

Module 6

**Online
Harassment
and
Anonymity**

*Modules on Digital Rights
and Freedom of
Expression Online in
Europe*



ISBN 978-0-9935214-1-6

Published by Media Defence: www.mediadefence.org

This module was prepared with the assistance of ALT Advisory: <https://altadvisory.africa/>

Published in May 2024

This work is licenced under the Creative Commons Attribution-NonCommercial 4.0 International License. This means that you are free to share and adapt this work so long as you give appropriate credit, provide a link to the license, and indicate if changes were made. Any such sharing or adaptation must be for non-commercial purposes and must be made available under the same “share alike” terms. Full licence terms can be found at <http://creativecommons.org/licenses/by-ncsa/4.0/legalcode>.



TABLE OF CONTENTS

1. INTRODUCTION – ONLINE THREATS AND HARASSMENT	1
1.1. International Context.....	3
1.2. Regional Context: European Union.....	3
1.3. Regional Context: Council of Europe	4
2. PROTECTING ONE’S IDENTITY: ANONYMITY, ACCESS TO VPN SERVICES, USE OF ENCRYPTION	5
2.1. International Context.....	5
2.2. Regional Context: European Union.....	7
2.3. Regional Context: Council of Europe	9

MODULE 6

1. INTRODUCTION – ONLINE THREATS AND HARASSMENT

It has been widely recognised that the Internet serves as an enabler for the exercise of a wide range of human rights, in particular for freedom of expression and the right to receive information.¹ At the same time, while new technical developments have enhanced options for journalists to communicate and engage in their journalistic work, they have also led to of online harassment and abuse, in particular affecting women journalists and other marginalised groups. For more information, read our factsheet on Gender & Online Harassment [here](#).

While online harassment occurs in many different fora, social media platforms constitute an especially fertile ground for such behaviours.² For those experiencing online harassment directly, these encounters have profound real-world consequences, ranging from mental or emotional stress to reputational damage or even fear for one’s personal safety.

The ongoing harassment and attacks on members of the media online have become a worrying trend. To exercise their rights to freedom of expression, journalists require access to spaces for public debate, share their ideas and opinions without being censored or in fear of retaliation.³ The fear for their security or when online abuse becomes unbearable may lead to self-censorship and drive them offline or to stop reporting.⁴

Online harassment describes a wide range of digital attacks, including doxxing, surveillance, threats, the non-consensual distribution of intimate or sexual images, stalking, hacking, identity theft and discriminatory speech.⁵ In this context, harassment can also include unwanted and intimidatory activities, for instance through messages or apps.⁶ Some of the most relevant definitions can be found below:

Types of online harassment

Some of the key types of online harassment include the following concepts (Source: PEN America, Defining “Online Abuse”: A Glossary of Terms, (accessible [here](#))).

- **Cyberbullying:** An umbrella term (like “online harassment”) meant to encompass a number of harassing online behaviours. Like physical bullying, “cyberbullying” is generally aimed at young people and refers to the “wilful and repeated harm inflicted through the use of computers, cell phones, and other electronic device”.

¹ See for instance UN Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* UN Doc A/HRC/17/27 (2011), para 67; EEAS, EU Guidelines on Freedom of Expression Online and Offline (undated), p. 3, (accessible [here](#)).

² UNESCO, *Protecting journalism sources in the digital age* (2017), pp. 132-133, (accessible [here](#)).

³ Article19, *Online abuse and harassment against women journalists* (undated), (accessible [here](#)).

⁴ *Ibid.*

⁵ *Ibid.*; see also for a glossary of terms: PEN America, Defining “Online Abuse”: A Glossary of Terms (undated), (accessible [here](#)).

⁶ *Ibid.*

- **Cyber mob attacks:** Cyber-mob attacks occur when a large group gathers online to try and collectively shame, harass, threaten or discredit a target, who often belongs to a traditionally marginalised group. Often, cyber mob attacks occur in retaliation for taking a stance on a politically charged topic or expressing ideas the outrage mob disagrees with.
- **Cyberstalking:** In a legal context, “cyberstalking” refers to the prolonged use (a “course of conduct” of online harassment intended to kill, injure, harass, intimidate, or place under surveillance a target. Cyberstalking can comprise a number of harassing behaviours committed repeatedly or with regularity that usually cause a target to suffer fear, anxiety, humiliation, and extreme emotional distress.
- **Denial of service (DoS) or Distributed Denial-of-Service (DDoS) attacks:** A DDoS attack is a cyberattack that temporarily or indefinitely disrupts internet service by overwhelming a system with data, resulting in the web server crashing or becoming inoperable. In a DDoS attack, the attacker(s) take control of multiple users’ computers in order to attack a different user’s computer. This can force the hijacked computers to send large amounts of data to a particular website or send spam to targeted email addresses.
- **Doxing (or doxing – short for “dropping docs”):** Doxing refers to the publishing of sensitive personal information, such as the home address, email, phone number, photos etc., online to harass, intimidate, extort, stalk, or steal the identity of a target.
- **Hateful speech:** Hateful speech refers to attacks on a specific aspect of a person’s identity, such as their race, ethnicity, gender identity, etc.
- **Non-consensual sharing of intimate images and videos:** Includes sextortion, a form of blackmail in which the abuser threatens to expose intimate or sexually explicit images in order to get a person to do something, as well as the unsolicited sending of sexually explicit or violent images and videos.
- **Online sexual harassment:** Online sexual harassment encompasses a wide range of sexual misconduct on digital platforms and includes some of the more specific forms of online harassment, such as “revenge porn”. It often manifests as hateful speech or online threats. There are four distinct types of online sexual harassment: non-consensual sharing of intimate images and videos; exploitation, coercion and threats; sexualised bullying; and unwanted sexualisation.
- **Trolling:** “Trolling” is one of those terms that’s evolved so much over time as to have no single agreed-upon meaning. The term “trolling” is defined here as the repetitive posting of inflammatory or hateful comments online by an individual whose intent is to seek attention, intentionally harm a target, cause trouble and/or controversy, and/or join up with a group of trolls who have already commenced a trolling campaign. There are three subcategories of trolling to be aware of: concern trolling, where harassers pose as fans or supporters of your work with the intention of making harmful or demeaning comments masked as constructive feedback; dogpiling, where a group of trolls works together to overwhelm a target through a barrage of disingenuous questions, threats, slurs, insults, and other tactics meant to shame, silence, discredit, or drive a target offline; and botnet or sock-puppet trolling, which are used for a variety of reasons, from promoting propaganda to amplifying hate or defamation against targeted individuals.

Combatting online harassment involves many challenges, including getting lawmakers and law enforcement officials to recognise the severity of such harassment and threats, and to treat it with the appropriate levels of concern, recognising that the real and persistent harm suffered applies whether the harassment and threats take place online or offline. Other challenges that arise that are exacerbated in the online sphere relate to the volume of threats that can be received, given the relative ease with which this can be done via social media platforms, for instance; and the concurrent difficulties in identifying perpetrators who are sometimes able to mask their online identities. While this issue ties in with the issue of anonymity online and encryption, it should not be regarded as a sufficient basis for a blanket ban on those technical tools.

1.1. International Context

Freedom of expression is guaranteed both online and offline and crimes against journalists are also committed in both spaces. The UN Human Rights Council (HRC) has emphasised “the particular risks with regard to the safety of journalists in the digital age” which lead to violations of their rights to privacy and freedom of expression.⁷ In addition, it found that impunity for crimes committed against journalists remains “one of the greatest challenges” to their safety and condemns all attacks against journalists online and offline.⁸

In its General Comment No. 34, the UN Human Rights Committee further provides that under no circumstance “can an attack on a person, because of the exercise of his or her freedom of opinion or expression” be justified.⁹ In addition, it recognises that journalists and others are often subjected to threats, intimidation and attacks because of their work.¹⁰

1.2. Regional Context: European Union

Both the Treaty of the EU (Articles 2, 6, 21 and 49) as well as the EU Charter (Articles 7, 8, 10, 11 and 22) contain provisions applicable to online harassment of journalists.¹¹ In this context, the EU has declared as one of its priority for action the “combating violence, persecution, harassment and intimidation of individuals, including journalists and other media actors, because of their exercise of the right to freedom of expression online and offline, and combating impunity for such crimes”, calling upon states to create safe environments for media actors and prevent violence against them.¹² In addition, the EU has committed to “promoting and respecting human rights in cyberspace and other information and communication technologies”.¹³ In 2021, the European Parliament also adopted a legislative-initiative resolution which recommended the Commission to criminalise gender-based cyber violence.¹⁴

⁷ Human Rights Council, Resolution 45/18: The safety of journalists (6 October 2002), A/HRC/RES/45/18, p. 3, (accessible [here](#))

⁸ *Ibid.* p. 4.

⁹ UN Human Rights Committee, General Comment No. 34: Article 19: Freedoms of opinion and expression (12 September 2011), CCPR/C/GC/34, para 23, (accessible [here](#)).

¹⁰ *Ibid.*

¹¹ EEAS, EU Guidelines on Freedom of Expression Online and Offline (undated), pp. 3-4, (accessible [here](#)).

¹² *Ibid.*, p. 7.

¹³ *Ibid.*, p. 10.

¹⁴ European Parliament, Combating gender-based violence: cyber violence (14 December 2021), (accessible [here](#)).

At the same time, experts have criticised that in the EU level, there is no coherent definition of online harassment, which reduces the ability of law enforcement authorities to take action.¹⁵

1.3. Regional Context: Council of Europe

Within the CoE, the Committee of Ministers has dealt with the topic of online harassment in several recommendations. For instance, it has invited states to raise awareness about the sexist misuse of social media and online threats¹⁶ and expressed concern over online harassment and threats¹⁷. The CoE's Parliamentary Assembly has also stressed the need for

“the effective protection of the right to freedom of expression and freedom of information, online and offline, and [...] more must be done to counteract the dangers brought about by abuses of the right to freedom of expression and information on the internet, such as incitement to discrimination, hatred and violence, aimed at women or ethnic, sexual or other minorities in particular; child sexual abuse content, online bullying; the manipulation of information and propaganda; and incitement to terrorism.”¹⁸

The ECtHR has adopted a similar approach. While acknowledging that the Internet has many benefits, it also recognises its dangers, including the dissemination of hate speech and speech inciting violence.¹⁹ Due to the distinct features of the Internet compared to printed media, and the different risks its use poses for the enjoyment of human rights, the rules applied to it must be modified.²⁰

The ECtHR has recognised – although not in the context of journalism – cyberviolence as a specific form of violence against women²¹ and acknowledged its close link to “real life” violence.²² In a case concerning the non-consensual sharing of images and online threats by a former partner, the ECtHR clarified that under Article 8 ECHR, states are obliged to prosecute perpetrators and protect victims from recurrent cyberviolence.²³ It addition, it found that the lack of an investigation into discriminatory and hateful comments can amount to a violation of Articles 14 and 8 ECHR.²⁴

¹⁵ Maria Walsh, Online Harassment: Breaking cyber violence (16 June 2021), (accessible [here](#)).

¹⁶ CoE Committee of Ministers, Recommendation/Rec(2019)1 on preventing and combating sexism (27 March 2019), II.B.3, (accessible [here](#)).

¹⁷ CoE Committee of Ministers, Recommendation/Rec(2016)4 on the protection of journalism and safety of journalists and other media actors (13 April 2016), 18, (accessible [here](#)).

¹⁸ PACE, Internet governance and human rights, Resolution 2256(2019)(23 January 2019), 5., (accessible [here](#)).

¹⁹ ECtHR [GC], *Delfi AS v. Estonia*, App No. 64569/09, §110, 16 June 2015.

²⁰ ECtHR, *Shtekel v. Ukraine*, 33014/05, §63, 5 May 2011.

²¹ ECtHR, *Buturugă v. Romania*, App No. 56867/15, §74, 11 February 2020.

²² *Ibid.* para 74; ECtHR, *Volodina v. Russia* (No. 2), App No. 40419/19, §49, 14 September 2021.

²³ ECtHR, *Volodina v. Russia* (No. 2), App No. 40419/19, §§58-59, 69, 14 September 2021

²⁴ ECtHR, *Beizaras and Levickas v. Lithuania*, App No. 41288/15, §129, 14 January 2020.

2. PROTECTING ONE'S IDENTITY: ANONYMITY, ACCESS TO VPN SERVICES, USE OF ENCRYPTION

Encryption and anonymity are vital to the protection of freedom of expression and the right to privacy online.²⁵

Anonymity can be defined either as acting or communicating without using or presenting one's name and identity or as acting or communicating in a way that protects the determination of one's name or identity or using an invented or assumed name that may not necessarily be associated with one's legal or customary identity.²⁶ Anonymity may be distinguished from pseudo-anonymity: the former refers to taking no name at all, whilst the latter refers to taking an assumed name.²⁷

As recognised by different international bodies,²⁸ anonymity is crucial for the exercise of the right to freedom of expression online. The willingness of individuals to engage in public debates online, in particular those on controversial subjects, is closely linked to the possibility of doing so anonymously. In addition, the disclosure of journalistic sources and other protected materials can have negative consequences for freedom of expression. While the ECtHR found that the ECHR does not contain an absolute right to remain anonymous online, it acknowledged that anonymity is a tool of "avoiding reprisals and unwanted attention [and] is capable of promoting the free flow of opinions, ideas and information".²⁹

Encryption refers to "a mathematical 'process of converting messages, information or data into a form unreadable by anyone except the intended recipient'" and, in doing so, "protects the confidentiality and integrity of the content against third-party access or manipulation."³⁰ With so-called "public key encryption" – the dominant form of end-to-end security for data in transit – the sender uses the recipient's public key to encrypt the message and its attachments, and the recipient uses their own private key to decrypt them.³¹ It is also possible to encrypt data at rest that is stored on one's device, such as a laptop or a hard drive.³²

2.1. International Context

Anonymity and encryption are intrinsically linked to the concepts of privacy and data protection, as they are tools that can be used to protect and advance these rights. In particular, encryption and anonymity have become important ways for political actors, activists, journalists and dissidents to protect their privacy and freedom of expression against specific

²⁵ Article 19, Right to Online Anonymity (June 2015), p. 1, (accessible [here](#)).

²⁶ Electronic Frontier Foundation, *Anonymity and encryption* (2015) at p. 3 (accessible [here](#)).

²⁷ *Ibid.*

²⁸ See Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye* (22 May 2015), A/HRC/29/32, para 60, (accessible [here](#)); Committee of Ministers of the Council of Europe, Declaration on freedom of communication on the Internet (28 May 2003), (accessible [here](#)).

²⁹ ECtHR, *Standard Verlagsgesellschaft MBH v. Austria* (No. 3), App No. 39378/15, §76, 7 December 2021; see also ECtHR [GC], *Delfi AS v. Estonia*, App No. 64569/09, §147, 16 June 2015.

³⁰ Report of the UNSR on Freedom of Expression, 'Report on anonymity, encryption and the human rights framework', A/HRC/29/32 (2015) at para 7 (accessible [here](#)). For further discussion and resources, see UCI Law International Justice Clinic, 'Selected references: Unofficial companion report to Report of the Special Rapporteur (A/HRC/29/32) on encryption, anonymity and freedom of expression' (accessible [here](#)).

³¹ *Ibid.*

³² *Ibid.*

surveillance tools that access data in transfer. As described by the United Nations Special Rapporteur (UNSR) on freedom of expression:³³

“Encryption and anonymity, separately or together, create a zone of privacy to protect opinion and belief. For instance, they enable private communications and can shield an opinion from outside scrutiny, particularly important in hostile political, social, religious and legal environments. Where States impose unlawful censorship through filtering and other technologies, the use of encryption and anonymity may empower individuals to circumvent barriers and access information and ideas without the intrusion of authorities. Journalists, researchers, lawyers and civil society rely on encryption and anonymity to shield themselves (and their sources, clients and partners) from surveillance and harassment. The ability to search the web, develop ideas and communicate securely may be the only way in which many can explore basic aspects of identity, such as one’s gender, religion, ethnicity, national origin or sexuality.”

Encryption and anonymity are essential for the development and sharing of opinions online, particularly in circumstances where persons may be concerned that their communications may be subject to interference or attack by state or non-state actors. They enable individuals to express controversial ideas without fear of reprisal and are of particular importance for whistle-blowers, dissidents and in environments where freedom of expression is heavily censored.³⁴ Encryption and anonymity are therefore specific technologies through which individuals may exercise their rights. The role of encryption as an “enabler of privacy and human rights” has been widely recognised by international bodies and human rights experts.³⁵ Accordingly, restrictions on encryption and anonymity must meet the three-part test in order to be justifiable.

With concern, the Office of the UN High Commissioner for Human Rights (OHCHR) notes that in recent years, governments have increasingly taken steps to undermine the security and confidentiality of encrypted communications, stressing its importance for people to safely holding, expressing, and exchanging opinions.³⁶ In particular, the OHCHR highlights that the essential role of encryption for journalists, human rights defenders, women and civilians in armed conflict.³⁷

According to the UNSR on freedom of expression, while encryption and anonymity may frustrate law enforcement and counter-terrorism officials and complicate surveillance, state authorities have generally failed to provide appropriate public safety justification to support the restriction or to identify situations where the restriction has been necessary to achieve a

³³ Report of the UNSR on Freedom of Expression, ‘Report on anonymity, encryption and the human rights framework’, A/HRC/29/32 (2015) at para 12 ([accessible here](#)).

³⁴ Article 19, Right to Online Anonymity (June 2015), p. 1, ([accessible here](#)).

³⁵ Human Rights Council, ‘The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights’ (2022) A/HRC/51/17 ([accessible here](#)) at paras 20 and 22, UN High Commissioner for Human Rights, Apple-FBI case could have serious global ramifications for human rights (3 March 2016), ([accessible here](#)); see also: UN General Assembly, Resolution 75/176: The right to privacy in the digital age (16 December 2020), A/RES/75/176; Human Rights Council, Resolution 39/6: The safety of journalists 27 September 2018), A/HRC/RES/39/6; Human Rights Council, Resolution 45/18: The safety of journalists (12 October 2020), A/HRC/RES/45/18; Human Rights Council, Resolution 48/4: The right to privacy in the digital age (13 October 2021), A/HRC/RES/48/4

³⁶ Human Rights Council, ‘The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights’ (2022) A/HRC/51/17 ([accessible here](#)) at para 21.

³⁷ *Ibid.*

legitimate goal.³⁸ Outright prohibitions on the individual use of encryption technology disproportionately restrict the right to freedom of expression as it deprives all online users in a particular jurisdiction of the right to carve out a space for opinions and expression, without any particular claim of the use of encryption being for unlawful ends.³⁹ Likewise, state regulation of encryption may be tantamount to a ban, for example through requiring licences for encryption use, setting weak technical standards for encryption or controlling the import and export of encryption tools.⁴⁰

The UNSR on freedom of expression has called on states to promote strong encryption and anonymity and noted that decryption orders should only be permissible when they result from transparent and publicly accessible laws applied solely on a targeted, case-by-case basis to individuals (not to a mass of people), and subject to a judicial warrant and the protection of due process rights of individuals.⁴¹ Likewise, the OHCHR has echoed these calls by recommending that States avoid all direct, or indirect, general and indiscriminate restrictions on the use of encryption, target individuals only when authorised by an independent juridical body on a case-by-case basis, and only when strictly necessary for the investigation or prevention of serious crimes.⁴²

2.2. Regional Context: European Union

Various EU institutions have stressed the importance of encrypted communications. For instance, in 2020 the Council of the European Union drafted a resolution on encryption noting that:

“The European Union fully supports the development, implementation and use of strong encryption. The European Union underlines the need to ensure full respect for fundamental and human rights and the rule of law in all actions relating to this resolution, online as well as offline. Encryption is a necessary means of protecting fundamental rights and the digital security of governments, industry and society. At the same time, the European Union needs to ensure the ability of competent authorities in the area of security and criminal justice, e.g. law enforcement and judicial authorities, to exercise their lawful powers, both online and offline protecting our societies and citizens.”⁴³

Similarly, the European Communications Code, [Directive 2018/1972](#) of the EU, also recognises the need for encryption as a security measure and provides that:

“Member States shall ensure that providers of public electronic communications networks or of publicly available electronic communications services take appropriate and proportionate technical and organisational measures to appropriately manage the risks posed to the security of networks and services. Having regard to the state of the art, those measures shall ensure a level of security appropriate to the risk presented. In particular, measures, including

³⁸ Report of the UNSR on Freedom of Expression, ‘Report on anonymity, encryption and the human rights framework’, A/HRC/29/32 (2015) at para 36 (accessible [here](#)).

³⁹ *Ibid* para 40.

⁴⁰ *Ibid* para 41.

⁴¹ Report of the UNSR on Freedom of Expression, ‘Report on anonymity, encryption and the human rights framework’, A/HRC/29/32 (2015) at paras 59-60 (accessible [here](#)).

⁴² Human Rights Council, ‘The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights’ (2022) A/HRC/51/17 (accessible [here](#)) at pp.16-17.

⁴³ Council of the European Union, ‘Council Resolution on Encryption: Security through encryption and security despite encryption’ (2020) 13084/1/20 REV 1 (accessible [here](#)) at p. 2.

encryption where appropriate, shall be taken to prevent and minimise the impact of security incidents on users and on other networks and services.”⁴⁴

At the same time, anonymity online and encryption have sparked debates between lawmakers, state agencies and civil society actors in recent years. The use of encrypted communications has in particular raised concerns with law enforcement authorities regarding the identification of terrorists and perpetrators of cybercrime, citing the “dilemma of privacy versus security online.”⁴⁵ Against the backdrop of several terror attacks in Europe in the mid-2010s, some – including several lawmakers – begun perceiving encryption as an obstacle to law enforcement and have engaged in efforts to weaken it.⁴⁶

In 2020, the European Commission’s draft paper on “Technical solutions to detect child sexual abuse in end-to-end encrypted communications” was leaked. The document details different options to detect illegal content in end-to-end encrypted communications,⁴⁷ which were heavily criticised by experts for their numerous security and privacy risks⁴⁸.

On 11 May 2022, the European Commission then release a proposal for a law to “Prevent and Combat Child Sexual Abuse” (CSA Regulation), which would impose an obligation on hosting, interpersonal communication and other service providers to detect, report, remove and block CSA material. This obligation extends to unknown CSA material in end-to-end encrypted, interpersonal communications, while the proposal did not include the possibility for providers to refuse the execution of a detection order based on its technical impossibility.⁴⁹ This proposal received widespread criticism, including by tech experts and civil society organisations. The European Data Protection Supervisor and the Chair of the European Data Protection Board released a joint opinion, highlighting how encryption technologies “contribute in a fundamental way to the respect for private life and confidentiality of communications, freedom of expression as well as to innovation an growth in the digital economy”.⁵⁰ With regards to the Commission’s proposal, they raised “serious data protection and privacy concerns” and called for an amended proposal that meets the requirements of necessity and proportionality and does “not result in the weakening or degrading of encryption on a general level.”⁵¹

On 14 November 2023, the EU Parliament’s Committee on Civil Liberties, Justice and Home Affairs adopted its position, adding protection for end-to-end-encrypted communication⁵² by

⁴⁴ Article 40 of the European Electronic Communications Code.

⁴⁵ Europol, ‘Director’s Speech at the conference: Privacy in the Digital Age of Encryption and Anonymity Online’ (19 May 2016) (accessible [here](#)).

⁴⁶ Cited in Maria Koomen, ‘The Encryption Debate in the European Union: 2021 Update’ (2021) at pp. 1-2 (accessible [here](#)).

⁴⁷ See Technical Solutions to Detect Child Sexual Abuse in End-to-End Encrypted Communications (accessible [here](#)).

⁴⁸ Global Encryption, Breaking encryption myths: What the European Commission’s leaked report got wrong about online security (November 2020), (accessible [here](#)).

⁴⁹ EDPB-EDPs, Joint Opinion 4/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse (28 July 2022), p. 6, (accessible [here](#)).

⁵⁰ *Ibid.* p. 6.

⁵¹ EDPB-EDPs, Joint Opinion 4/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse (28 July 2022), p. 36, (accessible [here](#)).

⁵² European Parliament, Child sexual abuse online: effective measures, no mass surveillance (14 November 2023), (accessible [here](#)); see also Andy Yen, EU Parliament made the correct decision on Chat Control today (14 November 2023), (accessible [here](#)).

excluding it from the scope of detection orders⁵³. Eyes have now turned to High-Level Expert Group on access to data for effective law enforcement, co-chaired by the Commission and the Presidency of the Council of the EU,⁵⁴ for which encryption and anonymisation have been, inter alia, identified as the most pressing issues⁵⁵.

2.3. Regional Context: Council of Europe

The Council of Europe's Commissioner for Human Rights has stressed that encryption is "indispensable for the effective protection of the right to privacy, freedom of expression, and many other human rights" as well as the confidentiality for journalistic sources and the physical security of individuals such as human rights defenders, their families, networks, beneficiaries and colleagues.⁵⁶

On 13 February 2024, the ECtHR issued a judgment in *Podchasov v Russia*, a case which concerned a fine imposed on the messenger Telegram after it had refused an order by Russian authorities to disclose technical information to disclose the end-to-end encrypted communications of several individuals suspected terrorism-related activities. The Court also highlighted the importance of encryption technology to protect the right to private life and freedom of expression and as a defence "against abuses of information technologies, such as hacking, identity and personal data theft, fraud, and the improper disclosure of confidential information."⁵⁷ The Court then goes on to explain that to enable the decryption, it would be necessary to weaken encryption for all users by creating backdoors, making it technically possible to perform general and indiscriminate surveillance of all users' communications.⁵⁸ It concludes that the

"obligation to decrypt end-to-end encrypted communications risks amounting to a requirement that providers of such services weaken encryption mechanisms for all users; it is accordingly not proportionate to the legitimate aims pursued."⁵⁹

⁵³ European Parliament, Child sexual abuse online: effective measures, no mass surveillance (14 November 2023), (accessible [here](#)).

⁵⁴ European Commission, High-Level Group (HLG) on access to data for effective law enforcement (21 March 2024), (accessible [here](#)); Statewatch, "Going dark": will the next assault on privacy take place behind closed doors? (19 April 2023), (accessible [here](#)); Article19, EU: Open letter on security-cloaked threats to encryption (11 January 2024), (accessible [here](#)).

⁵⁵ Council of the European Union, Scoping paper for the High-Level Expert Group on access to data for effective law enforcement (13 April 2023), p. 5, (accessible [here](#)).

⁵⁶ CoE Commissioner for Human Rights, Encryption in the age of surveillance (26 September 2023), (accessible [here](#)).

⁵⁷ ECtHR, *Podchasov v. Russia*, no. 33696/19, §76, 13 February 2024.

⁵⁸ *Ibid.* §77.

⁵⁹ *Ibid.* §78.