EUROPEAN INFORMATION SOCIETY INSTITUTE, O. Z.
Registration address: Štítová 1243/1 040 01 Košice, Slovakia
Postal address: Martin Husovec, Haviarska 6, 040 01, Košice, Slovakia
IČO: 42 227 950, www.eisionline.org, eisi@eisionline.org

28th of September 2021

The Registrar

European Court of Human Rights

Council of Europe

F-67075 Strasbourg Cedex

France

Third-Party Intervention by

European Information Society Insitute (EISi)

In re *Valeryevich PODCHASOV v. Russia*

App. No. 33696/19

Introduction

(1) Since the arrival of smartphones, people gravitate towards the use of messaging services as a basic means of communication. Surveillance of what is being said by whom on these apps undoubtedly invades people's privacy. Encryption is a form of self-defence against such surveillance. Backdoors to encrypted communications weaken everyone's self-defence and expose people to security risks.

(2) In *Podchasov v Russia*, the European Court of Human Rights ('ECtHR' or 'Court') is being asked to further clarify its case-law concerning the permissible scope of state surveillance powers. The case concerns a measure of *indiscriminate* surveillance of electronic communications that is based on inadequately drafted legislation with insufficient safeguards. The legislation in question affords Russian authorities the ability a) to arbitrarily target communication services, and b) to extend their surveillance beyond individual suspects with due cause. The Russian authorities used the legislation to effectively ban encrypted messaging services unless they obtain backdoor access to the contents of messages exchanged on them. Such legislation is far from necessary. Law enforcement authorities can investigate and routinely conduct *targeted* surveillance even if suspects use encryption.

(3) Our submission focuses on the "disclosure order" concerning "information necessary to decode electronic messages" directed at "Internet communications organisers" used by millions of individuals around the world. It proceeds as follows. First, we illustrate the *importance of encryption* as a tool that helps to safeguard the right to privacy and freedom of speech. Second, we explain why requiring backdoor access to *all* encrypted messages is *neither necessary nor proportionate*. It generates broad security risks that impact the rights of all users for the sake of few suspects and there are multiple less intrusive alternatives to it. As will be shown, encryption does not stand in the way of the protection of rights or national security. Finally, we address the problem of *effective remedies* in the context of state enforcement delegated to non-state actors by analysing how to protect people affected by orders issued against their services providers.

Encryption and the Convention

(4) End-to-end encryption is a mathematics-based tool that preserves confidentiality and integrity of communications while they are exchanged among individuals. There are many designs of how encrypted services operate, but end-to-end encryption is one of the most privacy-preserving. It works as follows: with a help of a key, any message ('plaintext') is translated into a seemingly random combination of letters, numbers or symbols ('cyphertext'). Apart from senders and receivers, the outsiders see only the cyphertext. In order to translate the cyphertext to plaintext, the receiver needs a 'key' – a short string of text. Such keys are generated in pairs – one is public, the other private.[1] The sender of the message has the receiver's public key, which is used to encrypt the plaintext of the outgoing message. Once the message is received, it cannot be translated back without the private key, which is kept securely on the receiver's phones. The conversion into plaintext takes place directly on the receiver's phone. With end-to-end encryption, neither the private key nor the original message, are available to the operator of the messaging service at any point. This means that no general access to the exchanged content is possible (see generally Kerr & Schneier, Encryption Workarounds (2018) 106 *Georgetown Law Journal* 989).

(5) Encryption guarantees that messages are not modified or intercepted during their travel. It provides technical protection to everyone – the most vulnerable, such as journalists, researchers and opposition leaders, victims of domestic violence against cyber abuse, and to professionals and companies against cyber espionage. The strong relationship between encryption and human rights (in particular Articles 8 and 10 ECHR) has led organisations, such as Human Rights Watch, to call it 'a cornerstone of security in the digital age', one that should not be undermined on purpose by anyone, including national security agencies.[2] As explained by UN rapporteur David Kaye, the encryption software acts as a 'shield' for opinions against external scrutiny – a fact that is 'particularly important in hostile political, social, religious and legal environments'. In *Ahmet Yıldırım v. Turkey* (App. No. 3111/10) the Court held that the internet is 'one of the principal means by which individuals exercise their right to freedom of expression and information' and that it provides essential tools for participation in activities and discussions concerning political issues and issues of general interest'. Without encryption and anonymity, such tools for participation and discussions are of limited use.[3]

---

[1] Kalia, A (2016). *Encryption is a human rights issue: Your privacy and free speech depend on it*, Learn Liberty, [online]. Available at: https://www.learnliberty.org/blog/encryption-is-a-human-rights-issue-your-privacy-and-free-speech-depend-on-it/

[2] Human Rights Watch (2017). *Perils of Back Door Encryption Mandates*, [online]. Available at: https://www.hrw.org/news/2017/06/26/perils-backdoor-encryption-mandates

[3] Kaye, D. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Human Rights Council (2015).

(6) The private sphere that is granted through encryption ensures that one can freely express his or her own opinions. Encrypted communications allow people to develop their personalities without being watched at every step. In this sense, the privacy and speech rights under Article 8 and Article 10 ECHR are mutually reinforcing. They both protect people from *security risks* posed by governments and other actors (see on the concept of data security, see German Federal Constitutional Court, Case No. 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274; CJEU in *Digital Rights Ireland*, C-293/12, para 66 to 68).

Quality of the law

(7) The Russian telecommunications surveillance works in two stages. In the first stage, private companies collect data. To date, the ECtHR's holding in *Zakharov v Russia* (App. No. 47143/06), has not been implemented in Russia.[4] Instead, the quantity of data that telecommunications companies are required to store has been further expanded. For example, communications service providers and Internet communications organisers ('ICOs') are now required to store the content of phone calls and messages for up to six months, on top of the requirement to store information about all subscribers and services provided to them, including metadata, for three years (for telecommunications companies) or one year (for ICOs).[5] ICOs are also required to install equipment permitting the FSB to carry out operational-search activities which are similar to "the SORM" equipment criticized in *Zakharov*.[6] If the content of communications is normally encrypted on the service, the FSB can also request that an ICO effectively stops engaging in full end-to-end encryption ("backdoor order") by storing a separate key relating to all its users just in case one of them might be a suspect in the future (see sub-section 4.1 of section 10.1 of the Information Technologies Act (Federal Law No. 149-FZ of 27 July 2006)). In *Podchasov v Russia*, it is the legality of the "backdoor" order against Telegram, and its future impact on the users of Telegram, that is at stake.

(8) In the second stage, the legislation empowers Russian investigative authorities to gain access to the data gathered.

(9) The ECtHR emphasises that a law must not grant unfettered discretion, even when it relates to national security (*Malone v the United Kingdom,* App. No. 8691/79*,* para 68; *Zakharov,* para 247). Instead, 'the law must indicate the scope of any such discretion conferred on the competent authorities' and 'the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures' so as to 'give individuals adequate protection against arbitrary interference' (*Malone,* para 68; *Zakharov,* para 229).

(10) When FSB issues a "backdoor order" to a particular ICO, such as Telegram, it creates an interference with the rights of affected users of the service. Such an order is secret from the perspective of affected users. It means that all users of that particular platform do not enjoy the effective privacy of their communications anymore, as their contents can be handed over to the FSB and decrypted with help of the centrally stored key. The "backdoor order" is indiscriminate in its nature. It affects all users of a service, not just those who will be targets of further follow-up disclosures. Moreover, since the measure is meant to apply indefinitely, for the messaging service, it becomes a secret law that strips the provider and its users of a possibility to provide a fully encrypted service.

---

[4] Anna Pushkarskaya, Russia is not inferior to the leadership in the number of outstanding decisions of the ECHR, 4 April 2019, https://www.kommersant.ru/doc/3933154

[5] Sub-section 1 of section 64 of the Communication Act (Federal Law No. 126-FZ of 7 July 2003), sub-section 3 of section 10.1 of the Information Technologies Act.

[6] Sub-section 4 of section 10.1 of the Information Technologies Act.

(11) Sub-section 4.1 of section 10.1 of the Information Technology Act provides unchecked discretion to FSB that can formulate their request arbitrarily broadly. According to the law, an ICO must present to the FSB 'the information which is necessary for decoding received, transmitted, delivered or processed electronic messages'. Once ICOs are included in the official register, they are under increased attention of the authorities with separate obligations. It is also worth pointing out that the register of ICOs held by Roskomnadzor at the moment does not include all popular messengers engaged in the usage of the encryption mechanisms.[7] Viber and WhatsApp — the two most popular messengers in Russia — are not included in the register. The FSB arbitrarily targets its "backdoor order" only at Telegram. This means that Telegram, unlike other companies, cannot legally provide end-to-end encrypted services to its users (storage of keys defies the privacy goals of such measures). This broad discretion to deploy such measures allows the Russian authorities to abuse it. For instance, the authorities also attempted to add Zello to the register (a walkie-talkie app that has far fewer users in Russia but was used by truckers protesting a toll collection system) and, when the app provider failed to cooperate, the authorities decided to ban it.[8]

(12) In *Zakharov*, the Court explains that the requirement of foreseeability merits a different interpretation in the context of secret surveillance and interception of communications, as the target's ability to anticipate interception would defeat its purpose (*Zakharov*, para 229). Therefore, the Court collapses the 'quality of law' and the 'necessity' requirement, requiring that the measures should only be applied when they are 'necessary in a democratic society' and that 'adequate and effective safeguards and guarantees against abuse' exist. For this reason, the next two sections explain why "backdoor orders" in the presented setting cannot be viewed as proportionate and can hardly be seen as equipped with sufficient safeguards against abuse by state and non-state actors.

The Necessity of Encryption Backdoors

(13) As pointed out by Amul Kalia, encryption is mathematics.[9] We cannot manipulate a mathematics problem to be solvable by only one specific group of people (e.g. the government). If encryption is compromised by a backdoor, it can be exploited by *anyone*. This is particularly concerning in the modern age, with the ever-increasing numbers of cyber-attacks, including on regular citizens and businesses (e.g. through so-called ransomware attacks that lock systems and demand ransom). The central storage of keys required by orders like the one at stake provides real or potential access to the messages of *all* users without their knowledge. This means that while governments are arguing that backdoors would only be used in investigations, it is the overall security of users that is at risk – at any point in time, any conversation may potentially be decrypted. Since the keys are not stored only by parties to the communication but are also centrally by a messaging app, or another third party, these other parties can be attacked or their access misused.

(14) The request to install encryption backdoors is, therefore, an *indiscriminate measure* interfering with an individual's right to privacy and freedom of expression. It has wide-ranging collateral effects. While accessing the content of encrypted communications may in some cases assist legitimate law enforcement activities, backdoor access compromises the privacy of everyone using the service. Instead of targeting a suspected individual, it affects the privacy of millions of users, thus seriously endangering their private autonomy to speak and think. It exposes them to risks of unauthorized state

[7] See https://www.statista.com/statistics/1116011/poll-on-most-popular-messengers-russia/
[8] See https://techcrunch.com/2018/04/17/russias-telegram-ban-that-knocked-out-15m-google-amazon-ip-addresses-had-a-precedent-in-zello/
[9] Kalia (fn 1).

surveillance and activities of cybercriminals or other actors. Even if the dangers do not materialize, the *knowledge* of such risks produces chilling effects. When authors, researchers, journalists or activists are reluctant to speak up or communicate with their sources, this not only affects *their* freedom of expression and privacy but also the freedom within *society at large*.[10]

(15) Backdoors therefore fundamentally undermine the freedom of expression and privacy benefits that encryption provides. Moreover, they are a drastic response that does not take into account the wider context. Even when the *content* of communications is entirely unavailable due to end-to-end encryption, law enforcement agencies have several ways how to still investigate crimes (see Kerr & Schneier (2018)). They can employ *encryption workarounds*, such as guessing or obtaining private keys held by parties to the communication, using vulnerabilities in the target's software,[11] recover plain-text backups of messages, or access data on a device before it is encrypted. They can also use *alternative techniques*, such as conducting searches, targeted wire-tapping and arrests.

(16) These workarounds and alternative techniques are less restrictive than backdoors because they only impact individuals on a case-specific basis. Only marginally do they impact innocent bystanders. The law enforcement agencies thereby still can achieve access to the relevant messages and they also limit collateral damage. Another obvious difference between backdoors and their alternatives is the costs of the two approaches. While indiscriminate backdoors might be cheaper for the state than some targeted measures (e.g., use of exploits, searches and arrests), they are expensive for society at large due to the security risks they produce. The fact that vulnerabilities are significantly more difficult to use on a large scale due to their labour intensiveness, cost, and logistical complexity, should be viewed positively as hurdles forcing prioritization and targeting of measures.[12]

(17) This approach is also supported by Europol and ENISA that recently issued the following statement: *"Intercepting an encrypted communication or breaking into a digital service might be considered as proportional with respect to an individual suspect, but breaking the cryptographic mechanisms might cause collateral damage. The focus should be on getting access to the communication or information; not on breaking the protection mechanism. The good news is that the information needs to be unencrypted at some point to be useful to the criminals. This creates opportunities for alternatives such as undercover operations, infiltration into criminal groups, and getting access to the communication devices beyond the point of encryption, for instance by means of live forensics on seized devices or by lawful interception on those devices while still used by suspects."*[13] For example, French authorities recently successfully extracted data from an encrypted phone network of criminals by sending an implant to relevant devices under the cover of an apparent update.[14] Similarly, in the case of a murder of a Slovak journalist, Jan Kuciak, Europol together with Slovak law enforcement managed to obtain access to encrypted communications of the alleged instigator of the crime, which were then accepted as legal evidence by courts, without breaking encryption.[15]

---

[10] Parliamentary Assembly of the Council of Europe, Committee on Legal Affairs and Human Rights, Report on Mass Surveillance, AS/Jur (2015) 01, 26 January 2015, p27.

[11] Lily Hay Newman, 2021, *How Law Enforcement Gets Around Your Smartphone's Encryption*, Conde Nast, viewed 28 January 2021, < https://www.wired.com/story/smartphone-encryption-law-enforcement-tools/>

[12] Bellovin S et al., 'Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet', *Northwestern Journal of Technology and Intellectual Property*, 2014 Vol. 12 Issue 1.

[13] Europol and ENISA Joint Statement, 20 May 2016, https://www.europol.europa.eu/publications-documents/lawful-criminal-investigation-respects-21st-century-data-protection-europol-and-enisa-joint-statement-0.

[14] https://www.europol.europa.eu/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe; A & Ors, R. v [2021] EWCA Crim 128.

[15] The data were decrypted by a Slovak law enforcement authority after Europol assisted with extraction of data from the devices (see CJEU, T-528/20, para 68 ff.). For the Slovak Supreme Court ruling, see https://dennikn.sk/2533496/najvyssi-sud-v-pisomnom-rozsudku-o-vrazde-kuciaka-oslobodenie-je-predcasne/

(18) It is important to remind that in addition to measures focused on accessing the *content* of encrypted communications, other viable investigative tools include targeted surveillance and court-ordered use of *metadata*, including location data. Metadata may be sometimes of greater probative value to a criminal investigation than the content of encrypted communications, which may be altered or deleted by users. For instance, when criminals use doublespeak, additional evidence, such as geo-location data, might be required to collect evidence of their intent. Meta-data can link suspects and witnesses to entire social graphs or provide a less manipulable mapping of their daily routines or usual behaviour.

(19) Thus, while encryption may be an obstacle to indiscriminate surveillance, it does not render law enforcement powerless in the context of its *targeted* operations.

(20) Weakening encryption mechanism through "backdoor" orders compromises the overall security of all users of such services. The state is therefore also violating its positive obligation to protect people against abuses by other actors, such as cybercriminals or foreign governments (see e.g. on the positive obligation to protect in cases of cybercrimes, *Volodina v. Russia* (no. 2), App. no. 40419/19). Malicious attacks on people by non-state actors may be facilitated by the state's 'protective' measures weakening encryption for investigations. As aptly put by Europol and ENISA, *"[s]olutions that intentionally weaken technical protection mechanisms to support law enforcement will intrinsically weaken the protection against criminals as well, which makes an easy solution impossible."* Legally mandated introduction of *"backdoors or key escrow to weaken encryption"* would in their view, *"give investigators lawful access in the event of serious crimes or terrorist threats"* but also *"increase the attack surface for malicious abuse, which, consequently, would have much wider implications for society. Moreover, criminals can easily circumvent such weakened mechanisms and make use of the existing knowledge on cryptography to develop (or buy) their own solutions without backdoors or key escrow."*[16]

(21) Any interference with privacy and speech rights must comply with the principle of proportionality, striking a fair balance between the various interests at stake and using the least restrictive means to achieve a particular result. In the present case, "backdoor" orders require a balancing of several different rights: the right to privacy (negative interference), right to freedom of expression (negative interference), and right to life and private life (positive obligations due to security risks) on one hand, and national security and protection of rights of others on the other.

(22) According to the case law, the state must show that less intrusive means to achieve the legitimate law enforcement or national security aims are unavailable or have failed.[17] This has not happened. The state or its authorities did not justify why alternative ways of enforcement (encryption workarounds, alternative techniques and meta-data access) are not sufficient to persecute crimes on messaging services, and how the general security risks created are outweighed by potential benefits in concrete investigations.

(23) Finally, even if states do not abuse their special access, the knowledge that states may engage in mass surveillance without their knowledge has a *chilling effect* on their privacy and speech rights,[18] particularly when it indiscriminately impacts the actions of authors, journalists or civil society activists.[19] Such chilling effects are the reason why the Court of Justice of the European Union is very critical of domestic indiscriminate surveillance measures (*Digital Rights Ireland*, para 37: "is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of

---

[16] See fn (13).
[17] *Cumpănă and Mazăre v Romania* [GC], App. No. 33348/96, para 111, ECHR 2004-XI.
[18] Digital Rights Ireland (C-293/12) at [37], citing Opinion of Advocate General at paragraphs [52] and [72].
[19] Parliamentary Assembly of the Council of Europe, Committee on Legal Affairs and Human Rights, Report on Mass Surveillance, AS/Jur (2015) 01, 26 January 2015, p27.

constant surveillance") and ECtHR when emphasizing deterrence effects and "climate of self-censorship" (*Nedim Şener v. Turkey*, App. No. 38270/11, para 122).

(24) Therefore, the encryption backdoors applied to general messaging services used by the public cannot satisfy the standards for permissible restrictions on Convention rights; by facilitating indiscriminate surveillance of and security risks to large parts of the innocent population, they fail to be proportionate. Backdoors affect all users not only those with 'reasonable suspicion' (*Zakharov*, para 260). The weakening of cryptographic protection mechanisms increases the vulnerability to abuse by both state and non-state actors. Such backdoors cannot be justified by any paralysis of law enforcement operations because the authorities can and routinely do, investigate crimes and national security threats by conducting *targeted* surveillance, even if suspects use encryption. Encryption where only parties to the conversation hold the keys is equally not an obstacle to the enforcement of laws aiming to reduce illegal material online (see CDT 2021 report).[20]

Effective Safeguards

(25) ECtHR has already held in *Zakharov* that the Russian data collection framework violates human rights, as it creates a risk for arbitrary and illegitimate access to data (*Zakharov* at para 196 and 263). At present, encryption is a 'self-defence mechanism' employed by individuals to avoid the potentially arbitrary tapping of their conversations by authorities.

(26) The Russian regulatory regime contains no safeguards for the data collection phase, which includes the storage of keys. The provision requiring messaging services to cooperate by abandoning end-to-end encryption does *not* require the FSB to even obtain formal judicial authorisation. The FSB can target any ICO and formulate the request in any way it seems fit. The law also does not require that the request for encryption keys should be connected to any investigation or any criminal activity. It only states that ICOs are required to provide decoding information to the authorities. The Russian authorities can issue "backdoor" orders without any assessment of proportionality.

(27) Safeguards exist only for the access stage and only to a limited extend. Although there is a requirement under Russian legislation that relevant evidence in criminal proceedings must be obtained through a court order, the de facto situation differs. Firstly, the Court in *Zakharov* acknowledged that Russian investigative authorities have 'direct remote access to those databases' and possess the 'technical means to circumvent the authorisation procedure and to intercept any communications without obtaining prior judicial authorisation' (*Zakharov*, para 196). Secondly, in February 2021, the Ministry of Digital Development, Communications and Mass Media of the Russian Federation suggested carving out certain metadata, including duration of phone calls, and location data from the secrecy of communication which means that the authorities will no longer require court authorisation to receive such data.[21]

(28) In *Szabo and Vissy v Hungary*, the Court summarized that its long-standing case law on domestic surveillance requires clarity on the following six requirements: "the nature of offences which may give rise to an interception order; the definition of the categories of people liable to [be affected]; a limit on the duration [..]; the procedure to be followed for examining, using and storing the data obtained;

[20] Dhanaraj Thakur and others, Outside Looking In: Approaches to Content Moderation in End-to-End Encrypted Systems, available at https://cdt.org/insights/outside-looking-in-approaches-to-content-moderation-in-end-to-end-encrypted-systems/
[21] Vladislav Viktorov, The secrecy of communication will clarify its location, 4 February 2021, https://www.kommersant.ru/doc/4673648

the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or destroyed" (*Szabo and Vissy v Hungary*, App. No. 37138/14, para 56). A quick look at these minimum safeguards shows that they *cannot* be complied with in the context of "backdoor" orders.

(29) Even in the cases of foreign bulk surveillance, the Court required that these minimum safeguards require that "at the domestic level, an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken; that bulk interception should be subject to independent authorisation at the outset when the object and scope of the operation are being defined; and that the operation should be subject to supervision and independent ex post facto review" (*Big Brother Watch and others vs the United Kingdom*, App. No. 58170/13, 62322/14 and 24969/15, para 350).

(30) No such stage-by-stage assessment is possible in the case of backdoor mandates. The weakening of encryption prospectively affects all users of those services. There is no time limit to their application. The law might legislate the requirements that constrain the power of the state to access collected keys and encrypted messages, but such laws only help with safeguarding against *access* abuses. They do not remedy the problem of *security risks* and *chilling effects* that are created by such collection mandates in the first place.

(31) An analogy can be made with the practice of whole-site blocking. The long-standing case law of the Court says that it is an extreme measure because of its *collateral* effects on legitimate content. In *OOO Flavus and Others v. Russia* (App No. 12468/15, 23489/15, and 19074/16), the Court states that the wholesale blocking of access to a website *"is an extreme measure which has been compared to banning a newspaper or television station (..). Such a measure deliberately disregards the distinction between the legal and illegal information the website may contain, and renders inaccessible large amounts of content which has not been identified as illegal. Blocking access to the entire website has the practical effect of extending the scope of the blocking order far beyond the illegal content which had been originally targeted"* (para, 37). Therefore, the measures restricting access should be limited to illegal content. The impact assessment of the blocking measure must ensure that it strictly targets the unlawful content and has no arbitrary or excessive effects, including those resulting from the method chosen to implement it (*Bulgakov v. Russia* (App. No. 20159/15), para. 37).

(32) Stripping users of an entire service of their encryption protection against the outside world and thus exposing them to security risks constitutes a large-scale case of clear collateral damage. By pursuing enforcement in the name of public security, it weakens the self-defence tools of the public.

(33) Therefore, the Court should follow similar argumentation in cases of encryption. If the service at stake is evidently and predominantly used by criminals and terrorists, there might be a case for imposing encryption backdoors on the entire service. However, if the service is used by the country's population in general, the collateral effect on innocent people who will be stripped of their privacy protections is too substantial. With backdoors targetting entire services, all users end up being innocent bystanders to a few investigations conducted by authorities.

(34) As explained in *Engels v Russia* (App. No. 61919/16), within the scope of Article 13 of the Convention, entities subject to restrictive orders should be afforded procedural safeguards and access to effective legal remedies. The remedies must be effective both in law and in practice.

(35) As clearly stated in the ECtHR website blocking case law, even if an extreme measure is permissible, users as the affected parties must have a possibility to appeal the decisions and their implementation. According to *Engels v Russia*, the national procedural rules must also provide a possibility for affected persons to assert their rights before the courts once the restrictive measures

are taken by the service provider. This is particularly important because the participation of the messaging app provider as the party is "not sufficient to endow the proceedings with an adversarial character" (by analogy, *Engels v Russia*, para 32). In particular, it cannot be expected that such a provider will possess the knowledge, motivation and resources required to mount a vigorous defence of his consumers' interests. This is particularly true when a lack of privacy protections aligns with their business interests in surveilling their customers for advertising. Private companies aim to make a profit and hence should not be relied upon to act as a check on the power of the state.[22]

(36) ECtHR has repeatedly held that a state could not absolve itself of responsibility under the Convention by delegating its obligations to private bodies or individuals (*Vukota-Bojić v. Switzerland* App. No. 61838/10, para 47; *Costello-Roberts v. the United Kingdom*, App. No. 13134/87, para 27). Advocate General of the Court of Justice of the European Union, Henrik Saugmandsgaard Øe, succinctly expressed this principle as follows: "The 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" (C-401/19, *Poland v European Parliament/Council*, para 84).

(37) Thus, any legal framework of delegated enforcement requires that the legislator who put it in place can do so only under the condition that it is accompanied by "sufficient safeguards" affected individuals (C-401/19, *Poland v European Parliament/Council*, para 115). This means that if the state decides to mandate the collection of data that creates risk for its people, it has to equally impose strict laws that control how non-state actors secure such data. A failure to align incentives of non-state actors with the state's obligation to protect its people against cyberthreats should be viewed as the state's failure to protect its people in the first place (for the analyses of ECtHR and CJEU case-law to date, see Husovec, (Ir)Responsible Legislature? Speech Risks under the EU's Rules on Delegated Digital Enforcement (2021))[23].

(38) Furthermore, the restrictions must be based on transparent and publicly accessible laws.[24] A court, tribunal or other independent adjudicatory body must supervise the application of the restriction.[25] Public authorities should be obliged by law to assess the potential outcome of implementing orders on innocent users of such services not only at the point when such measure is imposed, but also periodically to make sure that the collateral effect on the security of innocent users is not too substantial. And finally, even in such extreme cases, where collateral effects are assessed to be very low, the risks must be safeguarded not only when the state obtains access to information but also before when the information is still only stored by private parties.

(39) No such effective safeguards exist in the domestic law in Russia today.

---

[22] In the Russian context, see for instance: https://www.nytimes.com/2021/09/17/world/europe/russia-navalny-app-election.html and https://www.reuters.com/world/europe/navalny-allies-accuse-telegram-censorship-russian-election-2021-09-18/

[23] Available at https://ssrn.com/abstract=3784149.

[24] Report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (2015) https://www.undocs.org/A/HRC/29/32, para. 60

[25] Report of UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (2015) https://www.undocs.org/A/HRC/29/32, para. 32

CONCLUSIONS

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

- *holds* that the encryption backdoors applied to general messaging services used by the public cannot satisfy the standards for permissible restrictions on Convention rights; by pursuing enforcement in the name of public security, it weakens the self-defence tools of the public.
- *recognizes* that such backdoors affect all users not only those with 'reasonable suspicion' since the weakening of cryptographic protection mechanisms increases the vulnerability to abuse by both state and non-state actors; backdoors cannot be justified by any paralysis of law enforcement operations because the authorities can and routinely do, investigate crimes and national security threats by conducting *targeted* surveillance, even if suspects use encryption.

- *holds* that any legal framework that delegates enforcement tasks to non-state actors require that the legislator who put it in place can do so only under the condition that it is accompanied by "sufficient safeguards" of rights of affected individuals.
- *recognizes* that the national procedural rules must also provide a possibility for affected persons to assert their rights before the courts once the restrictive measures are taken by the service provider; the presence of the provider alone is not sufficient to endow the proceedings with an adversarial character and it cannot be expected that such a provider will possess the knowledge, motivation and resources required to mount a vigorous defence of his customers' rights.