EUROPEAN INFORMATION SOCIETY INSTITUTE, O. Z.
IČO: 42 227 950, www.eisionline.org, eisi@eisionline.org

5th of November 2024

The Registrar
European Court of Human Rights
Council of Europe
F-67075 Strasbourg Cedex
France

Third-Party Intervention by

European Information Society Institute (EISi)

In re *Artur Volodymyrovych BOYAROV against Ukraine*
Application no. 79083/17

Introduction

(1) The internet has emerged as a crucial technology for human communication, facilitating access to information, community building, public discourse, and global business. It is a powerful tool that governments naturally seek to regulate. One of the legitimate reasons for such regulation is national security, including the maintenance of public order. Website blocking is, according to the Court, an 'extreme measure'[1] that manifests coercive power of the state by making an entire website inaccessible to everyone in the country. The state sometimes go even further. In contrast to website blocking, an internet shutdown aims at the total interruption of all or many digital services, effectively disconnecting individuals from the global network and stifling any human communication.[2] *Boyarov v Ukraine* concerns a generic ban of a group of websites, which sits somewhere between website blocking and all-out internet shutdowns. Such **generic website blocking** is almost indistinguishable from a partial internet shutdown. Its key characteristic is that the ban covers a group of digital services that ought to be blocked due to a shared characteristic (e.g., time, geography, ownership, category of services, etc.). The Court is asked to set the human rights limits on this kind of extreme measures that suppress freedom to receive and impart information by individuals.

(2) **It is important that the Court distinguishes such generic bans from regular website blocking**, or typical regulation of the internet that demands providers to take down specified content, accounts, or sub-pages of websites. Whereas any targeted measures are justified by illegality of individual items of content, accounts, or websites, internet shutdowns and generic bans rely on an abstract justification that allegedly connects all the websites in the group (e.g., communicating tools during terrorist attacks,

[1] *Vladimir Kharitonov v Russia* (App no 10795/14) 23 June 2020 [38].
[2] E Zuckerman, 'The Internet Shutdown: How Governments are Restricting Freedom Online' in T Gillespie and C Lobato (eds), *The Cambridge Handbook of Technology and Communication* (Cambridge University Press 2019) 145–162.

or in a geographical area, or of containing specific features). In this case, the common denominator seems to be the country of origin of the service provider, i.e. Russia.

(3) Generic and specific restrictions on digital services in the name of national security are increasingly implemented around the world. India leads the world in internet shutdowns. Indians witnessed at least 116 disruptions in 2023 alone, affecting over 120 million people, particularly in regions like Manipur, Punjab, and Jammu and Kashmir. Initially justified as temporary measures for maintaining law and order, these shutdowns often extend for months.[3] Despite the Indian Supreme Court's ruling in *Anuradha Bhasin v Union of India*,[4] which mandates that internet restrictions be temporary, lawful, necessary, and proportionate, officials frequently fail to publish shutdown orders and face repeated court corrections for non-compliance. In Pakistan, millions of individuals experience problems with communications over the messaging apps like WhatsApp and social media (e.g., X formerly Twitter) due to the restrictions placed on them on the national security grounds.[5]

(4) In Europe, the 2024 Turkish law allows authorities to arbitrarily block and remove online content widely.[6] French government temporarily blocked access to TikTok in the territory of New Caledonia justified by the goal to quell protests alongside a state-of-emergency order and curfew.[7] In all these instances, website bans or throttling of communication of a group of services typically begins as a temporary measures based on national security grounds but frequently evolve into permanent restrictions.[8] According to a study by Access Now, in 2023, only liberal democracies so far use the internet shutdowns sparingly or not at all:[9]

Liberal Democracy	2.6%	1 out of 39 [Suriname]
Electoral Democracy	15.4%	6 out of 39 [e.g., Brazil, Indonesia, Israel, Kenya]
Electoral Autocracy	46.1%	18 out of 39
Closed Autocracy	35.9%	14 out of 39

(5) The international practice of internet restrictions must serve as a backdrop for the Court's considerations. The exercise of the executive power in the name of national security to curtail access to internet as a technology of communication is becoming all to frequent around the world. *Boyarov v Ukraine* gives the opportunity to the Court to set an important precedent for how the Council of

---

[3] Access Now Report, 'Shrinking Democracy, Growing Violence: Internet Shutdowns in 2023' (Access Now, May 2024) https://www.accessnow.org/wp-content/uploads/2024/05/2023-KIO-Report.pdf accessed 4 November 2024.

[4] *Anuradha Bhasin v Union of India* AIR 2020 SC 1308 19 January 2020.

[5] 'Social Media Platform X Blocked in Pakistan over National Security, Ministry Says' *Reuters* https://www.reuters.com/world/asia-pacific/pakistan-blocked-social-media-platform-x-over-national-security-ministry-says-2024-04-17/ accessed 4 November 2024. 'Pakistan's attempt to tamper with the Internet is leading to economic turmoil' (August 2024) https://thediplomat.com/2024/08/pakistans-attempt-to-tamper-with-the-internet-is-leading-to-economic-turmoil access 4 November 2024.

[6] Human Rights Watch, 'Turkey: Dangerous, Dystopian New Legal Amendments' (2024) https://www.hrw.org/news/2022/10/14/turkey-dangerous-dystopian-new-legal-amendments accessed 4 November 2024.

[7] 'France blocks TikTok in New Caledonia' (June 2024) https://www.accessnow.org/france-blocks-tiktok-new-caledonia/

[8] Another example is the U.S. law that would ban the video app TikTok unless it is sold by its Chinese parent company. See *TikTok Inc v Merrick Garland* (App no 24-1113) (D.C. Cir 16 October 2024.

[9] 'France blocks TikTok in New Caledonia' (June 2024) https://www.accessnow.org/france-blocks-tiktok-new-caledonia/

Europe countries are allowed to exercise such authority. The Court's holding will influence practices ranging from generic blocking of websites to internet shutdowns, or slowdowns. The Ukrainian ban covers a wide range of communication tools, such as social media, webmail, and search engines. The ban has been repeatedly extended, effectively becoming a permanent feature of the life in Ukraine.

(6) This submission proceeds as follows: First, we examine the potential interference with Article 10 ECHR. Second, we explore the circumstances under which such interference can be considered 'provided by law'. Third, we discuss when such interference is deemed necessary in a democratic society. And finally, we consider whether a state's derogation from Article 10 ECHR exempts it from strictly adhering to the requirements of Article 10(2) of the ECHR.

I. GENERIC WEBSITE BANS AS INTERFERE WITH ARTICLE 10 OF THE ECHR

(7) Article 10 of the ECHR states that everyone has the right to freedom of expression, which includes the 'freedom to hold opinions' and the 'freedom to receive and impart information and ideas' without interference by a public authority 'regardless of frontiers'. Article 10(2) contemplates limitations on these freedoms and exhaustively enumerates the limited grounds for interference by public authorities. The scope of freedom of expression under Article 10 includes the freedom to choose the language in which one wishes to express oneself,[10] the right to access information on social media platforms.[11]

(8) As previously decided by the Court, the internet deserves to receive special consideration as a medium for free speech and expression. The Court confirmed that the internet and social media as being one of the "principal means" to enhance "the public's access to news and facilitating the dissemination of information generally".[12] Repeatedly, it regarded the internet as an essential tool for participation in activities and discussions.[13] In other words, the internet is the most participatory technology humans ever developed owing to low barriers to entry for speakers and readers, leading to diverse content and significant access regardless of frontiers.[14] The special character of the technology is also recognised by the Court of Justice of the European Union ('CJEU') that underlined its potential for "user-generated expressive activity".[15]

(9) The Committee of Ministers of the Council of Europe has recognized that "limited or no access to [information and communication technologies (ICTs)] can deprive individuals of the ability to exercise fully their human rights".[16] The Committee of Ministers identified that ICTs provided "unprecedented opportunities" for everyone to enjoy freedom of expression and posited further that

---

[10] *Egitim v Bilim Emekçileri Sendikasi v Turkey* (App. 20641/05) 25 September 2012.

[11] *Cengiz and Others v Turkey* (App no 48226/10) 1 December 2015 [34]; *Magyar Jeti Zrt v Hungary* (App no 11257/16) 4 December 2018 [66].

[12] *Times Newspapers Ltd (Nos. 1 and 2) v United Kingdom* App Nos. 3002/03 and 23676/03) 10 March 2009; *Perrin v United Kingdom* (App. 5446/03)18 October 2005; *Cengiz and others v Turkey* (App. No. 48226/10) 1 December 2015.

[13] *Murphy v Ireland*, (App No. 44179/98) 10 July 2003 [74]; *Magyar Jeti Zrt v Hungary*, (App. 11257/16) 4 December 2018 [66].

[14] Martin Husovec, 'Rising Above Liability: The Digital Services Act as a Blueprint for the Second Generation of Global Internet Rules' (10 October 2023) Berkeley Technology Law Journal Vol 38, No 3.

[15] ibid.

[16] Preamble, Declaration of the Committee of Ministers on Human Rights and the Rule of Law in the Information Society (CM(2005)56 final of 13 May 2005).

the freedom of expression, information and communication should be respected equally in a digital world; being subjected only to those restrictions provided for in Article 10(2) of the ECHR.

(10) Previously, the Committee had observed that 'prior control' of communication through the internet (i.e., pre-emptive restrictions on what the public can access on the internet) should be an exception and that there was a need to remove barriers to individual access to the internet.[17] Significantly, this Declaration, stipulates the principle that a Member State should not subject content on the internet to restrictions that would go further than those applied to other means of content delivery.[18] Principle 3 of this Declaration emphasizes the importance of the absence of no prior State Control,[19] and states that practices of prior State control, including the 'tendency to block access by the population to content on certain foreign or domestic websites for political reasons' ought to be 'strongly condemned'. The Committee of Ministers has restated its emphasis on 'access to' and 'openness of' the internet as a resource across several recommendations.[20]

(11) Article 19 of the International Convention on Civil and Political Rights ('ICCPR'), like Article 10 of the ECHR, guarantees 'everyone' the right to freedom of opinion and expression, including the freedom to seek, receive, and share information through any media.[21] Restrictions are permitted only when legally justified and necessary but claims of protecting national security often extend beyond legitimate purposes in accordance with Article 19(3). In respect of Article 19 of the ICCPR, the United Nations Human Rights Committee has stated that 'any restrictions on the operation of websites, blogs or any other internet-based, electronic or other such information-dissemination system' are only compatible if permissible under paragraph (3) of Article 19. **The UNHR emphasised that permissible restrictions should be "content-specific" and that "generic bans on the operation of certain sites and systems" were not compatible.**[22]

(12) The Court might also consider the Tshwane Principles, which provide global standards for ensuring the fullest possible public access to information while safeguarding legitimate national security interests.[23] Drafted by 22 organizations and academic centres, these Principles were

---

[17] Preamble, Declaration on Freedom of Communication on the Internet adopted by the Committee of Ministers on 28 May 2003, 840th meeting of the Ministers' Deputies.

[18] Principle 1, Declaration on Freedom of Communication on the Internet adopted by the Committee of Ministers on 28 May 2003, 840th meeting of the Ministers' Deputies.

[19] Principle 3, Declaration on Freedom of Communication on the Internet adopted by the Committee of Ministers on 28 May 2003, 840th meeting of the Ministers' Deputies.

[20] Recommendation on measures to promote the public service value of the Internet, CM/Rec(2007)16; Committee of Ministers, Recommendation on Promoting Freedom of Expression and Information in the New Information and Communications Environment, CM/Rec(2007)11; Recommendation of the Committee of Ministers to Member States on Measures to Promote the Respect for Freedom of Expression and Information with Regard to Internet Filters, CM/Rec(2008)6, adopted on 26 March 2008; Recommendation on the Protection of Human Rights with Regard to Search Engines, CM/Rec(2012)3, adopted on 4 April 2012.

[21] International Covenant on Civil and Political Rights, United Nations General Assembly resolution 2200A (XXI) https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights accessed on 3 November 2024. It was signed by Ukraine on 20 March 1968 and ratified by it on 12 November 1973.

[22] General Comment No. 34: Article 19: Freedoms of Opinion and Expression, UN Human Rights Committee, 21 July 2011 [45].

[23] "The Global Principles on National Security and the Right to Information (The Tshwane Principles)" (Open Society Justice Initiative) <https://www.justiceinitiative.org/publications/global-principles-national-security-and-freedom-information-tshwane-principles> accessed November 4, 2024

developed through consultations with over 500 experts from more than 70 countries across 14 meetings worldwide and were also endorsed by the Parliamentary Assembly of the Council of Europe.[24] As emphasized by Tshwane Principle 4, it is up to the government to prove the necessity of any restrictions on the right to information. The burden of demonstrating the legitimacy of any restriction rests with the public authority seeking to withhold information (Principle 4(a)).

(13) The Court has previously affirmed in *Cengiz and Others v. Turkey* that applicants may claim victim status for internet restrictions that are broad and not specific, and that consequently violate their right to receive information under Article 10.[25] It was observed that the blocking order restricts access to specific content and a significant amount of information that cannot be obtained by any other means, which would inevitably affect the rights of internet users and result in substantial collateral effects. The Court accordingly highlighted that there is a need for a flexible application of victim status criteria, which led it to conclude in the Cengiz case that a ban on YouTube indirectly impacted individuals' rights to receive and impart information. Consequently, it is crucial to consider the application of victim status criteria herein, as previously articulated before the Court, especially as it relates to Article 10.

(14) The right to access the open and unrestricted internet is inherent in the right to access information and communication, and it can be inferred from all the general guarantees protecting freedom of expression.[26] Without exaggeration one might say that **the open internet has become an indispensable technology of human cooperation**. It enabled human connections where they previously were not possible due to distance, it strengthened human cooperation in the public sphere, and fostered human relationships within private sphere, such as in families and communities. Any decision to interfere with the open and unrestricted internet access thus must be considered an interference with Article 10 ECHR.

II. PRESCRIBED BY THE LAW

(15) For an interference by the government to be accepted under Article 10(2) of the ECHR, it must be 'prescribed by law'. The key question in this case concerns what legal basis is appropriate for an extreme measure, such as generic ban on websites in the name of national security.

(16) Often the legal basis for blocking can be found in legislation adopted by the parliaments that empowers the executive to impose sanctions. The Ukrainian Decree was adopted following the Law on Sanctions, which lays down the Ukrainian sanction's regime. It includes two types of sanctions: (A) *personal sanctions:* defined as being imposed against 'a foreign state, a foreign legal entity, a legal entity that is under the control of a foreign legal entity or a non-resident natural person, foreigners, stateless persons, as well as entities that carry out terrorist activities';[27] and (B) *sectoral sanctions:* defined as targeting 'a foreign state or an unspecified group of persons of a certain type of activity'.[28]

---

[24] A Khattab, 'Council of Europe Endorses Global Principles on the Right to Information', (International Commission of Jurists, 2 October 2013) https://www.icj.org/council-of-europe-endorses-global-principles-on-the-right-to-information/ accessed 4 November 2024.

[25] *Cengiz and Others v Russia* (App no 48226/10) 1 December 2015 [55].

[26] *Ahmet Yildrim v. Turkey*, (App No. 3111/10) 18 December 2012 [32].

[27] The Law of Ukraine About sanctions [2014], art 1, para 2.

[28] ibid, art. 5 para 2.

(17) Website blocking bans were introduced through a decision made by the National Security and Defense Council ('NSDC') and then adopted by a presidential decree ('Decree'). Sectoral sanctions must be approved by the Ukrainian Parliament within 48 hours of the presidential decree's issuance.[29] The Decree imposed sanctions on 468 entities based on the nature of their activities. Thus, the sanctions seem more sectoral than personal. However, the parliament did not issue a resolution to approve the Decree as foreseen by law. Moreover, Article 92 of the Constitution of Ukraine states that rights and freedoms can exclusively be restricted by laws.[30] The Decree at issue is not a law, but rather a by-law or secondary legislation. Both points raise concerns as to the appropriate legal basis.

(18) In *Big Brother Watch and Others v. United Kingdom*, the ECtHR recognized that states may, under certain circumstances, exercise the power to intervene through secondary legislation. However, the Court emphasized that such interference must be sufficiently clear, accessible, and foreseeable to ensure compliance with the principle of 'prescription by law' under Article 10 of the ECHR. More precisely, the Court clarified that secondary legislation, adopted by the executive, may comply with the 'prescribed by law' criterion, but only if the legal texts are clear enough for individuals to anticipate and are formulated in such a way as to provide safeguards against arbitrariness.

(19) Even though sanctions often concern situations of emergency, the protection of human rights, namely the right to be informed of the reasons on the basis of which the sanction was imposed and the right to be heard, remain untouched. The CJEU, for instance, deemed them important enough to rule that internationally binding sanctions should still abide by European standards for respecting human rights.[31] The same must be true for generic or specific bans on the entire websites.

(20) The digital services that were blocked are **user-generated content services that not only broadcast editorial information to users**[32] **but also allow individuals to share their own views and communicate with others**. Thus, any ban on such services affects not only those who broadcast but inevitably also those wish to communicate through such services. This in turns affects the scope of individuals who are owed due process rights. In the end, **for user-generated content services it is the widest public that is owed an explanation and remedies to correct the abuses**.

(21) The Court has an elaborate case law to support this point. The case law usually requires[33] that any website blocking is subject to an independent review that is conducted by a decision-making body or a judge *before* blocking measures are adopted. This prior review ensures that the legality and consequences are assessed before individuals and providers are impacted. If an ex-ante review is not possible, then it is essential that at least a swift ex-post assessment is carried out. Emergencies might be a legitimate reason why the executive must act without prior judicial authorisation. However, **no emergency, including a formal derogation from Article 10, should justify that no independent review is ever conducted either before or after the sanctions are implemented**. This is effectively what seems to have happened in the present case. Since the Ukrainian President is the

---

[29] ibid.

[30] *Constitution of Ukraine* (1996); Olga Shumilo, Tanel Kerikmäe, and Archil Chochia, 'Restrictions of Russian Internet Resources in Ukraine: National Security, Censorship or Both?' (2019) 82 *Ukrainian Journal of Law* 88.

[31] *Case C-402/05 Kadi and Al Barakaat International Foundation v Council and Commission* [2008] ECJ.

[32] Compare with the RT Russia ban.

[33] *Ooo Flavus and Others v Russia* (App Nos 12468/15, 23489/15, and 19074/16, ECtHR, 23 June 2020) [40]; *Vladimir Kharitonov v Russia* (App No 10795/14, ECtHR, 23 June 2020) [43].

Chairman of the NSD Council and appoints its 'personal composition', no independent review of the far-reaching generic website bans ever took place.[34]

(22) The associated lack of transparency demonstrates the absence of yet another safeguard. In ECtHR cases so far, transparency usually implies that if the rationale behind the measures is explained in the law and a notice is given to internet access providers, they might be able to defend themselves.[35] The CJEU explicitly extends the right to contest the measures to the affected users,[36] and some national courts require publication of decision in the context of blocked websites.[37]

(23) The Decree in question does not explicitly state the reasons for which it was adopted. The service providers and users should always be able to understand the rationale behind measures that affect greatly either their business or their lives. Combined with the fact that no independent body reviewed the Decree, or its extensions, and the fact that service providers and users were not adequately provided with an opportunity to contest the sanctions in courts or other forum, it is hard to see what safeguards the sanctions regime really offers from abuses of public power. **Even in the situation of emergency, the public power cannot be blindly trusted to always do the right thing. This is why safeguards are an essential component of 'prescribed by the law'.**

III. NECESSITY

(24) Even if the Court were to accept that the measures were 'prescribed by law', the interference also must be 'necessary in a democratic society.' Given that the ECtHR has held that actions by member states in blocking access to social media platforms to be in violation of Article 10,[38] the necessity of such a broad and generic ban on a group of websites is highly questionable.

(25) The legitimate aims of interference are exhaustively set out in Article 10(2). The justified offered is as follows: (i) existence of concerns about safeguarding Ukrainian data and (ii) safeguarding against anti-Ukrainian messaging and/or pro-Russian propaganda. Both of these arguably fall within the scope national security. Moreover, undoubtedly, Ukraine has a broad margin of appreciation in this regard. However, even if a legitimate aim is pursued, the measure can go beyond what is necessary.

(26) To be 'necessary in a democratic society' the measure must use the least restrictive means required to meet the legitimate aim pursued.[39] **National security cannot be a trump card without scrutiny of the true intentions and alternatives of the executive power.** For instance, in this case, the ban: i) targets all Ukrainian citizens, rather than those with access to, for example, potentially sensitive data and ii) prevents the sharing and imparting of all beliefs on widely used platforms, rather than targeting specific speech which may be validly said to pose a threat to national security.

---

[34] Constitution of Ukraine (n 24), art. 107.

[35] *Ooo Flavus and Others v Russia* (App nos 12468/15, 23489/15, and 19074/16) 23 June 2020 [42]; *Vladimir Kharitonov v Russia* (App no 10795/14) 23 June 2020 [33]-[44].

[36] Case C-314/12 *UPC Telekabel Wien* (ECJ 27 March 2014), 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.')

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

[38] *Cengiz and Others v Turkey* (App no 48226/10) 1 December 2015 [34]. See also *Magyar Jeti Zrt v Hungary* (App no 11257/16) 4 December 2018 [66].

[39] *The Sunday Times v. United Kingdom* (No. 2) (App no 6538/74) 26 March1991),(n 7) [35].

(27) The ban is thus *overinclusive* because it prevents any communication on user-generated content platforms rather than targeting specific users, or speech that may pose a valid threat to national security under the Convention. Enforcing an indiscriminate restriction of this kind introduces significant risks to individuals' freedom of expression and their right to privacy[40].

(28) The ECtHR highlights that diverse political programmes must be able to be proposed and debated, even if they call into question the way a State is currently organised, provided that they do not harm democracy itself or advocate for political violence[41] Thus, it may be legitimate for any government to take legal steps to prohibit, and prevent, speech which advocates for engagement in separatist violence (as in *Kaptan v Switzerland*) or which harm democracy. However, the ban in question is an indiscriminate prohibition on communications that prevents imparting and receiving any speech through these platforms, regardless of its content and legality. Such interference goes beyond what is strictly necessary to address the kinds of speech which may present a valid threat to national security.

(29) The generic ban like the one in question also inevitably goes beyond what is necessary to combat disinformation campaigns during the war. The application of the ECHR to measures which specifically combat disinformation is complex, particularly given the high level of protection given to opinions which are less 'susceptible to proof'[42] and the practical difficulties in distinguishing intent for misinformation (spreading of false assertions of fact regardless of intent) and disinformation (deliberately misleading or biased information). In this instance, however, the measure was not specifically targeted at a clear class of disinformation (e.g., electoral disinformation). **The generic ban prohibits all speech, regardless of its content or legality. This is the crux of the measure's disproportionality. Any generic ban on a group of websites is inherently unable to engage with a balancing exercise or meaningful assessment of specific instances of disinformation, as it prohibits the platforms in their entirety.**

(30) Less restrictive measures could have been pursued to combat the illegal disinformation. This could have included prohibiting certain accounts spreading disinformation, demanding compliance from the providers of user-generated content services, or educational campaigns to combat disinformation. Such measures would have been more proportionate as they would have not prevented all speech, regardless of its nature, from taking place on these platforms.

(31) The over-inclusiveness of the ban is also visible from the fact that it targets all individuals using the communication technology indiscriminately, rather than solely those with access to potentially sensitive data. The specific need to preserve the secrecy of information relating to military operations has been recognised by the ECtHR in relation to complaints under Article 10[43]. However, the ban enacted, due to its blanket nature, is incapable of differentiating between, for example, military personnel, who may have access to confidential data which, if lost, would threaten national security, and civilians, who would have no access to any such data. **A less restrictive measure would**

---

[40] *Handyside v United Kingdom* (App no 5493/72) 7 December 1976 [49].

[41] *Socialist Party and Others v Turkey* (App. 25144/94) 25 May1998 [47].

[42] *Lingens v Austria* (App. 9815/82) 8 July 1986 [46].

[43] *Engels v The Netherlands* (No 1) (App no 44801/09) 8 June 1976 [101]-[103].

merely prevent the access to the platforms by military personnel and other persons with access to confidential information.

(32) Even if security concerns went beyond data possessed by members of the military, for instance the concerns about data held by opposition leaders, less restrictive measures could have been pursued. A measure advising individuals not to use these services, or prohibiting access in limited circumstances, would have been more proportionate to the aim pursued. By imposing such a blanket ban, any state risks disproportionately affecting users who are not involved in state activities or who do not have access to the kinds of data which would risk national security.[44]

(33) Therefore, any state must explore alternatives to generic ban on communication services, such as social media, webmail and search engines, before it can justify their blanket ban on the basis of national security. Ukrainian state in this case could have taken means of achieving the same ends (prevention of confidential data breaches and protection against speech which threatens national security) that would interfere less seriously with Article 10.[45] This conclusion is not challenged even by the fact of emergency.

IV. DEROGATION UNDER ARTICLE 15

(34) Under Article 15 of the ECHR, the existence of an emergency opens the door to a state's request for derogation, meaning the suspension of certain rights. However, this does not automatically legitimize all measures; these measures must meet the 'necessity' criterion.

(35) In *Lawless v. Ireland*[46], the Court emphasized that derogations can only be justified in the presence of a danger to national life, i.e., a real emergency. Therefore, when assessing necessity, the restrictions imposed by the state must be proportionate and compatible with the objective and must only respond to the emergency situation. In other words, if the restriction is not really 'necessary', it constitutes a violation of rights even on the grounds of 'emergency'.

(36) In this context, in *Mehmet Hasan Altan v. Turkey*, the Court held that although the state of emergency declared in the aftermath of the coup attempt constituted a justified emergency, some of the restrictions imposed were overbroad and therefore did not meet the necessity criterion.[47]

(37) Under Article 15(1) of the Convention, a State may validly derogate in a time of war or other public emergency threatening the life of the nation. The measures must not go beyond the extent strictly required by the exigencies of the situation and must not be inconsistent with the State's other obligations under international law.

(38) According to the Council of Europe, 'Ukraine's first derogation notification from the Convention and its Additional Protocols was made in June 2015, and amended in November 2015, June 2016, and February 2017. It was partially withdrawn in December 2019 and updated in April 2021. Eventually, it was superseded in March 2022 and extended in June and September 2022.[48]

---

[44] *Delfi AS v Estonia* [GC] (App no 64569/09)16 June 2015 [110]-[113].
[45] *Glor v Switzerland* (App no 13444/04) 30 April 2009 [94].
[46] *Lawless v Ireland* (App no 332/57) 1 July 1961 [28]-[30].
[47] *Mehmet Hasan Altan v Turkey* (App no 13237/17) 20 March 2018 [210]-[213].
[48] Council of Europe (2022), *Legal Analysis of the derogation made by Ukraine under Article 15 of the European Convention of Human Rights and Article 4 of the International Covenant on Civil and Political Rights*, p.7 https://rm.coe.int/legal-analysis-of-the-derogation-made-by-ukraine-under-article-15-of-t/1680aa8e2c accessed 29 October 2024.

Ukraine's earlier derogations did not refer to Article 10, and as such no valid derogation was in place when the measure was introduced. However, the derogation notification in March 2022 did seek to derogate from Article 10 of the Convention.[49] As the Decree was issued 5 years prior to Ukraine's derogation from Article 10, it raises issues of retrospectivity of the derogation, and it is doubtful that they can fall within its scope.

(39) In either case, the measures are still likely go beyond the 'extent strictly required by the exigencies' of the crisis (Article 15(1)) for the following reasons. The Court affords a wide, but not unlimited, margin of appreciation to states in cases involving Article 15.[50] The existence of a 'public emergency' must not serve as a pretext for limiting the freedom of political debate. Measures must seek to protect the democratic order from threats to it, and to safeguard the values of a democratic society[51]. The measures that constitute a blanket ban inevitably go beyond what is strictly necessary to address the security concerns because they suppress political debate by limiting the fora where it can take place. Moreover, the lack of sufficient safeguards undermines their lawfulness.[52] Thus, **even in a situation of valid derogation, the long-lasting and indiscriminate character of the generic ban on websites inevitably goes beyond what is strictly necessary to protect national security in the 'exigencies of the crisis'.**

Conclusions

The European Information Society Institute (EISi) suggests that the Court:

- *Recognises* the right to access the open and unrestricted internet forms part of right to the freedom of expression under Article 10 of the ECHR.
- *Holds* that generic bans of user-generated content websites, such as social media or webmail, or messaging services, disproportionately interfere with individuals' Article 10 rights, due to their indiscriminate nature and inability to engage with a balancing exercise regarding the specific content on, and users of, those websites.
- *Holds* that emergency, including a formal derogation from Article 10, cannot justify that no independent review is ever conducted either before or after the ban is imposed.

[49] Ibid, p. 22, Figure 4.

[50] *Ireland v the United Kingdom* (App no 5310/71) 18 January 1978 [207].

[51] *Mehmet Hasan Altan v Turkey* (App no 13237/17) 20 March 2018 [210]; *Şahin Alpay v Turkey* (App no 16538/17) 20 March 2018 [180].

[52] *Lawless v Ireland (No. 3)* (App no 332/57) 1 July 1961 1 EHRR 15 [37]; *Brannigan and McBride v United Kingdom* (App no 14599/89) 26 May 1993 17 EHRR 539 [61]-[65]; *Aksoy v Turkey* (App no 21987/93) 18 December 1996 23 EHRR 553 [79]-[84].