (2018) 42(1) *Columbia Journal of Law & the Arts* 53; Catalina Goanta, Thales Bertaglia, and Adriana Iamnitchi, ‘The Case for a Legal Compliance API for the Enforcement of the EU’s Digital Services Act on Social Media Platforms’ <<https://arxiv.org/abs/2205.06666>> accessed 18 September 2023.

⁶⁹ IJAS, ‘European Code of Standards for Independent Fact-Checking Organizations’ (*SafeJournalists*, 19 September 2022) <<https://safejournalists.net/european-code-of-standards-for-independent-fact-checking-organizations/>> accessed 18 September 2023.

⁷⁰ Martin Husovec, ‘Trusted Content Creators’ [2022] LSE Law School Policy Briefing Paper No 52 <<https://ssrn.com/abstract=4290917>> accessed 30 August 2023.

PART V
OUTLOOK

21

Principles

21.1 Introduction	465	21.3 Interpretative Principles	473
21.1.1 Promoting trustworthiness	466	21.3.1 Separation of powers	474
21.2 Statutory Design Principles	470	21.3.2 Shared responsibility	474
21.2.1 Accountable but not liable	471	21.3.3 Empowerment of individuals	475
21.2.2 Horizontality of regulation	472	21.3.4 Rewarding trustworthiness	476
21.2.3 Transparency	472	21.4 Conclusion	476
21.2.4 Public participation	473		

21.1 Introduction

In 1923, the Czechoslovak parliament adopted ‘the Act on Protection of the Republic’.¹ Only four years old, the new republic was looking for ways to defend itself against the rising tide of extremism undermining the liberal-democratic fundamentals of the newly created state. The Act was adopted weeks after the brutal assassination of the Czechoslovak Minister of Finance, Alois Rašín.² In many ways, it was similar to the German law of the same name adopted in 1922 following the assassination of Walter Rathenau, the Minister of Foreign Affairs of the Weimar Republic.³ Both these laws created new offences that targeted activities that subverted the state, prohibited certain types of disinformation⁴ and equipped the state with powers to seize and temporarily prohibit the distribution of newspapers or publications.⁵ Unfortunately, the liberal democracies of the Weimar and Czechoslovak republics were not saved by these legal instruments against extremism.

A hundred years later, the gradual erosion of democratic institutions in Europe is again apparent.⁶ The number of people questioning the key tenets of liberal democracy

¹ Law dated 19 March 1923 for the Protection of the Republic (Zákon na ochranu republiky) (Act no 50/1923 Collection of laws) <<https://www.aspi.sk/products/lawText/1/3259/1/2/zakon-c-50-1923-sb-na-ochranu-republiky/zakon-c-50-1923-sb-na-ochranu-republiky>> accessed 22 September 2023 (1923 Czechoslovak Act).

² Alois Rašín (Wikipedia, 9 September 2023) <https://en.wikipedia.org/w/index.php?title=Alois_Ra%C5%A1%C3%ADn&oldid=1174537664> accessed 22 September 2023.

³ Act to Protect the Republic (Gesetz zum Schutze der Republik) v 21 July 1922 <http://www.documentarchiv.de/wr/repchutz_ges01.html> accessed 22 September 2023 (1922 German Act). See Bundesarchiv, ‘Gesetz Zum Schutz der Republik’ (100 Jahre Weimarer Republik) <<https://weimar.bundesarchiv.de/WEIMAR/DE/Content/Dokumente-zur-Zeitgeschichte/1922-07-21-republikenschutzgesetz.html>> accessed 22 September 2023.

⁴ See § 18 of the 1923 Czechoslovak Act.

⁵ See §§ 20–22 of the 1922 German Act for the provisions regarding the press; and similar provisions in §§ 23–34 of the 1923 Czechoslovak Act.

⁶ ‘The Hard Right is Getting Closer to Power All over Europe’ *The Economist* <<https://www.economist.com/briefing/2023/09/14/the-hard-right-is-getting-closer-to-power-all-over-europe>> accessed 22 September 2023.

is growing. Attempts to establish ‘illiberal democracies’ that only pretend to practice the rule of law and respect civil liberties are increasing at an alarming rate.⁷ Disinformation, hate speech, extremism, and many other ills of society find their breeding ground in digital services. Again, we are trying to find ways to protect ‘the republic’ from both the inside and outside. This time, however, societies are much more globalised, and information travels faster. The state’s ability to suppress the distribution of information is heavily weakened by the emergence of the internet.

The Digital Services Act (DSA) is stylised as a law regulating digital services. But when we look at its ambitious goals, it is clearly a modern attempt to protect ‘the republic’—ie the system of liberal democracy. One of its core goals is to effectively suppress the distribution of illegal expressions, such as hate speech, terrorist content, or modern acts of subversion, such as election interference, computation propaganda, or attacks on democratic institutions. Thus, while the law is about digital services, its goals are also heavily positioned in the realm of public security.⁸

This is not immediately obvious because, unlike its 20th-century forerunners, the DSA is not only about suppression. The DSA is also trying to address the *erosion of social trust*, likely one of the root causes of many of society’s ills. The trust-enhancing tools of the DSA are more subtle, but nevertheless very important.

21.1.1 Promoting trustworthiness

Robert Post, a constitutional law scholar from Yale University, identifies six unique threats that the internet poses to democracy, two of which are key for my purposes: the loss of epistemological authority and the shift from a slow-thinking public to fast-thinking crowds.⁹

Post argues that technology and public opinion are inextricably linked. Technology enables the emergence of ‘public opinion’¹⁰ and thus of certain governance structures by improving the ability of strangers to exchange texts and discuss ideas without being simultaneously present in one space. Post demonstrates this by describing how the invention of the printing press democratised the reading and interpretation of the Bible and thus led to the loss of epistemological authority of the church. Before the printing press, the hand-copying of the Bible allowed the church to monopolise epistemological authority over salvation. But as people gained access to their copies of the holy text, they started questioning the official religious teaching, resulting in reformation and religious wars.

⁷ Fareed Zakaria, ‘The Rise of Illiberal Democracy’ (1997) 76(6) Foreign Affairs 22.

⁸ The word public security is mentioned in Recs 82, 91, 95, 34(1), 36(2), 42(5), and 48(1) DSA.

⁹ Robert Post, ‘The Internet, Democracy and Misinformation’ in Ronald Krotoszynski, Charlotte Garden, and András Koltay (eds), *Disinformation, Misinformation and Democracy* (forthcoming, CUP 2024); Yale Law School, Public Law Research Paper, <<https://ssrn.com/abstract=4545891>> accessed 19 December 2023.

¹⁰ *ibid* 1.

According to Post, the internet similarly weakened the epistemological authority of many actors, such as newspapers and experts, ‘by which modern society underwrites order and stability.’¹¹ He posits that ‘[a]s we lose the ability to identify figures of authority whom the public can trust to distinguish truth from fiction, we correspondingly lose the capacity to establish common facts.’¹² Invoking the work of Hannah Arendt, he argues that in the absence of consensus about facts, we cannot inhabit the common political world.¹³ The implication is that because democracy is a system of ‘government by public opinion,’¹⁴ we will struggle.

His second related argument is that because of the speed at which information travels online, its virality tends to ‘convert the demos of a democracy from a public into a crowd.’¹⁵ I already made this parallel in the introduction (Chapter 1) when I discussed the nature of the crowds and how they resemble many assemblies in the digital ecosystem. The implication is that crowds tend to engage less in slow-paced thinking but rather tend to be driven by emotions. Post draws a parallel to what Daniel Kahneman calls system 1 and system 2 thinking, the former being immediate and emotional, and the latter being slower and more reflective.¹⁶ According to Post, this weakens the ability of the public to think and rather invites instinctive reactions.

I find Post’s observations compelling. The corroding trust in authorities and the fast-paced mentality of crowds are arguably responsible for, or at least magnifying, many of the problems we observe today in the digital ecosystem. The comparison with the early post-printing age suggests that we might be living through an early disorienting period during which people gained new capabilities—cheap and seamless access to any information from around the world—without yet learning how to cope with its dangers. As Barber wrote in 1999, ‘[w]hilst for thousands of generations life for a cohort of grandchildren roughly resembled life for their grandparents, in our century there is enough change in a decade to confuse people in the fifteen years it takes to grow up.’¹⁷

Does the DSA respond to these challenges? I think it does.

Firstly, the DSA is trying to redistribute parts of the power technology companies gained over citizens by giving it to the state and, importantly, individuals. The former manifests in the public-enforcement regime of management of risks. The latter is visible from the set of privately enforceable procedural rights that individuals are owed when providers make decisions about their expressions online. These procedural rights might gain an important role in establishing trust in how providers govern their expressions and interactions.

In this book, I have sketched how the DSA’s procedural requirements, including the demand for greater explainability of decisions, might impact the formulation of rules

¹¹ *ibid* 6.

¹² *ibid* 6.

¹³ Hannah Arendt, *Between Past and Future* (Viking 1968) 238.

¹⁴ Carl Schmitt, *Constitutional Theory* (1928), edited and translated by Jeffrey Seitzer (Duke UP 2008) 275.

¹⁵ Post (n 9) 7.

¹⁶ Daniel Kahneman: *Thinking, Fast and Slow* (Farrar, Straus, and Giroux 2013).

¹⁷ Benjamin Barber, ‘Three Scenarios for the Future of Technology and Strong Democracy’ (2023) 113(4) *Political Science Quarterly* 573, 574.

and their subsequent enforcement (Chapters 11–12). I noted that achieving predictability of content moderation can come at the cost of its precision; however, it might still foster trust in the process. Arguably, every instance of unexplained interference with people's expressions or interactions only feeds conspiracy theories that eventually flow into a large current of anti-system sentiment. In such a situation, ensuring the explainability of content moderation might be an important achievement on its own because it enhances the individual's trust in the process, even if it reduces the precision of the decision-making.

Secondly, the DSA is carving out a serious role for European civil society, ie researchers, non-profit organisations, fact-checkers, trusted flaggers, content creators, out-of-court dispute settlement bodies, consumer groups, and many others. Civil society is poised to gain new tools to improve the trustworthiness of global communications through transparency, data access, and rewards. The position of content creators is given serious legal recognition with the hope that this will encourage the creation and, eventually, consumption of more trustworthy content.

This inclusion of civil society is not only performative. From the scholarship on post-transition societies, we learn that public (civic) participation is an important element of practising democracy¹⁸ and building trust.¹⁹ In totalitarian or authoritarian societies, autonomous social organisations need to be rebuilt brick-by-brick because the past regimes often replaced such organisations with state-administered apparatuses that coordinated the behaviour of social groups to preserve social control.²⁰ Often what citizens of post-transition countries must overcome is learned apathy or hostility toward participation in organisations and public life.²¹

The aftermath of self-regulation obviously cannot be analogised to an authoritarian society. The overall power that companies yield over individuals is simply incomparable with that of the state. Yet, some parallels can be made. Switching from self-regulation to rights-based regulation means giving some power to the formerly powerless. Thus, the law must help people to unlearn apathy. Moreover, already in the 19th century, John Stuart Mill cautioned that freedom of expression and thought was not only determined by formal state restrictions. He warned that there is 'an increasing inclination to stretch unduly the powers of society over the individual, both by the force of opinion and even by that of legislation.'²² Mill was as concerned by the 'the tyranny of the prevailing opinion and feeling' as he was by the 'tyranny of the magistrate.'²³ In our day, it is not the power of the church and its teachings, but contractual restrictions imposed by powerful commercial actors that would fit this description.

¹⁸ Michael Bernhard and Ekrem Karakoç, 'Civil Society and the Legacies of Dictatorship' (2007) 59(4) *World Politics* 539, 562.

¹⁹ Generally, Gabriel Badescu and Eric Uslaner (eds) *Social Capital and the Transition to Democracy* (Routledge 2003).

²⁰ Bernhard and Karakoç (n 18) 545.

²¹ Bernhard and Karakoç (n 18) 546.

²² John Stuart Mill, *On Liberty* (Penguin Books, 1998 (1859)) 23.

²³ Mill (n 22) 10.

To be clear, the DSA mostly leaves this power to formulate rules for others intact. However, it imposes procedural limits on decision-making and fairness rules on the overall design of services (Chapters 12 and 14). By doing this, the DSA imposes costs on the exercise of the platform power. This creates an opportunity. If providers recognise that too much rule-making power comes with costly responsibility, they might be more inclined to devolve that power to individuals or self-organised groups to lower the cost of their operations whenever possible. Thus, greater empowerment of individuals can emerge as a direct consequence of the DSA-imposed regulatory cost on central decision-making by platforms.

If the studies about trust and the empowerment of workers have any external validity for the digital environment,²⁴ again, there is a distinct possibility that more trust emerges from such devolution of decision-making. For this reason, I also argue that the empowerment of individuals must be at the heart of acceptable risk mitigation strategies (Chapter 15).

To formulate the above argument about the DSA's potential more explicitly, I argue the following:

1. If opacity and arbitrariness breed distrust of individuals, transparency and procedural fairness might foster trust.
2. If centralised content moderation by providers breeds distrust of individuals, empowerment and decentralisation might foster trust.

The trouble with the *trust-enhancing*, as opposed to information-suppressing, parts of the DSA is that they rely on social institutions, which require a degree of social trust to even emerge. As explained by Fukuyama, 'durable social institutions cannot be legislated into existence the way the government can create a central bank or an army'.²⁵ Thus, while information-suppressing tools can benefit from administrative enforcement as an arm of a strong state, the DSA can only foresee and incentivise trust-enhancing social institutions but cannot build them; only people can. There lies the key limit of the DSA's trust-enhancing attempt to repair 'the Republic(s)'.

Despite this limitation, the DSA rightly focuses on trust as one of the overarching goals of the law (Article 1(1)). Every 'trusted' environment is 'safe' and 'predictable', but not every 'safe' and 'predictable' environment is also 'trusted'. High-security prisons try to maximise safety and predictability precisely to compensate for lack of trust between individuals. The European dictatorships of the 20th century in Southern, Central, and Eastern Europe offered safe and predictable social environments to many, largely by shielding them from the real controversies of the day. However, such social environments were certainly not worthy of trust. This is evident from the fact that such regimes tend to leave behind decimated trust among people and in public institutions.²⁶

²⁴ Gretchen A Mosher, 'Trust, Safety, and Employee Decision-Making: A Review of Research and Discussion of Future Directions' (2013) 29(1) *Journal of Technology, Management, and Applied Engineering* 2.

²⁵ Francis Fukuyama, *Trust: The Social Virtues and the Creation of Prosperity* (The Free Press 1996) 5.

²⁶ Natalia Letki, 'Trust in Newly Democratic Regimes' in Eric M Uslaner (ed) *The Oxford Handbook of Social and Political Trust* (OUP 2017) 335, 336; Robert D Putnam, Robert Leonardi, and Raella Y Nanetti, 'Making

For these reasons, I think the focus on trust should guide the DSA's application as the norther star. It should keep the regulators on their toes whenever they try to go too far in their efforts to repair anything from the top-down. The goal of intervening is for people to regain confidence in the system of liberal democracy, to increase their resilience to risks, and to their autonomy. Excesses of state power will only engender disgust and mistrust in people and take us away from these goals. As I explained in Chapter 15, sometimes we need to balance trust and safety because too many top-down restrictions of freedom can corrupt trust.

Finally, the regulators should be reminded that trust emerges slowly and that being *worthy* of trust also means allowing for uncertainty. Allowing people to make their own mistakes is fundamental to learning and human life. The highest form of human knowledge, science, equally relies on 'its ability to self-correct as new evidence is established'.²⁷ It constantly 'operates on the "edge of error"'.²⁸ Some level of distrust is healthy for individuals, science, and ultimately society at large. As noted by Václav Havel, the first and last post-Communist Czechoslovak president, '[t]here can be no doubt that distrust of words is less harmful than unwarranted trust in them'.²⁹

This brings me to the key question: can this dual attempt to protect the liberal democracy work?

Only time will tell if the regulatory experiment works. However, to guide us to a brighter future, I propose several principles that should be observed when different actors decide to 'run with it'. The proposed principles constitute the connecting tissue for all the DSA's provisions. I offer the principles for two audiences. First, *statutory design principles* aim at those looking at the DSA from outside Europe as a potential solution to similar problems in their jurisdictions. Second, *interpretative principles* aim at those applying the DSA from inside the European Union (EU) (see Figure 21.1).

21.2 Statutory Design Principles

The DSA's provisions are built on four key principles: increasing accountability of providers and not their liability, horizontality of regulation, transparency, and public participation.³⁰

Democracy Work: Civic Traditions in Modern Italy' (Princeton UP, 1994); Martin Paldam and Gert T Svendsen, 'Missing Social Capital and the Transition in Eastern Europe' (2001) 5 *Journal for Institutional Innovation, Development and Transition* 21–34.

²⁷ The Royal Society, 'The Online Information Environment Understanding how the Internet Shapes People's Engagement with Scientific Information' (2022) 92 <<https://royalsociety.org/-/media/policy/projects/online-information-environment/the-online-information-environment.pdf?la=en-GB&hash=691F34A269075C0001A0E647C503DB8F>> accessed 19 December 2023.

²⁸ *ibid.*

²⁹ Václav Havel, 'Words on Words' (Acceptance speech upon receiving the Peace Prize of the German Booksellers Association at the Frankfurt Book Fair in Germany 1989) <<https://www.vhlf.org/havel-archives/words-on-words/>> accessed 22 September 2023.

³⁰ For a more extensive explanation, Martin Husovec, 'Rising Above Liability: The Digital Services Act as a Blueprint for the Second Generation of Global Internet Rules' [2023] *Berkeley Technology Law Journal* (forthcoming).

Statutory design principles	Interpretative principles
ACCOUNTABLE BUT NOT LIABLE The providers are asked to assist without becoming liable for others.	SEPARATION OF POWERS Content rules are dictated only by parliaments. Risks are supervised by authorities.
HORIZONTALITY OF REGULATION Uniform legal rules should apply across the entire legal system.	SHARED RESPONSIBILITY Everyone is expected to reasonably protect themselves/others from risks.
TRANSPARENCY Improving explainability of the digital ecosystem and individual decisions made.	EMPOWERMENT OF INDIVIDUALS Devolution of responsibility to individuals whenever it is meaningful and reasonable.
PUBLIC PARTICIPATION Solving problems by giving tools and involving civil society, researchers, and the public.	REWARDING TRUSTWORTHINESS Incentivising all actors to improve safety from illegal content and to facilitate trust building.

Figure 21.1 DSA Principles

21.2.1 Accountable but not liable

Providers of digital communication tools cannot be expected to bear the burden of liability borne by ordinary publishers, such as newspapers. The existence of some sensible legal immunities for the actions of others is the basic precondition of the viability of services fuelled by user-generated content (Chapters 3–4).

The ultimate value that liability exemptions protect is decentralised speech. The internet’s genius is in allowing anyone to speak their minds without seeking approval. Obviously, this creates challenges because editors were previously deputised to act as filters for the lawfulness, trustworthiness, and quality of information. Without editors, the ecosystem shifts from filtering the content’s quality upfront to managing its distribution. Imposing incentives that reinstate upfront editorial control automatically takes away the newly gained ability of individuals to speak and read what is not edited. The focus on addressing the digital risks should be on how to align providers’ business operations more with individual freedoms—ie how to make providers more accountable to society.

Unlike in the liability system, where the lack of diligence makes providers an accessory to the entire wrongs of others, the accountability system only blames them for not giving some specific assistance. The legal culpability implied in the two frameworks is very different and corresponds directly with the seriousness of the consequences for the platforms (Chapter 9). It is a qualitative difference between being regulated as a criminal or a sloppy business owner (eg a bank co-conspiring to evade sanction or a bank having a weak anti-money laundering system).

The distinction is key because such blameworthiness and the gravity of legal consequences directly affect the types of freedoms enjoyed by individuals using the services. If the liability for failing to assist is adequate, the health of the decentralised ecosystem is not put at risk; otherwise, the decentralised ecosystem is forced to inch closer to an editorial system of digital services with strong prior approvals.

21.2.2 Horizontality of regulation

The horizontality of regulation means that the same digital rules apply universally in all areas. Avoiding special regimes has many positive effects. The horizontality is useful for companies and individuals because it makes compliance cheaper and easier to implement (Chapters 11 and 15). It also prevents the gaming of the system because it reduces regulatory arbitrage.³¹

Given the never-ending cycle of balancing competing interests, a holistic policy allows regulators to better balance one interest against a number of others at the outset. Thus, for instance, the European Commission looking at risk mitigation by technological solutions must equally consider the under-detection of hate speech and overblocking of legitimate speech. Given that content moderation and risk mitigation really stretch to all areas of human interactions, having the broadest possible focus is key to any balanced policy.

Politically, the horizontal approach also moderates the excessive strength of some interest groups because it broadens the conversation and addresses the imbalance of voices by ensuring that the equally valid concerns of others are heard. If interrelated conversations are scattered into separate legislative debates, there is a risk that important voices can be strategically split into different legislative files. Horizontal rules do not have the same problem because they ensure everyone discusses the same instrument.

Moreover, if the argument for regulation is a general reshuffle of power from technology companies to individuals and the state, doing it only for some areas of our lives but not for others makes little sense. Sectorial rules can still play a role in addition to this general reshuffle.

21.2.3 Transparency

The DSA has a number of provisions that try to shine a light on decision-making by technology companies. This includes content moderation reports, individual explanations, access to data, audit reports, and publicly available databases (Chapters 11,

³¹ *ibid.*

15–16). These elements aim to enhance oversight but also the trust of individuals in what is going on behind the scenes in digital services.

The explainability of processes is thus one of the key ingredients that can foster a predictable and trustworthy online environment. In combination with other regulatory interventions, transparency can help us uncover practices that would otherwise lie hidden from the public debate. In the long run, it can force companies to better align their internal thinking with what they present to the public.

Access to data can help civil society and academia to better understand the interactions that people have online and how to address social phenomena, such as distrust, racism, and hate, that pervade our societies. Only such insights and knowledge can bridge our current situation to one with more targeted and sophisticated policies based on greater understanding.

21.2.4 Public participation

The DSA gives individuals and groups tools to rely on when protecting private or public interests. By doing this, it tries to equip societal structures, such as local organisations analysing threats, consumer groups helping content creators, and communities of researchers.

The alternative to public participation is to create a gigantic administrative machinery whose sole legitimacy rests on the legitimacy of state power. Such machinery can always be manipulated to maximise the wrong goals, as we have seen in the past. This, in turn, could paradoxically undermine the long-term legitimacy of the system because individuals and civil society would remain entirely excluded from supervising the system and correcting the wrongs.

The emphasis on ecosystem solutions, in contrast, assures public participation by other means and thus also decentralises how the information is acquired, processed, and eventually evaluated by the regulators (Chapters 13 and 20).

Even the DSA's allowance for private enforcement can be construed as a form of public participation (Chapters 19–20). Because individuals do not have to wait for authorities to intervene, they can act and potentially collectively organise around various causes they present to the courts. This, in turn, increases the legitimacy of the overall system, which is not dictated solely by regulators.

21.3 Interpretative Principles

The DSA's interpretation of provisions by courts and regulators should be guided by the following four key principles: separation of powers, shared responsibility, empowerment of individuals, and rewarding trustworthiness.

21.3.1 Separation of powers

The regulation of content moderation processes and risk management are perfectly legitimate tools of liberal democracies. However, they must respect the specifics of the medium that they regulate. Content moderation should always afford some leeway to companies to decide on their own content rules. The risk-based approach and its oversight cannot be allowed to be used as a convenient guise for the substantive regulation of content by the executive. And finally, access to data by civil society should not become a tool of surveillance by the state. The reason why the DSA allocates many functions to non-state actors reflects its commitment to the principle of the separation of powers.

The DSA distributes powers between legislatures, companies, the authorities, and civil society. Each of these actors keeps the other power in check. That balance is desirable, even though it might slow down the speed of response.

The interpretation of the DSA should not change the basic separation of powers in liberal democracies: legislatures decide what is illegal to say, and authorities only enforce these norms. That is the principle of legality (Chapters 13 and 15). If the interpretation of the DSA respects the division of powers between legislature and executive, it is less likely to be embroiled in partisan politics and constitutional challenges. If, on the contrary, the European Commission starts assuming the role of a surrogate legislature by imposing content-specific measures concerning lawful content, it is likely to undermine the legitimacy of the entire project.

Courts and regulators should be reminded that public discourse does not stop where the DSA's powers stop. Sometimes, the information that is amassed thanks to the DSA is only the start of the conversation that should take place before the legislatures—one that is reliably informed.

21.3.2 Shared responsibility

The DSA renews democratic support for the model of sharing the burden for societal risks on digital services. Under the principle of shared burden, everyone is expected to play their part—to do what is reasonable to protect oneself and others from risks that result in social costs. Shared responsibility means resisting the temptation to blame one actor for all ills. The DSA makes providers accountable for doing their best to ensure safety from the illegal content and activities of others. But it does not make them solely accountable. Along with providers, the public and state are also asked to play their part.

Shared responsibility can guide the interpretation of the DSA in many parts (Chapters 4 and 15). Content moderation, for instance, is a shared responsibility between individuals, civil society and the authorities on the one hand and technology companies on the other. Together, they have more information on how to act against

illegal content and activities. The NGOs and charities are closer to victims and know their stories and pains. Specialised authorities have an aggregate picture of what happens in our societies. Finally, providers have superior technical capabilities and can think of novel solutions to address the problems. By sharing the burden, each actor contributes their unique knowledge and skills.

The opposite of sharing is the concentration of all responsibility with providers. Such concentration creates a single point of failure, which is rarely the best strategy to protect the safety of the affected individuals. The regulators must be aware of the dangers of such concentration when they formulate their demands for risk mitigation under the risk management tools (Chapters 11 and 15). By deciding which actors they certify as trusted, they help manage the risks; by compiling useful information or periodical monitoring, they take part in the responsibility.

21.3.3 Empowerment of individuals

Individuals can only share as much risk as they are given a chance to counter. The principle of user empowerment speaks in favour of devolution of responsibility to individuals whenever it is meaningful and reasonable. Typically, this means that platforms provide individuals with tools that grant them agency in deciding about their digital experience, such as what they wish to see and from whom. Naturally, the key role for such empowerment lies in situations involving expressions that society had not previously proclaimed as illegal.

Empowerment benefits individuals and the public by recognising individuals' voices as participants in the environment (Chapters 10–11, 13, and 15). It is analogous to giving a larger responsibility to workers to win their trust—a move that ultimately leads to efficiency gains for the companies.³² Meaningful and reasonable empowerment can be a source of learning for individuals (eg children) and lead to new ways of achieving the goals of a trustworthy online environment.

The regulators should not frown upon providers delegating powers to individuals. On the contrary, they should encourage meaningful and reasonable empowerment. Empowerment should be considered a risk mitigation strategy on its own. The more agency platforms give individuals when using their products, the less responsibility they should bear (Chapter 15). If platforms leave little agency to users, they should insist that providers also assume more risks. This does not mean that the regulators should allow providers to completely shrug off any accountability for risks. Rather, it is simply that with reasonable and meaningful expectations on the side of individuals, such empowerment should reduce providers' compliance risks and thus be encouraged.

³² Allan Lee, Sara Willis, and Amy Wei Tian, 'When Empowering Employees Works, and When It Doesn't' [2018] *Harvard Business Review* <<https://hbr.org/2018/03/when-empowering-employees-works-and-when-it-doesnt>> accessed 22 September 2023.

21.3.4 Rewarding trustworthiness

The DSA rewards betterment and punishes efforts of subpar quality. The idea that trustworthiness should be incentivised runs in the veins of many of its provisions.

Consider the content moderation provisions (Chapters 10–12). Trusted flaggers are prioritised if they make a few mistakes when notifying illegal content. If the quality of their work deteriorates, they lose certification. Those who repeatedly violate trust by sending incorrect notifications or submitting illegal content must be excluded from services. Individuals who appeal content moderation decisions and win on merits are compensated by platforms. Such costs inflicted on platforms, in turn, incentivise them to improve their internal appeals processes so they can be better trusted. Out-of-court dispute settlement bodies are certified by regulators and are expected to be followed by platforms, but will lose their certification if they fall short of expected standards of fairness and diligence. The incentives are aligned with prosocial enforcement.

Even under risk management, rewards are present (Chapters 13–16). Platforms are primarily responsible for finding solutions to the problems they encounter. They formulate their house rules and develop the design of the services and strategies for overcoming challenges. Their thinking is documented through self-assessments, which are reviewed by auditors, regulators, researchers, and the public. If they fail to engage in good faith, they will be fined because their actions do not inspire public confidence. Auditors, again, are rewarded for doing their job properly because they can save their clients from embarrassment. Finally, researchers are given special access to data to uncover risks and test solutions; however, this is only if they can agree to conduct themselves in a certain way.

The regulators, consumer groups, and other private actors who enforce rights should be reminded that if incentives envisaged by the DSA are credible, they alone can do a lot of the heavy work to regulate the behaviour of providers in the direction of trustworthiness.

21.4 Conclusion

The internet revolutionised the distribution of information. Such decentralised content production brought many undisputed benefits. It democratised production of information and its distribution, allowing anyone to speak to large audiences and share their expertise or views. It weakened the role of traditional information gatekeepers, such as newspapers or broadcasters.

However, it also brought new challenges. With such abundant information, it is now more important than ever to find a way to navigate them meaningfully. Surveys of

internet users show that they struggle to distinguish facts from fabrication.³³ To make things worse, editorial content and the old institutions that supplied it are also simultaneously losing trust and, in some markets, also ground to content of lesser quality.³⁴ Thus, the mistrust is being fuelled from different sides.

The difficulty of regulating non-editorial content is that it requires different approaches compared to editorial content. Content creators are not confined to traditional professions, institutions, or geographies. Digital services that publish their content are not just some new-era publishers but genuinely new types of communication networks.

The experience of the last two decades has shown again and again that individuals from all walks of life can challenge and supplement formal institutions, such as academia, state authorities, broadcasters, or newspapers, in the search for truth. Therefore, the goal should not be to return to relying only on the old institutions that dominated editorial content to lend 'trust' to information flows. The superior policy goal should be to extract the best of both the old and new institutions: editorial and non-editorial content. The key component that should bridge their differences is the notion of *trust*.

The DSA and similar regulations should harness the power of non-editorial content to promote trustworthy content at the expense of an untrustworthy one. The obvious untrustworthy content is unsafe, illegal content, including age-inappropriate content for children, that has been outlawed by parliaments. Beyond such unsafe illegal content, regulators must avoid imposing the substantive notion of what should be trusted and leave the indicators of trust to society at large.

In short, the DSA's most ambitious goal is to prove that while non-editorial content lacks editors, it does not have to lack trust. If popularity and trust in existing older institutions are declining, one way to approach the situation is to give space to new organisational structures that complement existing institutions. If new trust structures can reduce the level of distrust among the public and serve as a remedy to one of the root causes of society's ills, then perhaps our liberal democracies, our *republics*, might be repaired at last. To paraphrase a popular adage, we ought to keep the company of those regulators who want to help people seek the truth and run from those who have found it.³⁵

³³ Nic Newman, Richard Fletcher, Kiersten Eddy, Craig T Robertson, and Rasmus Klein Nielsen, 'Digital News Report' (2023) Oxford: Reuters Institute for the Study of Journalism, p 17, available at <https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2023-06/Digital_News_Report_2023.pdf> accessed 22 September 2023 ('Across markets, well over half (56%) say they worry about identifying the difference between what is real and fake on the internet when it comes to news').

³⁴ *ibid* 24; for the discussion of the relationship between news publishers and platforms, Rasmus Kleis Nielsen and Sarah Anne Ganter, *The Power of Platforms Shaping Media and Society* (OUP, 2022).

³⁵ Quotersearch, 'Believe Those Who are Seeking the Truth; Doubt Those Who Find It' (*Quote Investigator*, 14 November 2013) <<https://quoteinvestigator.com/2013/11/14/seekers/>> accessed 22 September 2023.

Index

For the benefit of digital users, indexed terms that span two pages (e.g., 52–53) may, on occasion, appear on only one of those pages.

Tables, figures, and boxes are indicated by an italic *t*, *f*, and *b* following the page number.

- access to data, *see* data access
- accountability 66, 181–84, 346, 352, 373, 385–86, 470–72
- active recipient of the service 169, 174
- counting users 168–77
- actors
 - ODS bodies, *see* out-of-court dispute settlement bodies
 - trusted content creators, *see* trusted content creators
 - trusted flaggers, *see* trusted flaggers
 - user organisations 400–1; *see also* civil society
- advertisement
 - code of conduct 451
 - content creator advertisement 27, 297–99
 - design requirements 296–305
 - platform advertisement 297–99
 - prohibitions 303–5
- agency 11, 193, 230, 312, 343–45, 475
- Airbnb Ireland Case C-390/18* 136, 151–52, 372n.8, 379, 379n.39, 387, 411
- alternative dispute resolution 235, 241
- anti-abuse 265–68
 - prior warnings 265–67
 - scope and conditions 267–68
 - suspension 266, 267
- Anti-Trafficking Directive 2011/36/EU 228
- Audiovisual Media Services Directive 2018/1808/
EU 282–83, 311–12, 385–86, 394–95, 407–10
- Audit Regulation 537/2014/EU 329
- audits 323, 328–30, 331, 366
- CDSM Directive 2019/790/EU 78, 89, 118, 149, 356–57, 396–401
- child safety 340–46
 - ban on ads using profiling of children 304–5
 - protection by design 311–13
- Child Sexual Abuse Regulation 2021/1232/EU 348
- civil society 180–81, 197, 450–53, 459, 468, 473, 474
- codes of conduct
 - accessibility 451–52
 - advertising 451
 - crisis protocols, *see* crisis protocols
 - generally 274, 445–56
- Communications Decency Act 5–6, 60, 63, 112
- complaints to out-of-court dispute settlement bodies, *see* external appeals
- compliance by design 171, 314
- compliance function of VLOPs and VLOSEs 331–32
- CompuServe* 57–60, 185n.1, 374
- consumer
 - consumer protection 133–36, 259–60, 307–11, 436–37, 440–41
 - users as consumers 26–27, 168, 252, 313–14
- Consumer Rights Directive 2011/83/EU 313n.89
- content moderation
 - general explainability of rules 249–53, 260, 467–68
 - quality of automated tools 85–86, 365–66
 - scope 203–5
 - statement of reasons, *see* statement of reasons
- contract, interaction with 259–60
- control of meaning 101–11
- Counter-Terrorism Directive 2017/541/EU 228n.80
- country-of-origin principle 372–73, 379–80, 387, 419, 420–21
- crisis protocols 452–53
- crisis response mechanism 29, 282, 322–23
- dark patterns 305–11; *see also* fair design practices
- data access 349–59, 473
 - APIs 357
 - publicly available 351, 355–60
 - regulator’s access 331, 351*f*
 - researchers, generally 29, 300, 301, 321, 329–30, 350–55, 440
 - scraping 347–48, 356, 357–58
 - vetted researchers 29, 301, 350–55
- Data Governance Act 2022/868/EU 373n.10, 394n.7
- Data Protection Directive 95/46/EC 86n.76, 373
- Delfi v Estonia* 42–47
- Digital Markets Act Regulation 2022/1925/EU 7–10, 192, 410–11
- Digital Millennium Copyright Act 5–6, 60, 67n.2, 99n.18, 104n.44, 137, 182–83, 214, 221–22
- digital rights 391
- Digital Services Coordinator 20, 53, 154, 262, 294, 350, 426–27
- Digital Single Market 87, 95, 371–73, 377
- Directive 2011/93/EU on combating child sexual abuse 214n.41, 228n.79
- dissemination to the public 164–66, 204
- domain names 116, 166*t*, 235
- due diligence 22–30, 181–84
 - content moderation 26, 167–68, 202–9
 - fair design 285–87
 - risk management 26–27, 316–18
 - transparency 27–28, 347–49

- due process 7, 53, 187, 189, 193–201, 221–22, 253, 314, 373, 376, 429
- E-Commerce Directive 2000/31/EC 4, 42, 61–66, 68–72, 81–83, 93–95, 99, 113–15, 146, 181–82, 200, 295, 373–75, 379–80, 384–85, 394–95, 401–4
- eDate* 379, 381*t*, 438*n*.94
- empowerment
- individual empowerment 192–93, 475
 - public participation as principle 473
- ePrivacy Directive 2002/58/EC 373*n*.9
- establishment, *see* place of establishment
- European Media Freedom Act 2024/1083/EU 415
- external appeals 234–48
- complainant 236
 - philosophy 235–36
 - scope 237–38
- fair design practices
- advertising 27, 296–305
 - recommender systems, *see* recommender systems
 - user experience 305–13
- fundamental rights, *see* human rights
- General Data Protection Regulation 2016/679/
EU 86*n*.76, 225–27, 293–94, 303–4, 307–11, 358–59, 373, 393–94, 401–7, 420–21, 426–27, 444–45
- general monitoring obligation, prohibition of 67–69
- specific monitoring 72, 74, 75, 80, 83, 87, 90, 91
- Glawischnig-Piesczek* 54, 75–79, 90, 146, 147–48, 155
- goals
- predictability 235, 445
 - safety 474, 475
 - trustworthiness 466–70, 476
- Good Samaritans 112
- Google France* 63, 101–2, 138, 139–40, 143*n*.75, 302*n*.49
- Google Spain* 50, 54, 283*n*.68, 404*n*.44, 405*n*.55
- harmonisation (EU), 7, 20, 82, 87–90, 380–89, 443
- hosting 128–36
- content management systems 165
 - marketplaces 133–36
 - messaging services 125–26, 143, 165–66, 170, 173, 174–75, 203–4, 264–65
 - social media 97, 129, 402–3
 - web hosting 129, 133, 164–65, 210, 217–18
- human rights
- freedom of expression 36–38, 39–47, 48–49, 52–53, 83–87, 112, 139, 210, 217, 220, 281, 283–84, 327–28, 333, 337, 386, 453, 468
 - privacy and data protection 50, 83–87, 118, 131, 307–10, 358–59, 401–7, 450–51
 - right to conduct business 48–49, 50–52, 79, 83–87, 256
- illegal content
- cross-border implications 418–19
 - definition 31
 - manifestly illegal 219–21, 267–68
- information society services
- economic character 97, 113–16, 310
 - exclusions 114–16
- InfoSoc Directive 2001/29/EC 142*n*.69, 396–401, 437
- intellectual control, *see* control of meaning
- intermediary services 21–22, 24, 96–97, 113–16
- caching 21, 126–28
 - hosting 21, 128–36
 - mere conduit 21, 123–26
 - other 143–44
 - search 136–43
- internal appeals 229–34
- cost 233
 - human oversight 234
 - reasoned decision 234
 - reversibility of decision 233–34
- internal market, *see* Digital Single Market
- luKDG (German Federal Act Establishing the General Conditions for Information and Communication Services), 59, 63
- knowledge
- constructive knowledge 130–33
 - knowledge of illegality 107–8, 127–28, 129–33, 213–14
 - manifest illegality 25, 71–72, 131, 219–21, 265, 267–68, 412
 - neutrality, *see* neutrality requirement
- Law Enforcement Directive 2016/680/EU 86*n*.76, 373*n*.9
- legal representatives 20, 24, 30, 166, 200, 227, 422–23, 424, 439
- lex generalis* 309–10, 393, 394–96
- lex specialis* 169–70, 308–10, 356, 393–95, 398–401, 412, 414, 415
- liability exemptions
- caching 21, 126–28
 - hosting 21, 128–36
 - mere conduit 21, 123–26
- L'Oreal v eBay* 63, 69*n*.7, 72–76, 102–3, 104, 130–31, 211*n*.35
- mere conduit
- browsers 124–25, 166*t*, 209–10, 360*n*.36
 - domain name authorities 116, 124–25
 - live streaming 128
 - messaging apps 125–26, 143, 165–66, 170, 173, 174–75, 203–4, 264–65
 - TOR nodes 166*t*
 - VPNs 24, 166, 166*t*, 209–10
- mid-sized companies 167–68, 176, 234, 237, 272*t*, 417
- Misleading and Comparative Advertising Directive 2006/114/EC 308
- MTE v Hungary* 42–44
- must carry claims 386–87
- NetzDG (German Network Enforcement Law, *Netzwerkdurchsetzungsgesetz*), 211*n*.37, 216*n*.49, 221*n*.60, 311*n*.82, 324–25, 383*n*.54, 383*nn*.55–56, 386*n*.68

- neutrality requirement 101–11
 - appropriated/adopted content 109–10
 - deliberate collaboration 108, 126, 132–33
 - co-determining content 111*t*
- NIS2 Directive 2022/2555/EU 393–94
- non-platform activities 165, 170, 172–73, 174–77, 263–65, 361
- notice 212–14
 - adequately substantiated 130–31, 211–12, 213–14, 398–99
 - electronic 206, 211, 212–13
 - notifier 214
 - sufficiently precise 130–31, 211–12, 398–99
- notification of crimes 227–29
- notification of illegal product or service 225, 314
- online platform
 - marketplaces 73, 109, 130–31, 133–36, 162*t*, 163*t*, 169, 170, 172, 172*f*, 174, 178–79, 225, 237*t*, 238, 313–14, 321–22, 357, 423
 - medium to larger platforms 230, 232, 291, 292–93
 - mere hosting 129, 164–66, 167–68
 - messaging apps 125–26, 143, 165–66, 170, 173, 174–75, 203–4, 264–65
 - mini platforms 177–78
 - newspapers 97–98
 - online interface 169, 292–93, 296, 306, 363
 - online maps 162*t*, 163*t*, 170, 172, 237*t*, 446–47
 - VLOPs, *see* VLOP
- online search engine 136–43, 169–70, 289, 295–96, 302, 363–64, 384–85
- Open Internet Regulation 2015/2120/EU 52–53, 204*n*.6, 264*n*.55
- orders
 - content orders 153–55
 - independent oversight 149–50
 - information orders 156–57
 - injunction clauses 80, 83, 100, 145–58, 397
- out-of-court dispute settlement bodies
 - body 235, 242–43
 - content rules 239–40
 - expertise 238–39
 - fees and financing 243–46
 - impartiality 246–47
 - independence 247–48
 - procedure 236
 - review of decision 240–41
- Pihl v Sweden* 36*n*.11, 37*n*.25, 39*n*.36, 43
- place of establishment 20, 26, 30, 113, 175–76, 424, 438
- Platform to Business Regulation 2019/1150/EU 139, 225, 251, 402, 410–13
- point of contact 24, 154, 157
- Poland v EC* 49, 50, 76–77, 90, 132–33, 220
- power
 - legitimacy 189–92
 - private vs state power 9–12, 188–89
 - user empowerment 192–93, 196–97, 279, 312, 340*t*, 344, 346, 473, 475
- pre-emption 380–89
- private enforcement
 - collective redress 20–21, 53, 428, 436–37
 - cross-border jurisdiction 438–39
 - damages 434–35
 - delegated enforcement 12–14, 34–35
 - injunctions 436–37
- procedure, *see* due process
- Prodigy* 57–60, 112, 185*n*.1
- Product Safety Regulation 2023/988/EU 357
- Promusicae* 63, 146*n*.9
- protection of minors, *see* child safety
- public enforcement 420–28
 - competences 422–27
- recommender systems 27, 288–96
 - design explainability 291–93
 - opt-out 293–94
- redress, *see* external appeals;
 - internal appeals
- regulation, modes of
 - codes of conduct 445–56
 - command-and-control regulation 271–72, 286
 - co-regulation 30–31, 444–45
 - risk-based regulation 274–76
- risk assessment 322–32
 - audits 328–30, 476
 - scope 318–22
- risk management
 - allocation of risk 344
 - risk mitigation cycle 322–32
 - systemic risk 319–21
 - theory 333–46
- risks, categories of 318–22, 319*t*
- RTC v Netcom* 57–58, 60
- SABAM* 51*n*.108, 69*n*.7, 72, 75, 129*n*.16, 146*n*.8
- safeguards against abuse by users and notifiers, *see* anti-abuse
- Sanchez v France* 36*n*.14, 37*n*.26, 39*n*.35, 42*n*.61, 44–46, 102
- Scarlet Extended* 51*n*.108, 69*n*.7, 72, 75, 129*n*.16, 146*n*.8
- small and micro companies 25, 164, 176, 177–78
- Star Taxi* 379*n*.39, 411*n*.77
- statement of reasons 221–29
 - exceptions 224–25
 - scope 222–24
- supervisory fee 176, 425
- Tamiz v United Kingdom* 36*n*.11, 43, 129*n*.21
- terms and conditions
 - fairness of rules 253–65
 - validity 259–60
- Terrorist Content Regulation 2021/784/EU
- traceability of traders 27
- Trade Secrets Directive 2016/943/EU 348, 391, 413–15

- trader 27, 134, 135–36, 169, 238, 313–14
- transparency 27–28, 347–49
 - access to data, *see* access to data
 - advertising archives 179, 299–301, 302
 - automated tools 362, 401
 - content moderation reports 359–62, 365–66
 - recommender systems, *see* recommender systems
 - user numbers reporting 168–71
- treaty on the Functioning of the European Union 54, 113, 114, 179, 180, 181, 377, 380, 387, 432, 453–54, 456
- trusted content creators 388, 461
- trusted flaggers 26, 206–9
 - expertise 208
 - incentives 207
 - independence 207, 208
- Uber France* 167n.8, 379n.39
- Unfair Commercial Practices Directive 2005/29/EC 26–27, 258, 307, 436
- Unfair Contract Terms Directive 93/13/EEC 258, 259
- UPC Telekabel* 54, 73, 90–91, 157–58
- user-generated content 98, 317–18, 321–22, 334, 471
- VLOP 28–29
- VLOSE 30
- YouTube and Cyando* 102–5, 111–12, 130–33, 220, 396–97

