

Module 1

Digital Rights and Emerging Challenges

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



ISBN 978-0-9935214-1-6

Published by Media Legal Defence Initiative: www.mediadefence.org

This report 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.....	1
2. FREE EXPRESSION AND ONLINE RESTRICTIONS	1
2.1. Considerations for speech online.....	4
3. PROTECTING THE RIGHTS OF OTHERS ONLINE.....	5
4. KEY CONCEPTS IN ONLINE SPEECH LITIGATION.....	6
4.1. Intermediary Liability	6
4.2. Data Protection	6
4.3. Social Media Blocking.....	7
4.4. 'The Right to be Forgotten'.....	7
4.5. Artificial Intelligence	8
4.6. Net Neutrality	8
4.7. Transnational violations of digital rights.....	9

MODULE 1

1. INTRODUCTION

The term “digital rights” is commonly used to refer to the way in which the classic and fundamental human rights contained in instruments such as the International Covenant on Civil and Political Rights (the ‘ICCPR’) and the International Covenant on Economic and Social Rights (the ‘ICESCR’) are interpreted in our present digital era, where much of human life is intermediated by digital technologies such as the Internet and social media. Understanding digital rights is crucial to being able to protect fundamental human rights in any domain, as very little of our lives today is immune from the forces of technology and the internet, which have reshaped how humans communicate, participate in public life, and behave.

Digital spaces were largely unregulated when they first emerged. While many countries have since made progress in regulating the digital sphere, including passing data protection laws to protect privacy online and adapting criminal legislation to account for cybercrimes, these spaces continue to present novel governance challenges and new threats, as well as opportunities, for the advancement of human rights.

For example, the Internet, social media, and other technologies have created new opportunities for cross-border expression and collaboration that have radically advanced freedom of expression in some ways.

At the same time, however, digital technologies have been used in some places to further anti-democratic practices that limit freedom of expression - such as shutting down or censoring the internet and using digital technology to conduct mass surveillance. Across Eastern Europe and Central Asia, the use of technology to enable authoritarian tactics by governments and repressive techniques by private actors has ramped up in recent years.¹ As new technologies continue to evolve at a rapid pace with the development of, for example, live facial recognition and generative AI, these risks become increasingly complex to manage, including through the law. Protecting and developing online spaces where human rights can be respected and promoted therefore requires effective responses to oppressive regulations and innovative solutions.

2. FREE EXPRESSION AND ONLINE RESTRICTIONS

In 2022, international digital rights advocacy organisation Access Now published a [report](#) documenting the use of digital technology by both authoritarian and democratic regimes in Eastern Europe and Central Asia to “advance their interests at the expense of people’s freedoms.” For example, it notes that “artificial intelligence algorithms are used for racial profiling, spyware tools threaten people’s privacy, and digital identity programs undermine data protection and enable discrimination.”²

¹ Access Now, ‘Digital Dictatorship: Authoritarian Tactics and Resistance in Eastern Europe and Central Asia’ (October 2022) (accessible [here](#)).

² Ibid.

In parts of Europe, concerns have been raised about “the expansion of ubiquitous data collection systems, including biometric surveillance, powered by artificial intelligence (AI) and algorithmic decision-making,” “internet shutdowns and other network disruptions, as well as mass and targeted surveillance,” “government hacking or state-sponsored online harassment campaigns,” and “the expansion of digital authoritarian practices outside national borders through targeting diaspora or the export of surveillance technology.”³ The effect of these measures is that freedom of expression online is restricted, often unjustifiably.

Article 19(2) of the ICCPR stipulates that the right to freedom of expression applies regardless of frontiers and through any media of one’s choice. The UN General Comment No. 34 further explains that article 19(2) includes internet-based modes of communication.⁴

In a 2016 resolution, the UN Human Rights Council ([UNHRC](#)) affirmed that:⁵

[T]he same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one’s choice, in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.

While freedom of expression is clearly protected by a considerable body of treaty law, it can also be regarded as a principle of customary international law, given how frequently the principle is enunciated in treaties, as well as other soft law instruments. Most human rights treaties, including those dedicated to the protection of the rights of specific groups — such as women, children, and people with disabilities — also make explicit mention of freedom of expression.⁶ The European Convention on Human Rights (the ‘ECHR’) provides protection for freedom of expression through Article 10:

1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

³ European Parliament, ‘Digital technologies as a means of repression and social control’ (2021) ([accessible here](#)).

⁴ See UNHRC, ‘General Comment 34 on Article 19: Freedom of Expression’ (2011) ([accessible here](#)) at para. 12.

⁵ UNHRC, ‘Resolution on the promotion, protection and enjoyment of human rights on the internet’, (2016) at para. 1 ([accessible here](#)).

⁶ Id.

The European Court of Human Rights (the 'ECtHR') has noted in a number of cases that the Internet provides an unprecedented platform for the exercise of freedom of expression,⁷ holding that, in view of its accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information generally.⁸

The ECtHR has held that the blocking of access to the Internet may be a violation of Article 10, on the basis it offends the rights set forth in Article 10 which are secured "regardless of frontiers".⁹ Further, the Court has observed that an increasing amount of services and information is available only via the Internet¹⁰ and that political content ignored by the traditional media is often shared via the Internet thereby facilitating the emergence of 'citizen journalism'.¹¹

In the context of online speech, the ECtHR has emphasised that Article 10 is to apply to communication on the Internet, whatever the type of message being conveyed and even when the purpose is profit-making in nature.¹² It recently held in favour of a political party that made available a mobile application allowing voters to share anonymous photographs of their invalid ballot papers and their comments on why they were voting in this way.¹³

With respect to press freedom, the ECtHR has reiterated that, having regard to the role the Internet plays in the context of press activity and its importance for the exercise of the right to freedom of expression generally, the absence of an appropriate legal framework at the domestic level allowing journalists to use information obtained from the Internet without fear of incurring sanctions seriously hinders the exercise of the vital function of the press as a "public watchdog". This court has noted that the exclusion of such information from the legislative guarantees provided to journalists in the exercise of their role may give rise to an unlawful interference with press freedom.¹⁴

At the European Union level, press freedom is considered a fundamental right established in the EU Charter of Fundamental Rights, with its provision on press freedom similar to that of the European Convention on Human Rights (ECHR). Article 11 of the Charter states as follows:

1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.
2. The freedom and pluralism of the media shall be respected.

⁷ *Delfi AS v. Estonia* [GC], no. 64569/09, § 110, ECHR 2015; *Cengiz and Others v. Turkey*, nos. 48226/10 and 14027/11, § 52, ECHR 2015 (extracts).

⁸ *Times Newspapers Ltd v. the United Kingdom* (nos. 1 and 2), nos. 3002/03 and 23676/03, § 27, ECHR 2009; *Delfi AS v. Estonia* [GC], § 133.

⁹ *Yıldırım v. Turkey*, no. 21482/03, § 67, 24 November 2009.

¹⁰ *Kalda v. Estonia*, no. 17429/10, § 52, 19 January 2016

¹¹ *Cengiz and Others v. Turkey*, § 52.

¹² *Ashby Donald and Others v. France*, no. 36769/08, § 34, 10 January 2013.

¹³ *Magyar Kétfarkú Kutya Párt v. Hungary* [GC], no. 201/17, § 91, 20 January 2020.

¹⁴ *Magyar Jeti Zrt v. Hungary*, no. 11257/16, § 60, 4 December 2018.

The EU has been to the forefront in legislating for protections around privacy in the face of rapid technological advancements. The Court of Justice of the European Union (CJEU) has played a significant role to implementing those protections, often to the detriment of press freedom. These modules explore how the CJEU, and the ECtHR, have shaped the law in relation to press freedom in Europe, and indeed elsewhere, through a series of seminal judgments on a range of novel issues that have emerged as a consequence of online speech.

2.1. Considerations for speech online

The ECtHR has recognised that the Internet can facilitate clearly unlawful speech, including defamatory remarks, hate speech and speech inciting violence. The emphasis is on the speed with which such information can be disseminated, its reach, and its availability, theoretically forever.¹⁵ The ECtHR has distinguished the Internet from print media, especially as regards the capacity to store and transmit information. It has acknowledged that the electronic network, serving billions of users worldwide, is not and potentially will never be subject to the same regulations and control, and that the policies governing reproduction of material from the printed media and the Internet may differ. The rules governing the latter undeniably have to be adjusted according to the technology's specific features in order to secure the protection and promotion of fundamental rights and freedoms.¹⁶

However, the ECtHR has also noted that while social media platforms for example remain powerful communication tools, the choices inherent in the use of the Internet and social media mean that online information does not have the same effect as information published or broadcast through other media,¹⁷ and that a telephone interview broadcast in a programme available on an Internet site had a less direct impact on viewers than a television programme.¹⁸

The **CJEU** has also played a significant role in developing standards on online speech. With the introduction of the Fundamental Rights Charter in 2000, Article 11 of that treaty 'corresponds' to Article 10 of the ECHR subject to some deviations.

Although the Explanatory Note for Article 11 does 'not as such have the status of law', it provides essential information in explaining the textual differences between the Charter and ECHR.¹⁹ For example, in the note explicitly stating Article 10(2) ECHR and describing the role of Article 52(3) of the Charter in making the 'meaning and scope of this right' as the same as that guaranteed by the ECHR, it is observed that any limitations on the core freedom may not exceed those provided in Article 10(2). Article 11(2) of the Charter explicitly references the media in relation not only to the CJEU's 'case law [and legislation] regarding television' but also relates to the ECtHR's previous statements regarding the

¹⁵ *Delfi AS v. Estonia* [GC], § 110 above n 7.

¹⁶ *Editorial Board of Pravoye Delo and Shtetel v. Ukraine*, no. 33014/05, § 63, ECHR 2011 (extracts).

¹⁷ *Animal Defenders International v. the United Kingdom* [GC], no. 48876/08, § 119, ECHR 2013 (extracts).

¹⁸ *Schweizerische Radio- und Fernsehgesellschaft SRG v. Switzerland*, no. 34124/06, § 64, 21 June 2012.

¹⁹ Explanations relating to the Charter of Fundamental Rights (2007/C-303/02): explanation on Article 11.

media's broader societal role, as endorsed by the CJEU's statement that the media plays a significant role as a public 'watchdog'.²⁰

The CJEU **defines freedom of expression** as including "the expression of opinions and the freedom to receive and impart information".²¹ The case law of the CJEU is particularly interesting in the way it has balanced the right to freedom of expression online with the right to privacy. For example, in the debate between the right to be forgotten and the right to freedom of expression, it is the right to privacy that is emphasised. The CJEU has developed detailed balancing principles based on the idea in relation to the right to be forgotten that the ECtHR has expanded on, as discussed in more detail in Module 2 on privacy and data protection.²²

3. PROTECTING THE RIGHTS OF OTHERS ONLINE

In relation to online speech, the ECtHR has stated that the risk of harm posed by online content to the exercise and enjoyment of human rights and freedoms, particularly the right to respect for private life, is higher than the risk posed by the press.²³ The ECtHR has therefore recognised the importance of the Internet in the exercise of freedom of expression, but it has also established that liability for defamation or other unlawful speech must, in principle, be retained and constitute an effective remedy for violations of the right to reputation among other rights.²⁴ However, the Court may also take into account other factors that reduce the impact of online content on the interests protected by Article 10.²⁵

The **nature of the Internet** is a factor to be considered when ruling on the level of seriousness in order for an attack on personal reputation to fall within the scope of Article 8.²⁶ The amplifying effect of the Internet was considered in a case concerning an individual accused of antisemitism. The impugned speech was published on an association's website, and the association had been ordered to remove the article in question. The Court noted, in particular, that the potential impact of the antisemitism allegation was considerable and was not limited to the usual readership of the publication in which it had been published. Using a search engine allowed access to the article on a worldwide basis. The publication therefore had a considerable impact on the reputation and rights of the individual concerned.²⁷

Consistent with the position of the UNHRC, set out in its 2016 resolution,²⁸ the ECtHR considers that the general principles applicable to offline publications also apply online. Examples of this include where private or personal information is published on the Internet, such as a person's name or a description of them, the need to preserve confidentiality in this regard can no longer constitute an overriding requirement, in that this information has ceased

²⁰ C-421/07 *Frede Damgaard* [2009] ECR I-2629 [AG 81], citing *The Observer & The Guardian Ltd v United Kingdom* App No 13585/88 (ECtHR, 26th November 1991) para 59. N

²¹ *Tietosuoja- ja valtuutettu v. Satakunnan Markkinapörssi E.C.R. I-9831* [2008] Case C-73/07.

²² *Google Spain v. AEPD* (2016)

²³ *Delfi AS v. Estonia* [GC], § 133; *Editorial Board of Pravoye Delo and Shtekel v. Ukraine*, § 63.

²⁴ *Delfi AS v. Estonia* [GC], § 110

²⁵ *Kozan v. Turkey*, no. 16695/19, § 51, 1 March 2022.

²⁶ *Arnarson v. Iceland*, no. 58781/13, § 37, 13 June 2017.

²⁷ *Cicad v. Switzerland*, no. 17676/09, § ..., 7 June 2016

²⁸ UNHRC, 'Resolution on the promotion, protection and enjoyment of human rights on the internet', (2016) at para. 1 (accessible [here](#)).

to be confidential and is in the public domain. In such cases, the Article 8 rights fall to be considered.²⁹

In a finding that a webmaster's criminal conviction for public insult against a mayor in respect of comments published on the Internet site of an association chaired by him had been excessive, it was noted in particular that the comments in question related to expression by the representative body of an association, which was conveying the claims made by its members on a subject of general interest in the context of challenging a municipal policy.³⁰ In the context of animal and environmental protection which is undeniably in the public interest, the ECtHR has held that it had been proportionate to issue an injunction which prevented an animal rights organisation from publishing on the Internet a poster campaign featuring photos of concentration camp inmates alongside pictures of animals reared in intensive farming conditions.³¹

4. KEY CONCEPTS IN ONLINE SPEECH LITIGATION

In cases where online speech has been restricted, or where an individual's rights have been harmed as a consequence of an online publication, a range of different concepts have arisen. Most of those issues will be addressed in detail in the subsequent modules, so here they will only briefly be introduced. Other relevant concepts, such as net neutrality or the impact of artificial intelligence, will be considered here in more detail as they have not yet been the subject of extensive litigation in Europe.

4.1. Intermediary Liability

Intermediary liability occurs where governments or private litigants can hold technological intermediaries, such as ISPs and websites, liable for unlawful or harmful content created by users of those services.³² This can occur in various circumstances, including copyright infringements, digital piracy, trademark disputes, network management, spamming and phishing, "cybercrime", defamation, hate speech, child pornography, "illegal content", offensive but legal content, censorship, broadcasting and telecommunications laws and regulations, and privacy protection.

Notwithstanding that there is consensus among many freedom of expression advocates that insulating intermediaries from liability for content generated by others is a fundamental principle that protects the right to freedom of expression online, courts in Europe have taken a different view in a range of cases raising different factual considerations. This topic will be discussed in more detail in subsequent modules.

4.2. Data Protection

In Europe, the primary legislation governing protection of data is the GDPR, which took effect across all EU Member States from 25 May 2018. It replaced the 1995 EU Data Protection Directive. The GDPR is an ambitious piece of legislation which took over four years to agree.

²⁹ *Aleksey Ovchinnikov v. Russia*, no. 24061/04, § 49-50, 16 December 2010.

³⁰ *Renaud v. France*, no. 13290/07, § 40, 25 February 2010.

³¹ *PETA Deutschland v. Germany*, no. 43481/09, 8 November 2012.

³² See *Delfi AS v. Estonia* [GC] [GC], no. 64569/09, ECHR 2015.

One of its key aims was to create a harmonised approach to data protection across the EU, with increased rights for individuals in an age of rapid technological advances.

While the GDPR is primarily known for its effect on business, it has also brought about significant changes to data processing by media outlets, which are often overlooked in discussions about data protection. The GDPR recognises that data protection is not an absolute right. Regulators in different states are often asked to reconcile two fundamental rights: the right to data protection and freedom of expression, particularly in the context of journalism.

The 'journalistic exemption' is found at Article 85 of the GDPR and it requires Member States to regulate the extent to which GDPR applies to journalists and others writing in the public interest. As discussed in more detail in other modules the journalistic exemption can be applied unevenly across Member States, and this raises serious concerns about the use of data claims as a new form of SLAPP against journalists.

4.3. Social Media Blocking

Unlike in other jurisdictions around the world, countries in Europe have been less prone to shutting down the internet when faced with protests or other challenges. There have however been a number of important cases in the region on the blocking of particular social media websites or online media outlets. The ECtHR has found in several cases that a wholesale blocking order against a website is an extreme measure, which has been compared by the UN Human Rights Committee and other international bodies to banning a newspaper or broadcaster. In the case of *OOO Flavus and Others v. Russia*, concerning the unjustified wholesale blocking of opposition online media outlets, the ECtHR considered that this measure, which deliberately ignored the distinction between illegal and illegal information, was arbitrary and manifestly unreasonable.³³

4.4. 'The Right to be Forgotten'

The 'right to be forgotten' is not an international legal standard. It came to the fore with the decision of the CJEU in *Google Spain*³⁴ in which the CJEU held that data protection principles apply to the publication of search results of search engines. It held that **individuals should be able to ask search engines operating in the EU to delist search results obtained by a search of their name** if the links were "inadequate, irrelevant or no longer relevant, or excessive." The scope of the right to be forgotten was limited in a number of ways, including to search engines, and imposed the requirement to de-list search results associated with an individual's name.³⁵ It has since been codified as the Right to Erasure under the EU's General Data Protection Regulation (GDPR). According to the CJEU's judgments it did not extend to the underlying content in issue, for example newspaper archives. The expansion of the right to be forgotten by the ECtHR will be discussed in a later module.

³³ *OOO Flavus and Others v. Russia*, 12468/15 and 2 others, § 34, 23 June 2020.

³⁴ CJEU, *Google Spain v AEPD & Mario Costeja Gonzalez*, 13 May 2014, C-131-12. ECLI:EU:C:2014:317.

³⁵ Since then, the Article 29 Working Party and Google's Advisory Council have published guidelines on the way in which 'right to be forgotten' requests under *Google Spain* should be treated. The Article 29 Guidelines state that there is an exception to not delist pages "for particular reasons, such as the role played by the data subject in public life," such that the data processing is justified by "the preponderant interest of the general public in having, on account of inclusion in the list of results, access to the information in question."

4.5. Artificial Intelligence

The recent development of Large Language Models (LLMs) and their use in chatbots and LLM-enabled software systems have become increasingly popular. Although the impact AI will have on freedom of expression online will develop in the face of rapid technological advancement concerns have been raised about, for example, how culpability for privacy defamation and data protection breaches can be determined. Absent any significant case law on this emerging area, the impact of AI on one recently developed concept, the right to be forgotten, is briefly considered here.

Overall, LLMs have similar source data to search engines, and the datasets used to develop these models may contain personal data, causing similar concerns to those raised in the Google Spain case. That decision initially imposed an obligation on search engines to delist an impugned link, so that it would not appear in a search using particular terms. The ECtHR has endorsed the removal of the source - the impugned web page - containing the personal information.³⁶ Neither method works with LLMs. Efforts to remove personal data from training datasets in order to avoid publication of private information would almost certainly offend the requirement that such information be removed without “undue delay”, as required by the GDPR. Further, removing hallucinated data - that is, a response generated by AI which contains false or misleading information presented as fact – is difficult because such data are not contained in the training dataset of the model. Removing some hallucinated data could result in new hallucinations.

4.6. Net Neutrality

Net neutrality is primarily debated at the EU level. It refers to the way that Internet Service Providers (ISPs) manage the data or traffic carried on their networks when data is requested by broadband subscribers, referred to as end-users in EU law, from providers of content, applications, or services, as well as when traffic is exchanged between end-users. In the EU, this is dealt with by the **Open Internet Regulation**.³⁷

Under EU rules, ISPs are not permitted to block or slow down internet traffic, except where necessary. There are **exceptions** however, relating to: management of traffic to comply with a court order, to ensure the integrity of the network integrity and to ensure security, and to manage temporary network congestion or congestion which arises exceptionally, but only as long as equivalent categories of traffic are treated the same. EU law provide for an end-user’s right to be “free to access and distribute information and content, use and provide applications and services of their choice”.³⁸ Specific provisions ensure that national authorities can enforce this right. **The ‘best effort’ internet** is about the equal treatment of data traffic being transmitted over the internet. It envisages that ‘best efforts’ are made to carry data, no matter what it contains, which application transmits the data, or where it comes from.

In the US, the Federal Communications Commission (FCC), which had voted in 2017 to repeal the laws on net neutrality, recently decided to restore it to, as they describe it, “ensure

³⁶ *Biancardi v. Italy*, no. 77419/16, 25 November 2021.

³⁷ Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and retail charges for regulated intra-EU communications and amending Directive 2002/22/EC and Regulation (EU) No 531/2012.

³⁸ *Ibid.*

the internet is fast, open, and fair.” In so doing the FCC noted that it would be able to provide effective oversight over broadband service providers, giving it essential tools to: “Protect the Open Internet – Internet service providers will again be prohibited from blocking, throttling, or engaging in paid prioritization of lawful content ...; Safeguard National Security – The Commission will have the ability to revoke the authorizations of foreign-owned entities who pose a threat to national security to operate broadband networks in the U.S. The Commission has previously exercised this authority under section 214 of the Communications Act to revoke the operating authorities of four Chinese state-owned carriers to provide voice services in the U.S.; and Monitor Internet Service Outages – When workers cannot telework, students cannot study, or businesses cannot market their products because their internet service is out, the FCC can now play an active role.”³⁹

4.7. Transnational violations of digital rights

Many states have extended their cyber operations, including their surveillance capacity, beyond their territorial borders, increasing the risk that domestic legal restrictions will be evaded. This has important implications for press freedom, as such operations are capable of intercepting journalistic communications and related data that can identify journalistic sources. A cyber operation that facilitates state access to journalists’ communications and related data without adequate safeguards is more likely to affect public interest journalism due to the nature and content of that journalism.

In *Al-Skeini v United Kingdom* the ECtHR Grand Chamber described the general principles relevant to the question of extraterritorial jurisdiction in the following terms: “A state’s jurisdictional competence under article 1 is primarily territorial. Jurisdiction is presumed to be exercised normally throughout the state’s territory. Conversely, acts of the contracting states performed, or producing effects, outside their territories can constitute an exercise of jurisdiction within the meaning of article 1 only in exceptional cases. To date, the Court in its case law has recognised a number of exceptional circumstances capable of giving rise to the exercise of jurisdiction by a contracting state outside its own territorial boundaries. In each case, the question whether exceptional circumstances exist which require and justify a finding by the Court that the state was exercising jurisdiction extra-territorially must be determined with reference to the particular facts.”⁴⁰

Until recently, the ECtHR had not considered the question of extraterritorial jurisdiction in situations involving state cyber operations. The decision in *Wieder and anor. v United Kingdom* provided that court with an opportunity to do so, but it instead decided it was not required to assess the case on extraterritoriality grounds. Instead, the ECtHR found that the UK had *territorial jurisdiction* in cases that concern the risk of bulk interception of the electronic communications of persons residing outside its territory. So, for guidance on how courts might consider extraterritoriality in this context we can look to a recent decision of the German Constitutional Court on extraterritorial cyber operations for guidance on how this question is considered.⁴¹

The question before the Constitutional Court was whether the fundamental rights of the Basic Law are binding on the Federal Intelligence Service and the legislator that sets out its powers, regardless of whether the Federal Intelligence Service is operating within Germany or abroad,

³⁹ NPR, Net neutrality is back: U.S. promises fast, safe and reliable internet for all, (accessible [here](#)).

⁴⁰ ECtHR, *Al-Skeini and Others v the United Kingdom* [GC], no. 55721/07, §§131-132, ECHR 2011; See also ECtHR, *Georgia v Russia (II)* [GC], no. 38263/08, §81, 21 January 2021.

⁴¹ BVerfG, *Urteil des Ersten Senats vom 19 Mai 2020 - 1 BvR 2835/17 -*, Rn. 1-332 (accessible [here](#) and [here](#)).

and whether the protection provided by Article 5, relating to freedom of expression, and Article 10, relating to privacy, applies to telecommunications surveillance of foreigners in other countries.⁴² The challenge was brought against legislative provisions permitting the Federal Intelligence Service⁴³ to carry out surveillance of foreign telecommunications, to share that intelligence with domestic and foreign bodies, and to cooperate with foreign intelligence services in respect of that intelligence. It therefore raised very similar factual issues to the ones the Court must consider in these present cases.

The relevance of the Constitutional Court's analysis partly lies in its focus on the applicability of international human rights principles to that question. The Constitutional Court began by noting that the Basic Law provides that the authority of the state is bound by the fundamental rights contained within it and that no restrictive requirements that make that binding effect dependent on a territorial connection with Germany or on the exercise of specific sovereign powers can be inferred.⁴⁴ It specifically noted that this characterisation applies to freedom of expression and privacy, which require to be protected from surveillance measures.⁴⁵

The judgment emphasised the relationship between fundamental rights provided for in the Basic Law and international human rights law and noted that while “the Basic Law deliberately differentiates between human rights and rights afforded only to German citizens ... this does not mean that human rights should also be limited to domestic matters or state action in Germany. There is nothing in the wording of the Basic Law to suggest such an understanding.”⁴⁶ Importantly, it found that restricting the application of the Basic Law to Germany's territorial boundaries would undermine universal human rights.⁴⁷

One of the key factors in the Constitutional Court's analysis, no doubt influenced by the range of methods available to the state when engaged in extraterritorial surveillance, was the importance of ensuring fundamental rights protections march in step with state behaviour, noting that a failure to do so would “[g]iven the realities of internationalised political action and the ever increasing involvement of states beyond their own borders ... result in a situation where the fundamental rights protection of the Basic Law could not keep up with the expanding scope of action of German state authority and where it might – on the contrary – even be undermined through the interaction of different states. Yet the fact that the state as the politically legitimated and accountable actor is bound by fundamental rights ensures that fundamental rights protection keeps up with an international extension of state activities.”⁴⁸ This is particularly relevant in the context of states using technological and other advancements to evade their obligations under human rights law.

A further important aspect of this case lies in the Constitutional Court's recognition that the Basic Law is designed to “provide protection whenever the German state acts and might thereby create a need for protection – irrespective of where and towards whom it does so.”⁴⁹ This approach is consistent with recent developments on the international legal plane, notably

⁴² While this case deals with the extraterritorial application of the constitution of a state, the Intervener would submit that broadly the same considerations apply in that regard as apply to the extraterritorial application of the Convention.

⁴³ The *Bundesnachrichtendienst* or *BND*.

⁴⁴ See Article 1(3) Basic Law for the Federal Republic of Germany (*Grundgesetz – GG*). See also, BVerfG, *Judgment of the First Senate of 19 May 2020 – 1 BvR 2835/17*, §88 (accessible [here](#)).

⁴⁵ Article 5 and Article 1 Basic Law for the Federal Republic of Germany (*Grundgesetz – GG*).

⁴⁶ BVerfG, *Judgment of the First Senate of 19 May 2020 – 1 BvR 2835/17*, §94 (accessible [here](#)).

⁴⁷ *Id.*, §97.

⁴⁸ *Id.*, §96.

⁴⁹ *Id.*, §89.

with respect to the so-called ‘functional’ approach.⁵⁰ In applying this approach the Constitutional Court expressly noted that the Convention “does not stand in the way” of Basic Law rights being applied abroad.⁵¹ On that basis, an individual who is resident in London and who is the subject of a cyber operation conducted by German intelligence agents, would come within the jurisdiction of the German state.

⁵⁰ See for example Yuval Shany, *Taking Universality Seriously: A Functional Approach to Extraterritoriality in International Human Rights Law* (28 August 2013), *The Law & Ethics of Human Rights*, vol. 7, no.1, pp 47-71

⁵¹ BVerfG, *Judgment of the First Senate of 19 May 2020 – 1 BvR 2835/17*, §99, (accessible [here](#)).

Module 2

**Data
Protection
and Press
Freedom**

*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	1
2. THE RIGHT TO BE FORGOTTEN	3
2.1. CJEU Case-law	3
2.2. GDPR	4
2.3. Press Freedom v the Right to be Forgotten	5
2.4. 'De-indexing'	5
2.5. Anonymisation	7
2.6. Balancing in L.M. and W.W. v. Germany	7
2.7. The new balancing test in Hurbain v. Belgium [GC]	8
3. CONCLUSION	12

MODULE 2

In this new information age, the task of safeguarding personal information has gained dramatically in significance and complexity. As online data sharing and data collection continue to expand rapidly, law and policy makers play catch up with the threats the new reality poses to our privacy. Europe, with its high level of internet penetration,¹ has been at the forefront of developing legal safeguards for the protection of personal data online. Although laws and policies continue to evolve in this field and the tension between the right to personal data and other rights is far from being resolved, robust protection measures have already been implemented in most national jurisdictions and at the EU level. Some of them, however, come at a serious cost to freedom of expression. Within the Council of Europe framework, the European Court of Human Rights have tested some of these measures, with mixed results. Stronger protection of personal data is not always a bad thing for journalists. They benefit from it too, especially when it comes to such new threats as digital surveillance and online intimidation and harassment. This module, however, focuses on the aspects of data protection that come into conflict with freedom of expression online, with special emphasis the right to be forgotten.

1. INTRODUCTION

“Personal data” refers to any information relating to an identified or identifiable individual² (i.e., an individual who can be directly or indirectly identified without requiring unreasonable time, effort or resources³). While not an independent right under the European Convention of Human Rights, protection of personal data is recognised as an integral part of the right to respect for one’s private life guaranteed in **Article 8 of the ECHR**. For a long time, tension between freedom of the media and the right to privacy emerged largely from an act of *publishing* protected personal data. It is in this context that the ECtHR initially developed its approach to balancing between the two rights. However, digital technologies have revolutionised how personal data is collected, stored, analysed, and shared, and with the media having moved online, it has made almost all of media content indefinitely accessible to anyone with internet connection regardless of when it was published. Moreover, search engines have made retrieving such content exceptionally easy. In this new environment, the online *retention* of publications – that is, their continuous ready availability on the internet – has become a separate concern for anyone seeking to protect their privacy from the media. The solution to this new challenge arrived in the form of a “right to be forgotten”, famously conceptualised by the CJEU in the Google Spain case. Since then, national courts and the ECtHR have grappled with reconciling measures designed to implement the right to be forgotten with freedom of the media – with mixed results.

¹ In 2022, some 85% of Europeans were active on the internet. See Edouard Mathieu and others, ‘Number of people using the internet’ *Our World in Data* (2023) (accessible [here](#)).

² Article 2 of the Council of Europe’s Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) (accessible [here](#)).

³ Explanatory report, para. 17 (accessible [here](#)).

Legal framework for data protection: the European Union

The right to the protection of personal data is expressly recognised in Article 8 of [the Charter of Fundamental Rights of the European Union](#) (which is binding on both the EU institutions and bodies and the EU member states). Article 8 stipulates that personal data “must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law” and that everyone “has the right of access to data which has been collected concerning him or her, and the right to have it rectified.” It also obliges member states to establish independent authorities to supervise the implementation of these requirements.

Central to the EU’s data protection regime is the [General Data Protection Regulation](#) (GDPR), adopted in April 2016. As the world’s most advanced piece of legislation on the subject, it has influenced data protection laws in many countries outside the EU.

The **GDPR’s regime is based on the following principles** for processing personal data:⁴

- Personal data must be processed fairly and lawfully, and must not be processed unless the stipulated conditions are met.
- Personal data must be obtained for a specified purpose (or purposes), and must not be further processed in any manner incompatible with that purpose.
- Personal data must be adequate, relevant and not excessive in relation to the purpose (or purposes) for which it is processed.
- Data must be accurate and, where necessary, kept up to date.
- Personal data must not be kept for longer than is necessary for collection.
- Personal data must be processed in accordance with the rights of data subjects provided for under the data protection law.
- Appropriate technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data must not be transferred to another country that does not ensure an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal information.

Legal framework for data protection: the Council of Europe

The 1981 [Convention for the Protection of Individuals with regard to Automated Processing of Personal Data](#) (a.k.a. Convention 108) was the first legally binding international instrument dedicated to data protection. In 1999, it was [amended](#) to allow the European Communities to join it. In 2001, an [Additional Protocol](#) was adopted to introduce new obligations related to supervisory authorities and transborder data flow. Finally, in May 2018, an [Amending Protocol](#) was adopted to introduce a new, “modernised” version of the Convention, referred to as [Convention 108+](#) (not yet in force).⁵ The modernisation version brings the Convention closer to the GPDR regime. However, one of the significant remaining gaps is that Convention 108+

⁴ Information Commissioner’s Office, ‘A guide to the data protection principles’ (accessible [here](#)).

⁵ For a summary of the main changes introduced by Convention 108+, see Council of Europe, ‘The modernised Convention 108: novelties in a nutshell’ (accessible [here](#)).

does not introduce a data subject's right to obtain the erasure of their personal data (the right to be forgotten), which is expressly guaranteed in Article 17 of the GDPR.

In addition, the Committee of Ministers of the Council Europe has adopted several recommendations directly relevant to data protection online:

- Recommendation [CM/Rec\(2010\)13](#) of the Committee of Ministers to member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling;
- Recommendation [CM/Rec\(2012\)3](#) of the Committee of Ministers to member States on the protection of human rights with regard to search engines;
- Recommendation [CM/Rec\(2012\)4](#) of the Committee of Ministers to member States on the protection of human rights with regard to social networking services.

As was mentioned above, the right to the protection of one's personal data has been read by the European Court of Human Rights into Article 8 of the ECHR. A few examples of the large variety of personal data the European Court of Human Rights ('the ECtHR') has found to be protected by Article 8 include: internet subscriber information associated with specific dynamic; fingerprints, cellular samples, and DNA profiles; publicly accessible information on the taxable income and assets of private individuals; data collected by means of non-covert video surveillance.⁶

2. THE RIGHT TO BE FORGOTTEN

Digital technologies have fundamental changed not only how media content is created and published, but also how it can be stored, shared and accessed. Thanks to search engines, an article published online can now be easily retrieved by anyone with internet connection – and, in theory, may continue to be so for an indefinite period. This is even increasingly true for old publications that first existed only in print form, as print media archives become digitalised and available online.

The continuous ready availability of media content on the internet has become a separate data protection concern, the regulative response to which has taken the form of a "right to be forgotten."

2.1. CJEU Case-law

The right to be forgotten was famously endorsed by the Court of Justice of the European Union in the [Google Spain](#) case in 2014. At the heart of that case was a complaint to the Spanish Data Protection Agency that had been submitted by a person who did not want for two old newspaper reports with his name in them to appear in Google search results when his name was entered in the search engine. The part of the complaint that related to the newspaper had been rejected by the agency (as it found the publication of the information to be legally justified). However, the agency had upheld the request that Google remove links to the articles

⁶ For more examples, see ECtHR's Guide to the Case-Law of the of the European Court of Human Rights guide, p. 8 (accessible [here](#)).

from its search results. Google challenged the decision in Spanish courts, which eventually led to the case's referral to the CJEU for a preliminary ruling.

The CJEU established that a search engine was a 'controller' in the meaning of EU data protection law (paras.33-34) and the very display of personal information on a search results page constituted processing of that data (para. 57). It then observed that the processing of personal data by a search engine "is liable to affect significantly the fundamental rights to privacy and to the protection of personal data when the search [...] is carried out on the basis of an individual's name, since that processing enables any internet user to obtain through the list of results a structured overview of the information relating to that individual that can be found on the internet — information which potentially concerns a vast number of aspects of his private life and which, without the search engine, could not have been interconnected or could have been only with great difficulty — and thereby to establish a more or less detailed profile of him" (para. 80). The impact on the rights of data subjects is magnified by "the important role played by the internet and search engines in modern society, which render the information contained in such a list of results ubiquitous" (ibid). At the same time, the CJEU recognised that de-listing of links from search results could affect internet users' legitimate interest in access information and, therefore, requires balancing that takes account of the nature of the information in question, its sensitivity for the data subject's private life, and the interest of the public in having that information (para. 81).

The CJEU concluded that data subjects' requests for delisting lawfully published and factually accurate content must be satisfied, if the information "appears, having regard to all the circumstances of the case, to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine" (para. 94). However, an exception would have to be made when "for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of inclusion in the list of results, access to the information in question" (para. 97).

The **de-listing obligations** of search engines was further refined in several subsequent cases. In particular, in [GC and Others](#), the CJEU clarified the responsibilities of search engines in respect of so-called sensitive data (this type of data is defined in Article 9 of the GDPR which, with certain exceptions, prohibits its processing). The CJEU concluded that because of how search engines operate the restrictions on processing sensitive data do apply to them *ex ante* and systematically. Instead, search engines are only obliged to conduct *ex post* verification at the request of a data subject (para. 47). Other relevant cases include [Google v CNIL](#) (the territorial scope of the right to be forgotten) and [TU, RE v Google LLC](#) (delisting inaccurate information).

2.2. GDPR

Following the CJEU ruling in *Google Spain*, the right to erasure/the right to be forgotten was expressly introduced by the GDPR in Article 17. The right applies in the following circumstances:

- When the personal data is no longer necessary for the purpose for which it was originally collected or processed;

- When the data controller is relying on an individual's consent as the lawful basis for processing the data and that individual withdraws their consent;
- When the data controller relies on legitimate interests as its justification for processing an individual's data, the individual objects to this processing, and there is no overriding legitimate interest for the data controller to continue with the processing;
- If a data controller is processing personal data for direct marketing purposes and the individual objects to this processing;
- If a data controller processed an individual's personal data unlawfully;
- If personal data must be erased in order to comply with a legal obligation; or
- A data controller has processed a child's personal data in order to offer access to information society services.⁷

Importantly, **Article 17 also provides for exceptions** to the right to erasure which include, in particular, data processing necessary for exercising freedom of expression and information and for archiving purposes in the public interest or scientific or historical research.

The European Data Protection Board has issued [guidelines](#) on the application of Article 17 to search engines.

2.3. *Press Freedom v the Right to be Forgotten*

The CJEU case-law discussed above has dealt with only one of the possible ways to realise the right to be forgotten, namely, delisting through the removal of a link from search results based on the name of the person concerned. However, **national jurisdictions have developed other measures**, including those aimed directly at publishers/content providers. They include requesting website publishers to:

- de-index the article fully or partially by means of access codes or directives issued to search engine operators, so as to prevent certain publications to appear in name-based search results;
- remove a certain article from the index of the website's internal search engine;
- add a note to a published text where the information it contains is inaccurate, incomplete or outdated;
- anonymise the person referred to in the contested text;
- remove all or part of the contested text from a digital archive.

While the negative impact of search engine delisting on freedom of the media should not be underestimated, the impact of obligations imposed directly on publishers is, arguably, even more serious. The ECtHR has tested some of these measures, as it grapples with finding the right balance between the right to privacy manifesting itself in the right to be forgotten, on the one hand, and freedom of expression, on the other.

2.4. *'De-indexing'*

Similarly to delisting by search engines, 'de-indexing' – in the sense this term has been used by the ECtHR – is designed to make it impossible to search for an article about a certain

⁷ GDPR.EU, 'Everything you need to know about the "Right to be forgotten"' (accessible [here](#)).

person by entering the name of that person into a search tool, without affecting the article's content or online location. De-indexing, however, is carried out not by search engines, but by publishers/ website owners.

In *Biancardi v. Italy* (appl. no. 77419/16, judgment of 25 November 2021), the ECtHR examined the compatibility of de-indexing with freedom of expression for the first time. The applicant was the editor-in-chief of an online newspaper that had been required to de-index an old article about a restaurant fight and the resultant criminal case. About two and a half years after the publication, one of the persons involved in the fight requested that the applicant remove the article from the internet. The applicant refused to do it, but eight months later he de-indexed the article in an attempt to settle the court case initiated by the requestors. The domestic courts, however, found the applicant liable for failing to have the article de-indexed in a timely manner and ordered him to pay moral damages to the plaintiff. At the same time, the courts were satisfied that de-indexing alone was sufficient (as opposed to removing the article). The ECtHR agreed with the domestic courts and found that the applicant's freedom of expression had not been violated.

Most of the Court's previous balancing between freedom of expression and the right to privacy was concerned with the lawfulness of initial publications. In this case, however, it was the continued availability of an initially lawful publication that had to be assessed. This crucial difference led the Court to begin adapting its balancing exercise to the right to be forgotten. The Court identified the following two aspects of the case as the most relevant: the period for which the article remained online and how it impacted the right of the person concerned to his reputation, and the fact that the data subject was a private individual not acting within a public context as a political or public figure (para. 62).

In *Biancardi*, the Court effectively set aside the criteria formulated by the Grand Chamber in *Axel Springer AG v. Germany* [GC] (appl. no. 39954/08, judgment of 7 February 2012) (see para. 64). Instead, it focused on the following:

- (i) **the length of time for which the article was kept online:**
The criminal proceedings against the requesting party were still underway at the time the final decision was made by the Italian courts in the applicant's case. However, the Court did not make much of this fact, pointing out instead that the information contained in the article had not been updated since the occurrence of the events described (para 65). The Court also found it relevant that the article remained easily accessible (searchable) for eight more months after the formal right-to-be-forgotten request was submitted to the applicant (ibid).
- (ii) **the sensitiveness of the data:**
Because the data included in the article related to criminal proceedings, the Court considered it as 'sensitive' (and, presumably, requiring a higher level of protection) (see para. 67).
- (iii) **the gravity of the sanction imposed on the applicant (see para 64):**
The applicant was held liable under civil law (as opposed to criminal law), and while the amount of compensation he was ordered to pay was "not negligible", the Court did not find it to be excessive (para 68).

It is important to mention that in its Grand Chamber judgment in *Hurbain v. Belgium* (discussed below), the Court again revised the balancing test for right-to-be-forgotten cases, incorporating both the Biancardi criteria and the criteria previously articulated in *Axel Springer AG v. Germany*.

2.5. Anonymisation

With digitalised press archives made widely accessible online, it became conceivable for initially lawful publications to grow incompatible with the right to privacy simply because after a certain time the information they contained has lost its relevance. The ECtHR first grappled with this possibility in *L.M. and W.W. v. Germany* (appl. nos. 60798/10 and 65599/10, judgment of 28 June 2018). The applicants sought the anonymisation of old media files related to their criminal trial which, fourteen years later, were still available online. While recognising the novelty of the legal issues raised by the case, the Court applied the same balancing criteria as those developed for dealing with initial publications. It agreed with the decision of the German Federal Court of Justice to reject the applicants' request. In its Grand Chamber judgment in *Hurbain v. Belgium* [GC] (appl. no. 57292/16, judgment of 4 July 2023), the ECtHR revisited the issue of anonymisation, recalibrating the balancing test and, controversially, endorsing the modification of the contents of an initially lawful publication as an alternative to having it delisted or de-indexed.

2.6. Balancing in *L.M. and W.W. v. Germany*

L.M. and W.W. v. Germany

In 1993, the applicants were convicted of the murder of a well-known actor and sentenced to life imprisonment. In 2007, as they were about to be released from prison, they initiated proceedings against several media organisations, seeking the anonymisation of certain archive files related to the 1993 trial documents as they were still accessible on the organisations' websites. Their anonymisation requests were eventually rejected by the Federal Court of Justice.

Although the relevant media materials were unquestionably lawful at the time of their publication, the ECtHR recognised that the applicants had a legitimate Article 8 interest "in no longer being confronted with their acts, with a view to their reintegration" (para. 100). It tacitly accepted that the right to be forgotten could, in principle, impose obligations on the original publisher of information containing protected personal data. However, it indicated that the balancing outcomes might be different for a publisher ("whose activity is generally at the heart of what freedom of expression is intended to protect") and a search engine ("whose main interest is not in publishing the initial information about the person concerned, but in particular in facilitating identification of any available information on that person and establishing a profile of him or her") (para. 97). In other words, the Court suggested that a person's right to have certain media content delisted by search engines did not automatically translate into their right to have that content modified (anonymised).

For the actual balancing, the Court applied the same criteria as those it previously adopted for dealing with the privacy impact of media content at the time of its publication. In reaching its conclusion that the continuing online availability of the relevant media materials did not violate the applicant's rights under Article 8, the Court considered the following points:

(i) The materials' continuing contribution to a debate of public interest

The Court recognised that the public had an interest "in being informed about criminal proceedings and in being able to obtain information in that regard, especially when the proceedings concern particularly serious judicial facts which attracted considerable attention" (para. 98). Crucially, the contested materials still retained their public interest value when the anonymisation requests were made (para. 105).

The Court also recognised that anonymising a media report was still a sufficiently serious interference with freedom of the media, even if it was less restrictive than the deletion of the report in its entirety. Having reiterated that "the approach to covering a given subject was a matter of journalistic freedom", it concluded that "the inclusion in a report of individualised information such as the full name of the person concerned [was] an important aspect of the press's work [...], especially when reporting on criminal proceedings that have attracted considerable interest" (para. 105).

(ii) The applicants' public profile

The Court concluded that the applicants were not simply private individuals unknown to the public at the time of their request for anonymity. They acquired a degree of notoriety during the trial, which attracted considerable public attention because of the nature of the crime and the fame of the victim. Although the public's interest in the crime began to wane with time, the applicants returned to the limelight when they made several attempts to have their case reopened and spoke to the press on the matter (see para. 106).

(iii) The applicants' prior conduct vis-à-vis the media

The applicants' courted media attention as they campaigned for having their case reopened (see para. 108).

(iv) The materials' content, form, and dissemination

The contested materials reported objectively on the trial and their veracity, and their lawfulness at no time of publication was not called into question (para. 111). They only appeared in sections of the relevant websites that were clearly labelled as old news coverage, and, for that reason, they were not likely to attract the attention of internet users who were not seeking information about the applicants (paras. 112 and 113). There was no indication that access to the reports was maintained with the intention of re-disseminating information about the applicants (para. 113).

Although the Court expressly refrained from considering less restrictive alternatives to anonymisation because this point had not been discussed by the domestic courts, it did observe that the applicants had made no attempt to contact search engine operators to make the contested reports less easy to find (para 114).

2.7. The new balancing test in *Hurbain v. Belgium* [GC]

In this Grand Chamber [judgment](#), the ECtHR revisited the issue of anonymisation, refining and expanding the criteria for balancing freedom of the media against the right to be forgotten. The applicant, a newspaper publisher, was ordered by a Belgian court to anonymise the online version a twenty-year-old article stored in the newspaper's digital archive. The article contained a report on a fatal traffic accident and included the full name of the person responsible. The anonymisation order was based on a right to be forgotten request made by that person.

The Grand Chamber found the anonymisation order to be justified and, therefore, not in violation of the applicant's right to freedom of expression. It was the factual difference between this case and the one discussed above – especially, the difference in the public interest value of the respective publications and the respective profiles of the persons seeking the anonymisation – that ultimately accounted for a different balancing outcome. However, the Court also formulated additional balancing criteria, creating a test specific to the right to be forgotten.

As the Court was at pains to emphasise, the article was originally published in a lawful and non-defamatory manner, and the case concerned solely its continued availability of the information on the internet (see para. 134). Having stressed the “secondary but nonetheless valuable role” of the press in maintaining publicly available news archives (para 140), the Court declared the integrity of digital press archives to be “the guiding principle underlying the examination of any request for the removal or alteration of all or part of an archived article which contributes to the preservation of memory, especially if, as in the present case, the lawfulness of the article has never been called into question” (para. 145).

It is not clear, however, if this recognition of the importance of digital press archives had any meaningful effect on the actual balancing conducted by the Court and, particularly, on its examination of less restrictive alternatives such as de-indexing.

The balancing test included the following points:

(i) The nature of the archived information:

The inclusion of a person's full name in a press report on criminal proceedings against them did not, as such, raise an issue under the Convention, even though that information fell within the personal sphere protected by Article 8 (para. 216). The Court was satisfied that the article under consideration reported the accident accurately, succinctly, and objectively (para 219). At the same time, the reported events did not belong to “the category of offences whose significance, owing to their seriousness, is unaltered by the passage of time”; nor did they attract widespread publicity at the time or at a later point (para 219).

(ii) The time passed since the events and their initial reporting:

The Court began with a somewhat tautological observation that “the relevance of information is often closely linked to its topicality” (para. 220). Here, however, the Court's actual focus was not on the lasting relevance of the article's contents (this aspect was examined under the next criterion). Instead, the Court turned to the interests of the person requesting the anonymisation: “the passage of a significant length of time has an impact on the question whether a person should have a ‘right to be forgotten’” (ibid).

Given that sixteen years had passed between the initial publication and the anonymisation request, the Court concluded that the person in question (who had been rehabilitated in the meantime) “had a legitimate interest, after all that time, in seeking to be allowed to reintegrate into society without being permanently reminded of his past” (para. 221).

(iii) The contemporary interest of the information

The question here was whether, at the time of the submission of the anonymisation request, the article continued contributing to a debate of public interest or presented “any historical, research-related or statistical interest” (para. 222). While the existence of contemporary public interest in the information included in the article would have left “little scope” for exercising the right to be forgotten (para. 223), its absence was not necessarily decisive as long as the information could still be of interest for historical or scientific purposes (para. 224). The Court found that none of those elements were present in this case. It sided with the domestic courts’ conclusion that: (a) the article “merely made a statistical contribution to a public debate on road safety”, (b) the identity of the person responsible for the accident did not add to the article’s public interest as he was not a public figure, and (c) the reported events were “unexceptional” and “clearly not of historical significance” (see para. 224).

This approach is not easily reconciled with the importance of press archives the Court recognised earlier in the judgment. The dissenting opinion offered a compelling rebuttal to the majority’s position:

Taking into account the characteristic role of press archives, which is to preserve information, the effects of the passage of time should not be accorded too much weight in determining whether an article in the archives may be altered. Information published about a past event, which is initially relevant only as recent news concerning a person not in the public eye, may subsequently become more relevant if the person concerned comes to the forefront of public attention. Furthermore, archived information may have acquired historical, research-related or statistical interest or continue to have value for the purposes of placing recent events in context ...” (para. 11).

(iv) The public profile of the person requesting the anonymisation:

The person in question was unknown to the public either at the time of the reported events or at the time of his request, and the case did not attract widespread publicity at any point (para 229).

(v) The personal impact of the continuing availability of the information online:

As a general rule, “an attack on a person’s reputation must attain a certain level of seriousness and be made in a manner causing prejudice to personal enjoyment of the right to respect for private life” (para 231). In contrast to delisting requests addressed to search engines, the existence of “serious harm” was required for anonymisation requests that directly interfere with archived content (see para 232). In the case of a publication containing judicial information, the mere fact the person seeking anonymisation has been rehabilitated is not sufficient to justify their claim (para 233).

The Court agreed with the Belgian court’s conclusion that the information about his criminal conviction was “readily accessible to a wide audience which – since [the anonymisation requestor] was a doctor – inevitably included patients, colleagues and

acquaintances, and was thus liable to stigmatise him, seriously damage his reputation and prevent him from reintegrating into society normally” (paras. 234-235).

(vi) The degree of accessibility of the archived article:

The Court observed that an article stored in a digital archive was not likely to attract the attention of internet users who were not looking for information about a specific person (para 237). Nonetheless, the decisive consideration was whether access to an archived article was unrestricted or limited to subscribers or in some other way (para 238). In this case, public access to the digital archive was free of charge and unrestricted (para. 239).

(vii) The impact of anonymisation on freedom of expression/ freedom of the press:

The Court started by outlining various measures that have been developed in national jurisdictions to implement the right to be forgotten (see para. 241). Some are aimed at search engines (adjustments to how search results are presented; complete or partial delisting for searches based on the name of the person concerned). Others are aimed directly at website publishers and so, presumably, amount to a more serious restriction on freedom of expression (having the article de-indexed by search engines or de-indexing it on the publisher’s own website; adding a note to the original text; anonymising; removing all or part of the text from the digital archive).

The Court then went on to introduce a specific proportionality test that national courts are required to apply when examining the appropriateness of a specific measure: national courts “must give preference to the measure that is both best suited to the aim pursued by [the requesting person] – assuming that aim to be justified – and least restrictive of the press freedom which may be relied on by the publisher concerned” (para. 242).

It is important to note that the Court limited the requirement to consider less restrictive solutions to considering only measures aimed at the publisher and not those aimed at search engines, signalling this limited approach earlier in the judgment, when it stated that “the examination of an action against the publisher of a news website cannot be made contingent on a prior request for delisting” (para. 168). As a result, the Court confined itself to comparing anonymisation (“a particular means of altering archived material in that it concerns only the first name and surname of the person concerned”) to more radical interferences with the original content, such as the removal of an entire article (para. 249). As an additional justification for the choice of anonymisation, the Court referred to the fact that the original non-anonymised version of the article would still be available in print form and could be consulted by any interested person, thereby “fulfilling its inherent role as an archive record” (para. 252).

The Court’s refusal to consider delisting as a less restrictive solution contradicted its own acknowledgment that “G.’s chief concern was the fact that the article was displayed following Internet searches based on his first name and surname carried out via search engines” (para. 244). Nor does it sit well with the Court’s declaration that the integrity of digital press archives should its guiding principle. Unsurprisingly, the majority’s failure to consider delisting as a less restrictive measure that would serve the requesting person’s aims was one of the main criticisms Judge Ranzoni levelled against the judgment in his

dissenting opinion, joined by four other judges (see paras. 21-26 of the dissenting opinion).

The Court's position on the chilling effect of anonymisation is also vulnerable to criticism. Rather than considering the potential long-term effect on the media in general, it limited itself to addressing the more immediate impact of the anonymisation order on the applicant's newspaper only. In this regard, the Court noted that "in the circumstances of the present case, it [did] not appear from the file that the anonymisation order had [had] such a profound impact on the performance by the newspaper *Le Soir* of its journalistic tasks as to impair that performance in practice" (para 254). The dissenting opinion compellingly criticised the majority for its failure to address this vital question in a meaningful way, noting that "an obligation to review at a later stage the lawfulness of keeping an article online following [a right to be forgotten request] entails the risk, *inter alia*, that the press may refrain in future from keeping reports in its online archives or that it will omit individualised elements in articles that are likely to be the subject of such a request at a later stage" (para 27).

3. CONCLUSION

Establishing the limits of data protection vis-à-vis freedom of expression remains to be a work in progress for lawmakers and courts. This module has provided some insights into the complexity inherent in the task.

Europe has developed two parallel but interdependent and mutually enriching data protection regimes: within the EU and in the framework of the Council of Europe. The GDPR is at the centre of the EU regime, and its influence has spread far beyond the EU borders. The right to be forgotten, endorsed by the CJEU and later entrenched in Article 17 of the GDPR, is among the elements of the EU data protection law that have a particularly profound effect on the freedom of the media.

The EU has been an undisputed world leader in developing regulatory responses to the new threats digital technologies pose to the right to privacy. However, their impact on freedom of the media is a serious concern. The ECtHR has tested some of those responses, and its approach to balancing the right to be forgotten against freedom of expression has become more sophisticated and nuanced. Yet, one may question if the chilling effect of measures such as retroactive anonymisation is fully appreciated by the Court.

Module 3

**Content
Based
Restrictions
and
Intermediary
Liability**

*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	1
2. EU APPROACH TO INTERMEDIARY LIABILITY	1
2.1. The ECD Approach	2
2.2. The DSA Regime	3
2.3. Providers of Intermediary Liability	4
3. ECTHR APPROACH TO INTERMEDIARY LIABILITY.....	7
4. CONCLUSION.....	14

MODULE 3

1. INTRODUCTION

Content based restrictions¹ can be imposed on the basis they are required to tackle harms arising from user-generated content, or because they interfere with a countervailing right to that of freedom of expression, such as the right to reputation.² The nature of these restrictions can vary in form, from take down notices issued for online content, to imposing certain duties on intermediaries. This module aims to look at the different methods of applying those restrictions, with a focus on relevant precedents from the European Court of Human Rights ('ECtHR'), and the Court of Justice of the European Union ('CJEU').

There have been developments on content restriction at the EU level recently. The E-Commerce Directive³ (the ECD) had previously provided exemptions to intermediary services from civil and other liabilities if they met certain conditions. Now, the Digital Services Act (the DSA) provides those exemptions. At the Council of Europe level, the main developments have been at the ECtHR, which has, in recent years, published a number of important, and controversial, decisions on content moderation, as it seeks to balance the right to privacy or other countervailing rights, with the right to freedom of expression.

This module will consider those decisions as well as other developments in the area of intermediary liability.

2. EU APPROACH TO INTERMEDIARY LIABILITY

The DSA is the EU's effort at combatting unlawful speech on the Internet. Political agreement on the DSA was reached in April 2022 between the European Parliament and EU Member States. It entered into force in November 2022, but application of the provisions only began in February 2024.⁴ The DSA contains a common set of rules on responsibilities and accountability for providers of intermediary services and online platforms. It also aims to harmonise the legal frameworks in member states and provide protection to all Internet service users by setting out notice-and-action procedures for illegal content, and the possibility to challenge platform content moderation decisions.⁵

The DSA is applicable to 'intermediary services offered to recipients of the service that have their place of establishment or are located in the Union, irrespective of where the providers of those intermediary services have their place of establishment.' (The scope of application of the legislation is intermediary services consisting of services known as 'mere conduit',

¹ Global Network Initiative, *Intermediary Liability & Content Regulation*, (accessible [here](#)).

² *Ibid.*

³ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (accessible [here](#)).

⁴ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act).

⁵ Chapter III Section 4 of the DSA.

'caching' and 'hosting' services.⁶ This means that the DSA is not applicable to individuals that for example run a blog or discussion forum or allow discussions on their Facebook account or other platforms that create content or that are set up for the purpose of publishing user-generated content.⁷ However, this regulation is important for platform administrators because where they fail to remove content alleged to be unlawful, a request for removal of that content can be made to the service provider of that platform.

2.1. The ECD Approach

The transnational nature of the Internet and the publication of content can cause problems, as speech is published in one state from servers in another state. This was an issue in the well-known case of *Glawischnig-Piesczek v Facebook Ireland Limited*.⁸ The claimant was a prominent politician. The defendant, Facebook Ireland Ltd., was described as the operator of a global social media platform for users located outside the USA and Canada.⁹

In April 2016, an anonymous Facebook user shared an article from the Austrian online news magazine oe24.at titled 'Greens: Minimum income for refugees should stay' and published a comment calling Glawischnig-Piesczek "miese Volksverräterin" (lousy traitor), "korrupten Trampel" (corrupt bumpkin) and her party a "Faschistenpartei" (fascist party). This generated a thumbnail on Facebook containing the title of the article, and a photograph of Glawischnig-Piesczek. Both the post and comment could be accessed by any Facebook user. On 7 July 2016, Glawischnig-Piesczek asked Facebook to delete the posts and to reveal the user's identity. After Facebook neither deleted the posts nor revealed the user's identity, Glawischnig-Piesczek applied for an injunction. She argued that her right to control the use of her own image under the Austrian Law on the protection of copyright had been violated. She further claimed that the defamatory comment, which was posted together with the picture, constituted an infringement of the Austrian Civil Code, which protects people from hate speech.

Facebook Ireland Ltd. argued that it was governed by Californian law (site of its headquarters) or Irish law (European base) but not Austrian law. Secondly, it referred to its host-provider privileges under the ECD which excludes host-providers from liability for their users' content. Facebook also alleged that the impugned comments were protected under the right to freedom of expression under Article 10 ECHR.

The Austrian court ordered Facebook to 'cease and desist from publishing' the photograph if the accompanying text 'contained the assertions, verbatim and/or using words having an equivalent meaning' to the defamatory comment. Facebook Ireland disabled access to the said content in Austria. On appeal, the court upheld the order 'as regards the identical allegations' but held that the 'dissemination of allegations of equivalent content had to cease only as regards those brought to the knowledge of Facebook Ireland by the applicant or by

⁶ DSA (Article 1(2), 2(1-2) and Article 3((g)(i-iii)).

⁷ According to DSA 2(2) it is not applicable 'to any service that is not an intermediary service or to any requirements imposed in respect of such a service, irrespective of whether the service is provided through the use of an intermediary service, irrespective of whether the service is provided through the use of an intermediary service.'

⁸ C-18/18 *Glawischnig-Piesczek v Facebook Ireland Limited* [2016] ECLI:EU:C:2019:821.

⁹ *Ibid.*, §11.

third parties'.¹⁰ The Courts agreed that the defamatory comments implied she was engaged in illegal activities without providing any evidence and therefore, were harmful to Glawischnig-Piesczek's reputation. Both parties appealed this judgment to the Supreme Court. It referred to the CJEU the questions of

- 1) whether, under Article 15 of the Directive, an injunction against a hosting provider could extend to statements that are identically worded and/or have equivalent content; and
- 2) if such an injunction could apply worldwide.

The CJEU found that the ECD does not preclude a Member State from ordering a hosting provider to remove or block content that has been declared unlawful, or content that is identical or equivalent to such unlawful information. The Court also held that the Directive does not preclude Member states from ordering such removal worldwide, and therefore left it to the Member States to determine the geographic scope of the restriction within the framework of the relevant national and international laws. The Court found that monitoring for identical content to that which was declared illegal, would fall within the allowance for monitoring in a "specific case" and thus not violate the Directive's general monitoring prohibition. This allowance could also extend to equivalent content providing the host was not required to "carry out an independent assessment of that content" and employed automated search tools for the "elements specified in the injunction."

The judgment has **major implications for online freedom of expression around the world**. The judgment means that Facebook would have to use automated filters to identify social media posts that are 'identical content' or 'equivalent content'. Technology is used to identify and delete content that is considered illegal in most countries, for example, child abuse images. However, this ruling could see filters being used to search text posts for defamatory content, which is more problematic given that the meaning of text could change depending on the context. Compelling social media platforms like Facebook to automatically remove posts regardless of their context infringes free speech rights and restricts access to online information. One of the main concerns with the judgment was that it did not appreciate the limitations of technology when it comes to automated filters.

A further concern was that the judgment meant that a court in one EU member state could order the removal of social media posts in other states, even if they are not considered unlawful there. This would set a dangerous precedent where the courts of one country can control what Internet users in another country can see. This would allow for abuse, particularly by regimes with weak human rights records.

2.2. The DSA Regime

The case of Glawischnig-Piesczek v Facebook Ireland Limited was decided pursuant to the ECD. The DSA will continue to apply the hosting, caching, and mere conduit defences that first appeared in the ECD.

This includes prohibiting general monitoring obligations from being imposed on intermediary service providers and preserving the existing 'notice and takedown' process – where a hosting

¹⁰ *Ibid.*, §16

provider will only become liable for illegal content if they have actual knowledge of the unlawfulness and fail to remove or disable access to the content expeditiously.¹¹

Under the DSA a clearer line is drawn between the liability of online platforms and their liability under consumer law. Online platforms, such as marketplaces, will remain liable under consumer law when they lead an ‘average consumer’ to believe that the information, or the product or service that is the object of the transaction, is provided either by themselves or by a recipient of the service who is acting under their authority or control.¹² This will be the case, for example, where an online platform withholds the identity or contact details of a seller until after the conclusion of the contract between that seller and the consumer, or where an online platform markets the product or service in its own name rather than in the name of the seller who will supply that product or service.¹³

The meaning of ‘average consumer’ was considered by Advocate General Szpunar in the *Louboutin* case.¹⁴ The Advocate General’s opinion suggests that the marketplace will be liable where a ‘reasonably well-informed and reasonably observant internet user’ perceives the offer of the seller as an integral part of the commercial offer of the marketplace.¹⁵

Where an intermediary service provider automatically indexes information uploaded to its service, has a search function, or recommends information based on the preferences of the users, it will not be a sufficient ground for considering that provider to have specific knowledge of illegal activities carried out on that platform or of illegal content stored on it.¹⁶

Maintaining the hosting defence and other intermediary protections is positive but online platforms will now be subject to significant new obligations under the DSA.

2.3. Providers of Intermediary Liability

All intermediary service providers (including those only providing mere conduit and caching services) must comply with the following requirements:

- Reflecting the fact that some service providers can be difficult to identify and contact, they must provide a public ‘point of contact’ so they can be contacted by other authorities and users.
- If a service provider is based outside the EU (but offers services in the EU) it must appoint a legal representative in the EU. This sounds similar to the EU representative concept in the General Data Protection Regulation (GDPR).¹⁷ However, there is no exemption for small companies.^[16] In addition, under the DSA, that representative can be held *directly liable* for breaches. Given the potentially punitive sanctions (section 6 below), this is not a role to be undertaken lightly. It is not clear if there will be a ready (or cheap) pool of people willing to take

¹¹ Art. 6(1), DSA.

¹² Art. 6(3), DSA.

¹³ Recital 24, DSA.

¹⁴ Opinion of Advocate General Maciej Szpunar (2 June 2022), *Christian Louboutin v. Amazon*, Joined Cases C-148/21 and C-184/21, ECLI:EU:C:2022:422, paras 65-72.

¹⁵ *Ibid.*, §101.

¹⁶ Recital 22, DSA.

¹⁷ Art. 27(2), GDPR.

on this role, a matter which is highly problematic given the very large number of intermediary service providers subject to this obligation.

- The ISP must set out in their terms and conditions any restrictions on the service, alongside details such as content moderation measures and algorithmic decision making.
- The ISP must issue an annual transparency report on matters such as content moderation measures and the number of take down and disclosure orders received.
- Service providers that receive take down or information disclosure orders from judicial or administrative authorities in the EU must notify the authority of any action taken.

Hosting services are a subset of intermediary services consisting of the storage of information provided by or at the request of a user, such as cloud service providers, online marketplaces, social media, and mobile application stores.

In addition to the above, hosting providers are subject to **additional obligations**:

1. Anyone should be able to notify the hosting provider of illegal content (not just judicial or administrative authorities). The hosting provider must process that notice diligently and report back on whether the content was removed.
2. Hosting providers must notify users if they remove content. This also includes demoting or restricting the visibility of the content and the notification should include details of whether the decision was taken using automatic means (e.g. based on machine learning classifications).
3. Hosting providers must inform the judicial authorities if the hosted content creates a suspicion that a criminal offence has occurred, limited to offences involving a threat to life or safety.

New provisions in the DSA applies to online platforms such as social media services and online marketplaces. Any attempt to regulate user-provided content is fraught with difficulties and raises difficult questions about the balance between fundamental rights to freedom of information, the impact of online harms and the practical limitations attempting to moderate content at scale.

The DSA takes a generally back seat role. Except for large platforms there are limited obligations to oversee content on the platform. Instead, the new regime appears to have more of a bias to protect content by giving users a right to complain against the removal of content, and even use an out-of-court appeals process if they are unhappy with the platform's handing of that complaint. This is a significant change for many platforms who will have to be much more transparent about their moderation processes and may need significant additional resources to deal with subsequent objections and appeals from users.

Alongside these changes are other significant developments, including:

- Platform providers cannot use interfaces that manipulate or distort the choices taken by users – in addition to those forms of manipulative practices that are already set out in the Unfair Commercial Practices Directive¹⁸ and the GDPR.¹⁹
- *Suspension of repeat offenders*: Where a user continues, after being warned, to ‘frequently’ provide unlawful content, the platform provider must suspend them for a reasonable time.
- *Disclosure of monthly active users*: The platform provider must disclose the number of monthly active users in the EU.
- *Advertising and recommender system transparency*: Online platforms shall not present advertising to users based on profiling with special category data. The platform provider must provide users with information about advertisements they are shown including the reasons why that advertisement was selected for them. Where an advertisement is based on profiling, the platform provider must also inform the user about any means available for them to change such criteria. Similarly, the platform provider must be transparent about the operation of any recommender system.
- *Seller verification*: The platform provider needs to ensure seller on the platform identify themselves and make best efforts to verify certain traceability information before allowing them to use their platforms.
- *Online protection of minors*: Providers of online platforms accessible to minors shall put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors.

The highest tier of regulation applies to:

1. Very large online platforms (VLOP): These are very large online platforms which have over forty-five million monthly active users in the EU, a number equivalent to 10% of the EU population, and are designated as such by the Commission.
2. Very large online search engines (VLOSE): These are online search engines which have over forty-five million monthly active users in the EU and are designated as such by the Commission.

This designation brings with it some of the very strongest obligations in the DSA, considering the overall influence of such platforms. This includes obligations to conduct a risk assessment of their services and to take steps to mitigate any risks identified as part of that process.

Also, the DSA operates by putting in a baseline ‘notice and takedown’ system. Hosting providers (including online platforms) must allow third parties to notify it of any illegal content it is hosting. Once notified, the hosting provider will need to remove that content expeditiously to continue to benefit from the hosting defence. Added to that, online platform providers must

¹⁸ Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (Unfair Commercial Practices Directive).

¹⁹ European Data Protection Board, *Guidelines 3/2022 on Dark patterns in Social Media Platform Interfaces: How to Recognize and Avoid Them* (adopted on 14 Mar. 2022).

provide an expedited removal process for notifications from trusted flaggers, suspend users who frequently post illegal content and provide additional protection to minors.

Alongside these protections, VLOP and VLOSE have specific obligations to assess and mitigate 'systemic risks' arising from their services. That assessment must include the risks of or to:

1. *Illegal content*: This encompasses a wide range of harmful material including hate speech.
2. *Fundamental rights*: This applies where content would impact on the exercise of fundamental rights, such as freedom of expression, privacy, the right to non-discrimination and consumer protection. Importantly, this does not just mean removing content but also actively supporting free speech by taking measures to counter the submission of abusive take down notices.
3. *Democracy*: This encompasses negative effects on the democratic process, civic discourse, and electoral processes, as well as public security.

Finally, this framework will provide extra protection for recognised media sources through the proposed Regulation establishing a common framework for media services (European Media Freedom Act).²⁰ This requires VLOP to allow recognised media sources to declare their status and imposes additional transparency and consultation obligations on VLOP in relation to the restriction or suspension of content from those sources.

3. ECTHR APPROACH TO INTERMEDIARY LIABILITY

Article 10(2) of the European Convention on Human Rights (the 'Convention') provides that restrictions may be prescribed by law and necessary in the interest of "national security, territorial integrity, or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence or for maintaining the authority and impartiality of the judiciary."²¹

Inevitably the growth of the Internet and online communication platforms in recent years has had a profound effect on the interpretation of an individual's right to freedom of expression. Content published online, including user-generated allegedly defamatory comments, are accessible globally with the harm extending across states, often resulting in complex international legal disputes.²² In the case of *Delfi v Estonia*, the ECtHR commented that "defamatory and other types of clearly unlawful speech, including hate speech and speech inciting violence, can be disseminated like never before, worldwide, in a matter of seconds, and sometimes remain persistently available online".²³

²⁰ Regulation of the European Parliament and of the Council establishing a common framework for media services in the internal market (European Media Freedom Act) and amending Directive 2010/13/EU (2022/0277 (COD)).

²¹ Article 10(2) ECHR

²² Council of Europe study, *Liability and jurisdictional issues in online defamation cases*, (2019) – p. 6

²³ ECtHR, *Delfi AS v Estonia* [GC], App. No 64569/09, 16 June 2015 §110

The ECtHR considered intermediary liability for the first time in 2015, in *Delfi*. The principles that were developed in *Delfi* for determining intermediary liability were subsequently applied in the case of *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v Hungary*. In both of those cases the applicants were Internet news portals, the second applicant in MTE being a self-regulatory body of Internet content providers.

In *Delfi*, the Grand Chamber considered the following factors as being relevant in the finding that the applicant was liable for third party comments on its website:

- (i) the commercial nature of *Delfi*, and that it was one of the biggest media companies in Estonia with a wide readership.
- (ii) that it encouraged posting of comments, and that this encouragement formed part of its business model as engagement of readers would contribute to its overall revenue.
- (iii) that it had editorial control over comments once they had been posted
- (iv) that it was a “professional publisher” that should be familiar with the relevant laws and could also have sought legal advice.

The Grand Chamber identified four elements that required analysis when determining liability for third party comments:

- (i) the context of the comments.
- (ii) the measures applied by the applicant company to prevent or remove defamatory comments.
- (iii) the liability of the actual authors of the comments as an alternative to the intermediary’s liability; and
- (iv) the consequences of the domestic proceedings for the applicant company.

The Grand Chamber was **first** concerned with “the ‘duties and responsibilities’ of Internet news portals ... when they provide for economic purposes a platform for user-generated comments” and it expressly disappplied its findings to “other fora on the Internet where third-party comments can be disseminated, for example an Internet discussion forum or a bulletin board where users can freely set out their ideas on any topics without the discussion being channelled by any input from the forum’s manager; or a social media platform where the platform provider does not offer any content and where the content provider may be a private person running the website or a blog as a hobby”.²⁴ This differentiation between news portals and members of the public who use a social media account is stated clearly, and in unqualified terms. The President of the Court has explained that this distinction is made not on the basis “that economic operators exercising free speech rights should, because of that status, enjoy lower free speech protections as a matter of principle, but only that the economic nature of their activities may often justify imposing on them duties and responsibilities which are of a more stringent nature than can be made applicable to non-profit entities”.²⁵ The Grand Chamber’s clarification on this point alone would seem to exclude a user of a social media account from liability for failing to monitor and remove third party comments.

²⁴ ECtHR, *Delfi AS v Estonia* [GC], App No. 64569/09, 16 June 2015, §§115 – 116.

²⁵ Judge Spano, *Don’t Kill the Messenger – Delfi and Its Progeny in the Case Law of the European Court of Human Rights*, University of Tallinn Friday, (8 September 2017), (accessible [here](#)).

Second, the Grand Chamber placed particular weight on whether the identity of the authors of the third party comments could be established.²⁶ It started out by asking whether “the liability of the actual authors of the comments could serve as a sensible alternative to the liability of the Internet news portal”.²⁷

In noting that the parties disagreed as to the ‘feasibility’ of establishing the identity of the authors,²⁸ the Grand Chamber then held that the “uncertain effectiveness of measures allowing the identity of the authors of the comments to be established, coupled with the lack of instruments put in place by the applicant company for the same purpose with a view to making it possible for a victim of hate speech to bring a claim effectively against the authors of the comments” were relevant factors supporting its finding of no violation of Article 10.²⁹

The Grand Chamber’s judgment implicitly recognised that where the authors of impugned third party comments are known or can be readily identified, and therefore can be subject to legal action, taking legal action against the intermediary, especially where that intermediary is a social media user, can amount to an unduly disproportionate interference with their right to freedom of expression, in violation of Article 10. This principled approach is consistent with the Court’s well established case law on the important role of the Internet in facilitating the dissemination of information.³⁰

Third, it was an important part of the government’s case in *Delfi* that the third party commenters had “lost control of their comments as soon as they had entered them and they could not change or delete them”.³¹ The Court agreed that this detail was a factor in determining liability, stating that because *Delfi* “exercised a substantial degree of control over the comments published on its portal, the Court does not consider that the imposition on the applicant company of an obligation to remove from its website, without delay after publication, comments that amounted to hate speech and incitements to violence, and were thus clearly unlawful on their face, amounted, in principle, to a disproportionate interference with its freedom of expression”.³² This can be contrasted with comments made on social media platforms such as Facebook, where a commenter can still exercise control by withdrawing a comment after it has been posted, as happened in the present case when one of the commenters later deleted the allegedly unlawful online speech.³³

In *MTE*, the Court applied the principles developed in *Delfi* to determine liability for third party comments, carrying out a close analysis of the four elements outlined above.³⁴ In that case the Court found a violation of Article 10. The key difference between *MTE* and *Delfi* lay in the

²⁶ ECtHR, *Delfi AS v Estonia* [GC], App No. 64569/09, 16 June 2015, §77.

²⁷ *Ibid.*, §147.

²⁸ *Ibid.*, §150 “As regards the establishment of the identity of the authors of the comments in civil proceedings, the Court notes that the parties’ positions differed as to its feasibility”.

²⁹ *Ibid.*, §151.

³⁰ See ECtHR, *Jersild v Denmark*, App No. 15890/89, 23 September 1994, §35; ECtHR, *Thoma v Luxembourg*, App No. 38432/97, 29 March 2001, §62; and, mutatis mutandis, ECtHR, *Verlagsgruppe News GmbH v Austria*, App No. 76918/01, 14 December 2006, §31; ECtHR, *Print Zeitungsverlag GmbH v Austria*, App No. 26547/07, 10 October 2013, §39.

³¹ *Ibid.*, §85

³² *Ibid.*, §153

³³ See ECtHR, *Sanchez v France*, App No. 45581/15, 2 September 2021, §11

³⁴ ECtHR, *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v Hungary*, App No. 22947/13, 2 February 2016, §§60 – 88.

nature of the third-party comments in issue.³⁵ The Court in *MTE* noted that, unlike in *Delfi*, the comments did not amount to hate speech or incitement to violence. The domestic courts had held the applicants, a news portal and a self-regulatory body of Internet content providers, liable for the harm to the reputation of a business by ‘false and offensive’ statements by online users, noting that they should have expected that some ‘unfiltered comments’ might be in breach of the law. In finding a violation of Article 10, the Court held that a requirement that an online platform search for and take down unlawful user comments “amounts to requiring excessive and impracticable forethought capable of undermining freedom of the right to impart information on the Internet”.³⁶ In *Pihl v. Sweden* the Court referenced *MTE* in noting that it had “previously found that liability for third party comments may have negative consequences on the comment-related environment of an internet portal and thus a chilling effect on freedom of expression via internet. This effect could be particularly detrimental for a non-commercial website.”³⁷

The Court’s findings in both *Delfi* and *MTE* hold that where an intermediary fails to remove material that is “clearly unlawful”, it may be held liable for that failure.³⁸ The implication here is that the intermediary is required to determine the lawfulness or otherwise of the online content. The Grand Chamber in *Delfi* held that the intermediary must act “without delay” to remove unlawful speech.³⁹ However, this is a very high standard as even the most sophisticated intermediary would find it difficult to carry out an assessment as to whether a comment qualifies as unlawful speech to an appropriate legal standard, and in any event would feel compelled to remove that comment almost immediately to avoid liability.⁴⁰ This clearly creates a ‘chilling effect’.

Assessing whether material posted online is lawful or unlawful is complex and would amount to an excessively burdensome standard where applied, for example, to the user of a social media platform acting as an intermediary.⁴¹ It can involve an examination of the appropriate balance to be struck between the right to respect for private life and the right to freedom of expression. It might involve questions relating to defamation, privacy rights, or breach of data protection, and their relationship to the criminal law. A proper assessment of lawfulness might require consideration of whether certain legal defences are available. A further level of complexity stems from the fact that states within the Council of Europe classify certain offences differently, for example, where defamation is an offence under criminal law.⁴² Where intermediaries do remove content without properly assessing its lawfulness, they are likely to

³⁵ *Ibid.*, See Concurring Opinion of Judge Kuris §2

³⁶ ECtHR, *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v Hungary*, App No. 22947/13, 2 February 2016, §82

³⁷ ECtHR, *Pihl v Sweden*, App No. 74742/14, 7 February 2017, §35

³⁸ ECtHR, *Delfi v. Estonia* [GC], App No. 64569/09, 16 June 2015, §153; ECtHR, *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v Hungary*, App No. 22947/13, 2 February 2016, §§64 and 91.

³⁹ ECtHR, *Delfi v. Estonia* [GC], App No. 64569/09, 16 June 2015, §159

⁴⁰ See for example: ECtHR, *I.A. v. Turkey*, App No. 42571/98, 13 September 2005; ECtHR, *Lindon, Otchakovsky-Laurens and July v. France* [GC], App Nos. 21279/02 and 36448/02, 22 October 2007

⁴¹ According to the Council of Europe Committee of Ministers, “questions about whether certain material is illegal are often complicated and best dealt with by the courts”. See Committee of Ministers of the Council of Europe, Declaration on freedom of communication on the Internet, Adopted on 28 May 2003 at the 840th meeting of the Ministers’ Deputies p.7

⁴² See for example: Council of Europe, European Commission for Democracy Through Law (Venice Commission) – Opinion on the Legislation on Defamation, Opinion No. 715/2013, (9 December 2013)

do so without informing the author and where the author has no prospect of appealing the decision to remove their content. Ultimately, a requirement that intermediaries should determine whether online material is unlawful will invariably lead to lawful content being removed. Moderation is already a challenge for social media companies who are best placed to apply resources to this issue. For example, Facebook has admitted that their moderators “make the wrong call in more than one out of every 10 cases”.

These issues arose most recently in *Sanchez v. France*.⁴³ The applicant is a politician for the National Rally (a far-right party in France). While running for election to Parliament for the party in the Nîmes constituency, he posted a message about one of his political opponents, F.P., on his publicly accessible Facebook wall which he ran. The post itself was not inflammatory and only his friends could comment on it. Two third parties, S.B. and L.R, added a number of comments under his post, referring to F.P.’s partner Leila T. and expressing dismay at the presence of Muslims in Nîmes. Leila T. confronted S.B. who she knew, and he deleted his comment later that day.

The next day, Leila T. lodged a criminal complaint against the applicant as well as those who wrote the offending comments. The Nîmes Criminal Court found them all guilty of incitement to hatred or violence against a group or an individual on account of their origin/belonging or not belonging to a specific ethnic group, nation, race, or religion. The Nîmes Court concluded that by creating a public Facebook page Mr. Sanchez had set up a service for communication with the public by electronic means on his own initiative, for the purpose of exchanging opinions. By leaving the offending comments visible on his wall, he had failed to act promptly to stop their dissemination and was guilty as the principal offender. In its decision, the Nîmes Criminal Court noted that only ‘friends’ could comment on the applicant’s Facebook wall and that being a political actor, he had to be more thorough in monitoring his comments, as he was more likely to attract polemical content.

This decision was upheld by the Nîmes Court of Appeal which held that the comments had clearly defined a group - Muslims – and associated them with crime and insecurity in the city in a provocative way. The Court of Appeal also noted that by knowingly making his Facebook ‘wall’ public, the applicant had assumed responsibility for the offending content. Mr. Sanchez’ appeal to the Court of Cassation on points of law was rejected. He then went to the ECtHR, alleging that his criminal conviction for incitement to hatred violated Article 10.

The Chamber majority found that no violation had occurred.

The Grand Chamber, in examining whether the interference was necessary in a democratic society, noted that, according to *Feldek v. Slovakia*,⁴⁴ in the case of political speech there is little scope under Article 10 for it to be restricted,⁴⁵ as it is a very important feature of a democratic society, and that the governmental margin of appreciation, in this case, was particularly narrow. However, the Court noted that “the freedom of political debate is not

⁴³ See ECtHR, *Sanchez v France*, App No. 45581/15, 2 September 2021

⁴⁴ ECtHR, *Feldek v. Slovakia*, App No. 29032/95, 12 July 2001

⁴⁵ ECtHR, *Feldek v. Slovakia*, App No. 29032/95, 12 July 2001

absolute in nature,⁴⁶ especially when it comes to the prevention of forms of expression that can promote or propagate hatred or violence.

The Court relied on the case *Erbakan v. Turkey*,⁴⁷ to reiterate the responsibility of politicians in avoiding comments that might foster intolerance when speaking in public. Then, the Court added that Article 10 does not protect declarations that can arouse feelings of rejection or hostility towards a community.⁴⁸

Furthermore, the Court quoted the cases of *Sürek v. Turkey*⁴⁹, *Le Pen v. France, Soulas and Others v. France*,⁵⁰ and *E.S. v. Austria*,⁵¹ to highlight the broader margin of appreciation granted to states to assess the necessity when restricting freedom of expression in cases of remarks made to incite violence against one or many individuals. It also said that hate speech may take various forms: They are not always plainly aggressive remarks but can include implicit statements that can be equally hateful as determined in *Jersild v. Denmark*,⁵² *Le Pen*,⁵³ *Soulas, Ayoub and Others v. France*,⁵⁴ and *Smajić v. Bosnia and Herzegovina*.⁵⁵

Subsequently, the Court analysed the impact of hateful or discriminatory comments made on the internet and social media. It noted the many harmful risks that this content on the internet posed, and how hate speech can be rapidly disseminated. In order to strike a balance between the rights conferred by Article 10 and the harmful effects that hate speech on social media might have on the rights conferred by Article 8, the Court agreed on the possibility of imposing liability for defamatory speech as an effective remedy. In the case of liability for third-party comments on the Internet, “the nature of the comment will have to be taken into consideration, in order to ascertain whether it amounted to hate speech or incitement to violence, together with the steps that were taken after a request for its removal by the person targeted in the impugned remarks.”⁵⁶ The Court referred to the cases of *Pihl v. Sweden*⁵⁷ *Magyar Kétfarkú Kutya Párt v. Hungary*,⁵⁸ and *Index.hu Zrt v. Hungary*.⁵⁹

In order to analyse the necessity of the interference of the French government in the present case, the Court started by examining the context of the comments at issue. Given that the comments were directed to a specific group (i.e., Muslims) in an electoral context in a politician’s Facebook “wall”, the Court found that the comments were clearly unlawful. The Court stated that liability should be shared—in different degrees—between all the actors involved, including Mr Sanchez—even if the comments were posted by third parties. Otherwise, exempting producers from all liability “might facilitate or encourage abuse and

⁴⁶ ECtHR, *Sanchez v France* [GC], App No. 45581/15, 15 May 2023, §148

⁴⁷ ECtHR, *Erbakan v. Turkey*, App No. 59405/00, 6 July 2006

⁴⁸ ECtHR, *Le Pen v. France* (dec.), App No. 45416/16, 28 February 2017

⁴⁹ ECtHR, *Sürek v. Turkey* (no. 1) [GC], App No. 26682/95, 8 July 1999

⁵⁰ ECtHR, *Soulas and Others v. France*, App No. 15948/03, 10 July 2008

⁵¹ ECtHR, *E.S. v. Austria*, App No. 38450/12, 25 October 2018

⁵² ECtHR, *Jersild v. Denmark*, App No. 15890/89, 23 September 1994,

⁵³ ECtHR, *Le Pen v. France* (dec.), App No. 45416/16, 28 February 2017

⁵⁴ ECtHR, *Soulas and Others v. France*, App No. 15948/03, 10 July 2008

⁵⁵ ECtHR, *Smajić v. Bosnia and Herzegovina* (dec.), App No. 48657/16, 16 January 2018.

⁵⁶ ECtHR, *Sanchez v France* [GC], App No. 45581/15, 15 May 2023, §166

⁵⁷ ECtHR, *Pihl v. Sweden* (dec.), App No. 74742/14, 7 February 2017

⁵⁸ ECtHR, *Magyar Kétfarkú Kutya Párt v. Hungary* [GC], App No. 201/17, 20 January 2020

⁵⁹ ECtHR, *Index.hu Zrt v. Hungary*. App No. 22947/13, 2 February 2016.

misuse, including hate speech and calls to violence, but also manipulation, lies and disinformation.”⁶⁰

The Court continued by analysing the steps taken by Mr Sanchez regarding the comments on his Facebook “wall”. It stated that account holders have to act reasonably and cannot claim any impunity in how they use their electronic resources. That obligation, the Court concluded, is higher for politicians, which have to be aware of the fact that they can reach wider audiences, and whose burden of liability is higher than that of a regular citizen. The Court stressed that Mr Sanchez was aware of the controversial comments made on his Facebook “wall”, as he made a post warning his contacts about it, but nevertheless failed to delete the contested comments, or checked their content.

The Court also dismissed the applicant’s submission regarding the unreasonableness of his prosecution instead of the comments’ authors. According to the Court, he failed to show the arbitrariness of section 93-3 of Law no. 82-652 of 29 July 1982, especially as he was not prosecuted instead of the authors, but alongside them in different autonomous legal regimes. Consequently, by thirteen votes to four, the Court found that the French government’s interference was “necessary in a democratic society,”⁶¹ in accordance with Article 10 of the ECHR, as it was based on relevant and sufficient reasons to determine Mr Sanchez liability and his criminal conviction.

Hyperlink Publication

Courts assessing cases concerning intermediary liability have had to consider some interesting questions in recent years. The liability of intermediaries dealing with the publication of a hyperlink was examined by the ECtHR in *Magyar Jeti Zrt v Hungary*.⁶² The domestic courts in Hungary found the applicant, a company, to be liable for defamation after it posted a hyperlink to YouTube video that contained the impugned material.

The ECtHR had to consider whether the posting of a hyperlink amounted to distributing defamatory statements. In its assessment, the Court noted that domestic court had failed to examine various important factors including (i) whether the applicant company had endorsed the alleged defamatory material; (ii) whether the applicant company had repeated the material, without endorsing it; (iii) whether the applicant company had just posted the hyperlink without commenting on it; (iv) whether the applicant company had knowledge that the material it was posting to was or could be unlawful; (v) whether the applicant company had acted in good faith and performed the necessary due diligence required in responsible journalistic practices. Taking all relevant factors into consideration, the Court noted that the view of the domestic law in attributing liability to those hyperlinking to impugned content would have “negative consequences on the flow of information on the Internet, impelling article authors and publishers to refrain together from hyperlinking to material over whose changeable content they have no control. This may have, directly or indirectly, a chilling effect on freedom of expression on the Internet.”⁶³

⁶⁰ ECtHR, *Sanchez v France* [GC], App No. 45581/15, 15 May 2023, §185

⁶¹ ECtHR, *Sanchez v France* [GC], App No. 45581/15, 15 May 2023, §209

⁶² ECtHR, *Magyar Jeti Zrt v Hungary*, App No. 11257/16, 4 December 2018

⁶³ ECtHR, *Magyar Jeti Zrt v Hungary*, App No. 11257/16, 4 December 2018 §83

In the subsequent case of *Kilin v Russia*, the Court had to consider the conviction of the applicant who was prosecuted for public calls to violence through the sharing of third-party content via a social network website. In its assessment, the Court considered that the sharing of material via social media does not necessarily signify a particular attitude or acknowledgment of the user towards the content. The Court further confirmed that the motivations of the applicant in sharing the impugned content was to contribute to public interest debate but noted that on this occasion, the applicant had distorted the context as they had failed to provide any commentary. As such, the content could be “reasonably perceived as stirring up ethnic discord and violence”.⁶⁴ In view of this, the applicant’s prosecution was relevant and could be justified.

4. CONCLUSION

The impact of the Sanchez judgment could be serious for individuals who are prominent on social media, who may find themselves liable for comments made by third parties posted on their online accounts. Those involved in political campaigning and, possibly, day to day political activity, will be required to moderate their social media accounts to avoid criminal sanction for comments made by other people. Based on the ECtHR’s reasoning the same concerns might apply to other high-profile activists. This ties in with a key concern that imposing liability on social media users for third party content would be more likely to expose them to coordinated attack on forums or pages they administer in order to trigger their liability. This judgment makes that prospect more likely. Users might decide instead to prevent any comments being posted on their social media accounts.

⁶⁴ ECtHR, *Guide on Article 10 of the European Convention on Human Rights – Freedom of Expression*, 31 August 2022, p. 112 (accessible [here](#)).

Module 4

**Surveillance
of Journalists,
Searches and
Digital Device
Seizures**

*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	1
2. SURVEILLANCE: BULK DATA INTERCEPTION	1
2.1. What is bulk data interception?	1
2.2. International legal standards	2
2.3. Regional standards: EU	3
2.4. Regional standards: CoE	4
2.5. Litigating bulk data interception cases: Victim status	5
3. SURVEILLANCE: SPYWARE	6
4. SEARCHES AND DEVICE SEIZURE	9

MODULE 4

1. INTRODUCTION

Safeguarding the rights of journalists in the digital space, including protecting their communications and other sensitive data, has become an increasingly complex and relevant issue in the new information age. As the usage of the Internet, including online communication tools and electronic data sharing platforms, expand rapidly, a growing amount of data is transferred and stored digitally. In addition, many contributions to public debate are disseminated and received online.

While legislative, judicial and policy developments are struggling to keep up with the fast pace of technological developments, European countries and regional organisations, such as the European Union (EU) and the Council of Europe (CoE) have introduced measures addressing both old standing as well as emerging questions relating to privacy, security and freedom of expression. These include questions around the surveillance and retention of journalists' communications and other forms of access to their devices.

2. SURVEILLANCE: BULK DATA INTERCEPTION

Surveillance of communications, including by introducing bulk interception regimes, has been to the forefront of legal developments on the issue of surveillance in recent years. Not only the increased data flow online, but also the technical sophistication of surveillance tools increases the risk of citizens, including journalists, becoming "transparent persons"¹ for state authorities. According to the UN Special Rapporteur on freedom of expression:

"Technological advancements mean that the State's effectiveness in conducting surveillance is no longer limited by scale or duration. [...] As such, the State now has greater capability to conduct simultaneous, invasive, targeted and broad-scale surveillance than ever before."²

2.1. What is bulk data interception?

Bulk data interception is defined as "the gathering of large chunks of internet traffic from around the world" in situations where the target is unknown, and the intent of the measure is to discover rather than to investigate.³ The data gathered can include, besides the content of the communication, the circumstances of its transmission, including the "who", "when" and "where".⁴ It is closely linked to mass surveillance, which "involves the acquisition, processing, generation, analysis, use, retention or storage of information about large numbers of people, without any regard to whether they are suspected of wrongdoing."⁵

¹ This term, which was originally used in the debates around the 1982 German census law, describes the extensive collection of personal data by public authorities.

² UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (17 April 2013), para 33, A/HRC/23/40, (accessible [here](#)).

³ Big Brother Watch, Interception (undated) (accessible [here](#)).

⁴ Nóra Ní Loideáin, Bulk Surveillance: Europe's Recent Landmark Judgements (5 July 2021), (accessible [here](#)).

⁵ Privacy International, Mass Surveillance (undated), (accessible [here](#)).

Such practices – as well as targeted surveillance measures – infringe on the right to privacy (Article 17 ICCPR, Article 8 ECHR), as authorities gain access to intimate private and professional data. In addition, the knowledge – or even suspicion – of being surveilled undermines the right to freedom of expression (Article 19 ICCPR, Article 10 ECHR), as the fear of unwillingly disclosing online activity or the identity of journalistic sources creates a chilling effect and leads to self-censorship, in particular in repressive environments.

2.2. International legal standards

Various UN bodies have expressed concern over the human rights impact of surveillance measures. For instance, the UN Human Rights Committee has stated that “[s]urveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited.”⁶ It further stated that to comply with the requirements of Article 17 ICCPR, the right to privacy, the “integrity and confidentiality of correspondence should be guaranteed de jure and de facto.”⁷

Communications surveillance has been described as a “highly intrusive act” which can only be justified in the most exceptional circumstances and must be accompanied by sufficient safeguards.⁸ Beyond this – as criticised by the UN Special Rapporteur on counter-terrorism in 2014 – “[b]ulk access technology is indiscriminately corrosive of online privacy and impinges on the very essence of the right guaranteed by article 17 [ICCPR]”⁹ as it “eradicates the possibility of any individualized proportionality analysis.”¹⁰ Aligned with this assessment, the UN Office of the High Commissioner for Human Rights (OHCHR) has also stressed that indiscriminate mass surveillance, and communications interception, collecting, storing and analysing of all users, is “not permissible under international human rights law, as an individualized necessity and proportionality analysis would not be possible in the context of such measures.”¹¹ According to the OHCHR, “the mere possibility of communications information being captured” and thus the very existence of a mass surveillance programme, interferes with the right to privacy.¹²

⁶ UN Human Rights Committee, General Comment No. 16: Article 17 (The right to respect of privacy, family, home and correspondence, and protection of honour and reputation) (1988), para 8, HRI/GEN/1/Rev.1 (accessible [here](#)).

⁷ *Ibid.*

⁸ UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (17 April 2013), para 81, A/HRC/23/40, (accessible [here](#)) available at

⁹ Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Promoting and protecting human rights and fundamental freedoms while countering terrorism (23 September 2023), A/69/397, paras 47 and 59.

¹⁰ *Ibid.* para 12.

¹¹ UN OHCHR, Report on best practices and lessons learned on how protecting and promoting human rights contribute to preventing and countering violent extremism (21 July 2016), A/HRC/33/29, para 58, (accessible [here](#)) available at; see also: UN OHCHR, The right to privacy in the digital age (3 August 2018), A/HRC/39/29, para 17, (accessible [here](#)).

¹² UN OHCHR, The right to privacy in the digital age (30 June 2014), A/HRC/27/37, para 20, (accessible [here](#))

2.3. Regional standards: EU

For almost a decade, mass surveillance measures have been subject to interpretation by European courts. The Court of Justice of the European Union (CJEU), in particular, has dealt with the topic of data retention measures extensively in a number of landmark judgments, raising concerns about, inter alia, the fact that the retained data allows authorities to draw very precise conclusions about the private life of the individuals concerned.¹³

- In its judgment regarding the case [Digital Rights Ireland/Seitlinger and Others](#) (2014), the CJEU invalidated the Data Retention Directive (EU Directive 2006/24/EC), which, inter alia, required telecommunications providers to retain all users' traffic and location data for prolonged periods. The CJEU invalidated the Directive on the basis that it interfered with the right to respect for private and family life and the protection of personal data in a "particularly serious" and disproportionate manner.¹⁴
- Two years later, in [Tele2 Sverige AB/Watson and Others](#) (2016), the CJEU built on these findings, holding that EU law precluded domestic legislation imposing an obligation on electronic communications services to generally and indiscriminately retain traffic and location data for the purpose of fighting crime.¹⁵ The CJEU at the same time clarified that the targeted retention of data, limited to what is strictly necessary, and imposed by clear and precise legislation containing sufficient safeguards is not precluded by EU law.¹⁶
- In the case of [Privacy International](#) (2020), the CJEU reiterated the prohibition of general and indiscriminate retention of data. The case required it to consider the application of EU law to domestic legislation requiring communications service providers to retain data and/or forward it to national security and intelligence services.¹⁷ The CJEU expanded on its findings in the Tele2 case, holding that EU law precludes domestic legislation which requires electronic communication service providers to generally and indiscriminately transmit traffic and location data to *security and intelligence agencies* for the purpose of safeguarding national security.¹⁸ In the joined case of [La Quadrature du Net and Others](#) (2020), the CJEU held that an order requiring general and indiscriminate location and traffic data retention can be justified where the state is facing

¹³ See for instance CJEU, Judgment of the Court (Grand Chamber) concerning SpaceNet AG and Telekom Deutschland GmbH v Bundesrepublik Deutschland (20 September 2022), paras 117 and 184.

¹⁴ CJEU, Judgment of the Court (Grand Chamber) concerning Digital Rights Ireland Ltd v Minister of Communications, Marine and Natural Resources and Others and Kärtener Landesregierung and Others, Joined Cases C-293/12 and C-594/12 (8 April 2014), paras 37 and 69.

¹⁵ CJEU, Judgment of the Court (Grand Chamber) concerning Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others, Joined Cases C-203/15 and C-698/15 (21 December 2016), para 112.

¹⁶ *Ibid.* para 108.

¹⁷ CJEU, Judgment of the Court (Grand Chamber) concerning Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others, Case C-623/17 (6 October 2020), para 82.

¹⁸ *Ibid.* para 49; see for an analysis for instance Monika Zalnieriute, *A Dangerous Convergence: The Inevitability of Mass Surveillance in European Jurisprudence* (4 June 2021), (accessible [here](#)) and Juraj Sajfert, *Bulk data interception/retention judgments of the CJEU – A victory and a defeat for privacy* (26 October 2020), (accessible [here](#)).

a serious, genuine and present or foreseeable threat to national security.¹⁹ While this order must be limited in time to what is strictly necessary, it may be extended if the threat persists.²⁰ Additionally, the CJEU clarified requirements for targeted retention as well as retention of IP addresses and other data allowing the identification of users, classifying some types of data as “less sensitive”²¹.

- It its recent decision in the case [SpaceNet/Telecom Deutschland](#) (2022), the CJEU again confirmed that EU law precludes the requirement of preventive, general and indiscriminate data retention to combat serious crime and prevent serious threats to public security.²² It further elaborated on a number of measures which, insofar as they are established by clear and precise rules containing sufficient safeguards, are not precluded, including:²³
 - Instructions to generally and indiscriminately retain traffic and location data for the purpose of safeguarding national security where there is a serious, genuine, present and foreseeable threat to national security, insofar as an effective review process is in place and the instruction is limited in time to what is strictly necessary;
 - Targeted retention of traffic and location data, which is limited in time and scope, for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security;
 - In addition, the CJEU elaborates on the circumstances under which the indiscriminate and general retention of IP addresses, data relating to the civil identity of users and expedited retention of traffic and location data in the possession of service providers may be justified under EU law.

2.4. Regional standards: CoE

The European Court of Human Rights (ECtHR) has also assessed the legality of different domestic bulk interception systems in several landmark cases.

Initially, in the 2006 judgment in the case *Weber and Saravia v. Germany*, the ECtHR held that states generally enjoy a “fairly wide margin of appreciation” in respect to measures concerning national security and the prevention of crimes.²⁴

A few years later, the ECtHR had to examine the Russian secret telecommunications regime in light of the ECHR in *Zakharov v. Russia*. The Grand Chamber found a violation of Article 8 ECHR, arguing that the domestic provisions lacked “adequate and effective guarantees against arbitrariness and the risk of abuse which is inherent in any system of secret surveillance”.²⁵ Similarly, the ECtHR found that the Hungarian anti-terror legislation did not

¹⁹ CJEU, Judgment of the Court (Grand Chamber) concerning La Quadrature du Net and Others v Premier minister and Others, Joined Cases C-511/18, C-512/18 and C-520/18 (6 October 2020), para 168.

²⁰ *Ibid.*

²¹ *Ibid.* paras 152, 168.

²² CJEU, Judgment of the Court (Grand Chamber) concerning SpaceNet AG and Telekom Deutschland GmbH v Bundesrepublik Deutschland (20 September 2022), para 132.

²³ *Ibid.*

²⁴ ECtHR, *Weber and Saravia v. Germany*, App. No. 54934/00, §137, 29 June 2006.

²⁵ ECtHR, *Roman Zakharov v Russia* [GC], App No. 47143/06, §302, ECHR 2015.

contain sufficient safeguards and expressed its concern over the fact that virtually anyone in Hungary could be surveilled.²⁶

In a groundbreaking judgment on bulk surveillance, the ECtHR's First Section ruled in *Big Brother Watch v. UK* in 2018 that bulk interception by intelligence agencies is not in and of itself incompatible with the right to privacy.²⁷ This finding was later confirmed by the Grand Chamber, which found that bulk interception measures can be justified under certain circumstances, such as for gathering intelligence data and to counter terrorism and espionage.²⁸ The ECtHR held that while bulk interception regimes do not *per se* violate the Convention rights, they must contain end-to-end safeguards as well as sufficient protection for journalistic sources.²⁹ In the case of *Centrum för Rättvisa v. Sweden*, decided on the same day, the ECtHR's Grand Chamber found that the Swedish bulk interception regime violated Article 8 ECHR, but also explicitly held that "bulk interception is of vital importance to Contracting States in identifying threats to their national security" and "no alternative or combination of alternatives would be sufficient to substitute for the bulk interception power."³⁰

The Court has since examined further domestic mass surveillance and data retention systems and found violations of the ECHR.³¹

2.5. Litigating bulk data interception cases: Victim status

The term "standing" is usually understood as a person's or organisations ability to bring a case to a particular court. While its requirements differ between jurisdictions, an applicant is usually asked to establish why they are affected by the matter or what interest they represent. Often, they will be required to demonstrate a sufficient connection between an issue and their interest in it.

The ECtHR, as mandated by Article 34 ECHR, accepts applications from those "claiming to be a victim of a violation by one of the High Contracting Parties of the rights set forth in the Convention or the Protocols thereto." While this includes not only direct victims also those who would suffer harm or have a valid interest in the case,³² the ECtHR has made clear that:

"the Convention does not provide for the institution of an *action poularis* and that its task is not normally to review the relevant law and practice *in abstracto*, but to determine

²⁶ ECtHR, *Szabó and Vissz v. Hungary*, App. No. 37138/14, §88, 12 January 2016.

²⁷ ECtHR, *Big Brother Watch and Others v. the United Kingdom*, App Nos. 58170/13 and 2 others, §314, 13 September 2018; see for an analysis Nóra Ní Loideáin, Bulk Surveillance: Europe's Recent Landmark Judgements (5 July 2021), (accessible [here](#)).

²⁸ ECtHR, *Big Brother Watch v. UK*, App Nos. 58170/13 and Others, 25 May 2021; see for an analysis Eliza Watt, The legacy of the privacy versus security narrative in the ECtHR's jurisprudence (21 April 2022) (accessible [here](#)).

²⁹ ECtHR, *Big Brother Watch v. UK*, App Nos. 58170/1 and Others, §§350, 442-450, 25 May 2021.

³⁰ ECtHR, *Centrum för Rättvisa v. Sweden*, App. No. 35252/08, §365, 25 May 2021; Monika Zalnieriute, A Dangerous Convergence: The Inevitability of Mass Surveillance in European Jurisprudence (4 June 2021), (accessible [here](#)).

³¹ See for instance ECtHR, *Ekimdziev and Others v. Bulgaria*, App. No. 70078/12, 11 January 2022; ECtHR, *Podchasov v. Russia*, App. No. 33696/19, 13 February 2024; ECtHR, *Škoberne v. Slovenia*, App No. 19920/20, 15 February 2024.

³² ECtHR [GC], *Vallianatos and Others v. Greece*, App. Nos. 29381/09 and 32684/08, §47, 7 November 2013.

whether the manner in which they were applied or affected the applicant gave a rise to a violation of the Convention.”³³

Therefore, the ECtHR generally requires applicants to explain how they were victims of a specific act that they claim violated their rights. However, under certain circumstances, “potential victims” can apply to the ECtHR. This includes individuals suspecting to have been targeted by covert (surveillance) measures. As these individuals cannot know whether such a measure was used, the ECtHR accepts that “the mere existence of secret measures or of legislation permitting secret measures” can be sufficient.³⁴ This is the case where the applicant can possibly have been affected by the legislation in question and there are no sufficient and effective domestic remedies available.³⁵

Similar approaches are taken by some domestic courts. For example, the Federal Constitutional Court of Germany accepted the submission that the applicants, who had complained of the 2007 retention obligations in the Telecommunications Act, used telecommunication services in their private and professional capacity, accepting their standing based on the “reasonable likelihood” of being affected by such measures.³⁶ The Constitutional Court continued to follow this line of argument in subsequent cases, where there was a sufficient probability of the applicants having been targeted with measures under the provisions complained of when there were insufficient ex post facto disclosure obligations.³⁷

3. SURVEILLANCE: SPYWARE

Targeted surveillance describes surveillance which focusses on obtaining information about the communications of a specific individual, such as a person who is already a suspect in a criminal case.”³⁸ A prominent example is the use of spyware, a malicious type of software which “interferes with a device’s normal operation to collect information without alerting the user”.³⁹

The most intrusive type of spyware currently known to the public is Pegasus spyware, which is manufactured by the Israeli cyber-arms company NSO Group and is exclusively sold to governments. In 2021, the Organised Crime and Corruption Project (OCCPR), released a report which outlined the use of Pegasus spyware on, inter alia, journalists, human rights defenders, activists and political figures worldwide.

³³ ECtHR, *Roman Zakharov v Russia* [GC], App No. 47143/06, §164, ECHR 2015 with further references.

³⁴ See ECtHR, *Klass and Others v. Germany*, App No. 5029/71, §34, 6 September 1978.

³⁵ ECtHR, *Roman Zakharov v Russia* [GC], App No. 47143/06, §171, ECHR 2015; see also ECtHR, *Kennedy v. UK*, App No. 26839/05, §124, 18 May 2010; ECtHR, *Centrum för Rättvisa v. Sweden*, App No. 35252/08, §§166-167, 25 May 2021; ECtHR, *Wieder and Guarnieri v. The United Kingdom*, App Nos. 64371/16 and 64407/16, §§97-110, 12 September 2023.

³⁶ German Federal Constitutional Court, Order of 2 March 2010 (TKG), 1 BvR 256/08, 1 BvR 586/08, 1 BvR 263/08, §§177-178, (accessible [here](#)).

³⁷ German Federal Constitutional Court, Order of 20 April 2016, 1 BvR 966/09, §§82-84, (accessible [here](#)) and Order of 19 May 2020, BNDG, 1 BvR 2835/17, §§71-76, (accessible [here](#)).

³⁸ Nóra Ní Loideáin, Bulk Surveillance: Europe’s Recent Landmark Judgements (5 July 2021), (accessible [here](#)).

³⁹ Amnesty International, What is spyware and what can you do to stay protected? (14 December 2023), (accessible [here](#)).

Pegasus spyware can be installed covertly on an individual's device, often their mobile phone. Once installed, the spyware turns the device into a full-time surveillance tool, granting unrestricted access to the stored data, as well as the device's camera, microphone, messages, photos, passwords, calls, and geolocation

Methods of implantation on a device include the clicking on a malicious link by the user or the use of a wireless transmitter in close proximity to the phone. However, one of the most concerning revelations about Pegasus spyware is its capability to infect a device through the so-called "zero click"-method, which does not require any act by the user or any "jailbreaking" of the system.

Once a device is infected, it is extremely difficult to detect the spyware as well as its actions, for instance whether there has been an extraction of data.

3.1. International standards

Various international bodies have expressed serious concern over the use of spyware, including the UN Human Rights Committee.⁴⁰ As pointed out by the UN OHCHR, the development and use of pervasive surveillance tools is "profoundly alarming", threatening the rule of law and eroding pluralistic democracies.⁴¹ The targeting of journalists, human rights defenders and others with this spyware tool constitutes a serious interference with the right to privacy (Article 17 ICCPR)⁴² which, in particular when carried out for political reasons, can never be justified⁴³.

In addition, the use of Pegasus spyware violates freedom of expression, protected on the international level by Article 19 ICCPR. Infecting a personal communication device with spyware permits "insights into the thinking processes of individuals subject to hacking, as well as their political and religious views and beliefs".⁴⁴ This is especially true in the journalistic context as the protection of journalistic sources is circumvented and the mere existence of spyware creates a chilling effect.⁴⁵

3.2. Regional standards: EU

In the EU, targeted surveillance measures – with the exception of national security measures excluded from its scope by Article 4(2) TEU – must comply with applicable Union primary and secondary law, in particular the EU Charter, the ePrivacy Directive and the Law Enforcement

⁴⁰ HRC, *Concluding observations on the seventh periodic report of Germany* (30 November 2021), CCPR/C/DEU/CO/7, paras 42-43, ([accessible here](#)); HRC, *Concluding observations on the fifth periodic report of the Netherlands* (22 August 2019), CCPR/C/NLD/CO/5, paras 54-55, ([accessible here](#)); HRC, *Concluding observations on the sixth periodic report of Italy* (1 May 2017), CCPR/C/ITA/CO/6, paras 36-37, ([accessible here](#)).

⁴¹ UN Human Rights Council, *The right to privacy in the digital age. Report of the Office of the United Nations High Commissioner for Human Rights* (4 August 2022), A/HRC/51/17, para 54, ([accessible here](#)).

⁴² *Ibid.* paras 4-5 and 9, ([accessible here](#)).

⁴³ *Ibid.* paras 18-19.

⁴⁴ *Ibid.*, para 9, ([accessible here](#)); see also 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 20, ([accessible here](#)).

⁴⁵ *Ibid.* para 10.

Directive.⁴⁶ Article 52(1) EU Charter requires all acts limiting fundamental rights to confirm with the requirements of proportionality and necessity.⁴⁷

Due to the quality and quantity of data stored on smartphones, the EU Data Protection Supervisor, considers it “highly unlikely that spyware such as Pegasus, which de facto grants full unlimited access to personal data, including sensitive data, could meet the requirements of proportionality” as “the interference with the right to privacy is so severe that the individual is in fact deprived of it” and that the protection of third parties and those who are afforded special protection, such as lawyers, is not guaranteed.⁴⁸

In a similar approach, the European Parliament has condemned “the use of spyware by Member State governments, and members of government authorities or state institutions for the purpose of monitoring, blackmailing, intimidating, manipulating and discrediting opposition members, critics and civil society, eliminating democratic scrutiny and the free press, manipulating elections and undermining the rule of law by targeting judges, prosecutors and lawyers for political purposes.”⁴⁹

3.3. Regional standards: CoE

On 23 October 2023, the CoE’s Parliamentary Assembly issued a resolution expressing its deep worry about “mounting evidence that Pegasus and similar spyware have been used illegally or for illegitimate purposes by several member states, including against journalists, political opponents, human rights defenders and lawyers” and condemned its use for political purposes.⁵⁰

Even before the revelations about the intrusiveness of Pegasus spyware, ECtHR’s Grand Chamber has acknowledged that against the backdrop or rapid technical advancement, domestic law must be sufficiently clear “to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures.”⁵¹

The ECtHR has yet to deliver its first judgment on a case concerning the use of Pegasus spyware. However, its caselaw gives some insights into how it approaches such matters.

The use of intrusive spyware against journalists goes to the heart of their right to private and family life (Article 8 ECHR), as well as their freedom of expression (Article 10 ECHR), as it gives access to a range of sensitive information and correspondence and creates a chilling effect for those contributing to public debate. Its use fails to meet the conditions of the so-called three-part test, in particular the requirements of necessity and proportionality. Lastly, Pegasus spyware circumvents the protection of journalistic sources, without which, as

⁴⁶ See: The European Data Protection Supervisor, Preliminary Remarks on Modern Spyware (15 February 2022), p. 6, (accessible [here](#)).

⁴⁷ Ibid. p. 7.

⁴⁸ The European Data Protection Supervisor, Preliminary Remarks on Modern Spyware (15 February 2022), p. 8, (accessible [here](#)).

⁴⁹ EU Parliament, Investigation of the use of Pegasus and equivalent surveillance spyware (Recommendation) (15 June 2023), no. 3, (accessible [here](#)).

⁵⁰ PACE, *Pegasus and similar spyware and secret state surveillance*, Resolution 2513 (2023) (11 October 2023), (accessible [here](#)).

⁵¹ *Roman Zakharov v Russia* [GC], App No. 47143/06, §229, ECHR 2015.

stressed by the ECtHR, sources may be deterred from speaking to the press, which in turn cannot fulfil its public watchdog role.⁵²

Litigating spyware cases: Victim status

In contrast to cases concerning mass surveillance legislation, individuals targeted with spyware, such as Pegasus spyware, have usually been informed by technical experts, their devices' manufacturer or civil society organisations that they have been specifically targeted and that their devices have been infected. However, they often face other obstacles in litigating their cases, as the majority of the information about the hacking remains solely in the domain of the attacking state. These difficulties include, but are not limited to the following:

- Meeting the burden of proof required by the court they are accessing;
- Difficulties in obtaining detailed technical evidence that the hacking took place;
- Submitting details on the date and length of the infection, the data accessed/extracted and the aim of the measure;
- Identifying the attacking state.

4. SEARCHES AND DEVICE SEIZURE

Digital devices such as phones, cameras, laptops, and storage devices have become essential tools for journalists in conducting their work. They are used, for instance to conduct for research, recording, communicating with confidential sources and other journalists, and for publishing content. However, such devices often become subject to seizures and searches by authorities, in particular in situations perceived as sensitive, such as when covering protests⁵³ or at national borders⁵⁴. As civil society organisations are documenting growing number of seizures and (forensic) searches of journalists' digital equipment,⁵⁵ safeguarding digital security remains an important factor to ensure the functioning of the press. Practical tips for journalists covering protests can be found [here](#).

Through searches and seizures, authorities obtain access to protected materials, including the identity of journalistic sources, thus endangering their safety and creating a chilling effect. The search of mobile devices is particularly intrusive due to the quantity and the sensitivity of the data accessed. Such measures infringe on the right to privacy (Article 8 ECHR) and freedom of expression (Article 10 ECHR) and can only be justified if they meet the cumulative criteria of the so-called three-part test. In addition, the search of journalists' home, workplace and the seizure of their material must be accompanied by adequate and effective procedural safeguards.⁵⁶

⁵² See for instance ECtHR, *Telegraaf Media Nederland Landelijke Media B.V. and Others v. The Netherlands*, App No 39315/06, §127 22 November 2012; ECtHR, *Sedletska v. Ukraine*, App No. 42634/18, §§54-55, 1 April 2021.

⁵³ See for instance Media Defence, *Reporting at Protests: Factsheet* (undated), (accessible [here](#)).

⁵⁴ See for instance Article 19, *European Court of Human Rights: Search of journalists' devices at border* (31 August 2023), (accessible [here](#)).

⁵⁵ For example in West Africa: MFWA, *Seizure and Destruction of Journalists' Digital Tools: The Data Privacy and Censorship implications* (2 April 2020), (accessible [here](#)).

⁵⁶ CoE Platform to promote the protection of journalism and safety of journalists, *The Protection of Journalistic Sources, A Cornerstone of the Freedom of the Press* (June 2018), (accessible [here](#)).

The ECtHR has clarified that:

“journalists should enjoy a broad scope of protection, including a range of freedoms that are of functional relevance to the pursuit of their activities, such as: protection of confidential sources; protection against searches of professional workplaces and private domiciles and the seizure of materials, protection of news and information-gathering processes [...]”⁵⁷

Special attention must be paid to the protection of journalistic sources,⁵⁸ a principle which, in the words of the ECtHR, is “one of the cornerstones” of press freedom and essential to enable the press to fulfil its public-watchdog role.⁵⁹

The ECtHR has applied these numerous cases, confirming for instance that the search of a journalist’s laptop at a border crossing violated Article 8 ECHR due to the lack of effective and adequate safeguards in Russian domestic legislation and practice.⁶⁰ In *Sorokin v. Russia*, the ECtHR found a violation of Article 10 ECHR after a journalist’s flat and his electronic devices, which contained information related to his work, were searched without any procedural safeguards to protect the confidentiality of his sources.⁶¹ In *Nagla v. Latvia*, the ECtHR stressed that:

“the right of journalists not to disclose their sources cannot be considered a mere privilege to be granted or taken away depending on the lawfulness or unlawfulness of their sources, but is part and parcel of the right to information, to be treated with the utmost caution”⁶².

⁵⁷ ECtHR, *Man and Others v. Romania*, App. No. 39273/07, §131, 19 November 2019.

⁵⁸ See for instance CoE Committee of Ministers, Recommendation No. R (2000) 7 of the Committee to Ministers to member states on the right of journalists not to disclose their sources of information (8 March 2000), (accessible [here](#)).

⁵⁹ ECtHR, *Sedletska v. Ukraine*, App No. 42634/18, §§54-55, 1 April 2021; see also ECtHR, *Telegraaf Media Nederland Landelijke Media B.V. and Others v. The Netherlands*, App No 39315/06, §127 22 November 2012; ECtHR, *Goodwin v. The UK*, App No. 17488/90, §39, 27 March 1996.

⁶⁰ ECtHR, *Ivashchenko v. Russia*, App. No. 61064/10, §§63-69, 93, 13 February 2018.

⁶¹ Dirk Vorhoof, European Court of Human Rights: Sergey Sorokon v Russia (2022), (accessible [here](#)).

⁶² ECtHR, *Nagla v. Latvia*, App No 73469/10, §97, 16 July 2013.

Module 5

**‘False News’,
Misinformation
& Propaganda**

*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	1
2. WHAT IS 'FALSE NEWS'	1
2.1. Definition.....	1
2.2. International efforts	2
3. MISINFORMATION, DISINFORMATION AND MAL-INFORMATION	4
3.1. The socio-technical context.....	4
3.2. Journalism, political advertising, and elections.....	6
4. HOW TO COMBAT MISINFORMATION, DISINFORMATION AND MAL- INFORMATION	7
4.1. Media and Information Literacy (MIL) strategies and campaigns.....	8
4.2. Litigation where justifiable limitations exist.....	9
4.3. Fact-checking and social media verification	10
5. PROPAGANDA	11
6. CONCLUSION	12

MODULE 5

1. INTRODUCTION

In today's digital landscape, the proliferation of false news and misinformation has surged, particularly amplified by the rapid expansion of the internet and the pervasive reach of social media platforms. The manipulation and distortion of information have been prevalent throughout history, but the contemporary era has seen an unparalleled weaponisation of information in the new online environment, warranting an urgent response both domestically and throughout the region.¹ This module looks at false news, misinformation, and propaganda, shedding light on the urgency to combat these challenges effectively. It also explores possible response mechanisms, other than legal regulation, such as Media and Information Literacy (MIL) strategies and campaigns to counter misinformation without compromising the fundamental right to freedom of expression.

For the purposes of this module, the term “misinformation” is used broadly and, unless otherwise specified, includes reference to disinformation and malinformation.²

2. WHAT IS 'FALSE NEWS'

2.1. Definition

In the digital age, the dissemination of information has evolved, giving rise to distinct yet interrelated phenomena: false news, disinformation, and misinformation, as well as malinformation.

“False news” refers to purported news items that are intentionally and verifiably false and seek to mislead readers.³ False news mimics the format of credible news reports, harnessing attention-grabbing titles, images, and content designed to persuade readers into believing falsehoods. Usually, false news online is disseminated to amass “clicks,” “shares,” and engagement to bolster advertising revenue or further ideological agendas.⁴ The term has, in recent years, fallen out of favour due to the inaccurate implication that, despite being false, it nonetheless constitutes “news.”

Disinformation constitutes intentionally false or misleading content that is strategically propagated to deceive, manipulate, or achieve political or economic objectives.⁵

¹ UNESCO, 'Journalism, "Fake News" and Disinformation: Handbook for Journalism Education and Training (2018) ('UNESCO Handbook') at p. 15 ([accessible here](#)).

² For more on this topic see Media Legal Defence Initiative, 'Training Manual on Digital Rights and Freedom of expression Online: Litigating digital rights and online freedom of expression in East, West and Southern Africa' ([accessible here](#)). For further information see First Draft, 'Understanding and addressing the disinformation ecosystem' (2017) ([accessible here](#)).

³ Media Defence, 'False News, Misinformation & Propaganda' ([accessible here](#)).

⁴ Baptista and Gradim, 'Understanding Fake News Consumption: A Review' (2020) 9(10) *Soc. Sci 5*.

⁵ European Regulators Group for Audiovisual Media Services, 'Notions of Disinformation and Related Concepts' (2021) at p. 30 ([accessible here](#)) ('ERGA').

Lastly, misinformation entails false or misleading content shared inadvertently, lacking the malicious intent associated with disinformation.⁶ Despite the absence of deliberate deceit, the unintended consequences of misinformation can still be harmful, contributing to public confusion and creating mistrust in reliable information sources.

While misinformation and disinformation are premised on the dissemination of false information, malinformation is based on reality, with the information being used intentionally to inflict harm on a person, social group, organisation, or country.⁷

The following table highlights the commonalities and differences among the three types of false information:

Aspects	Misinformation	Disinformation	Mal-information
False information	Shared without intent to deceive	Deliberately spread to mislead	Truthfully represents but aims to deceive
Intent	No intention to deceive	Intentionally deceptive	Intends to deceive despite truthful content
Representation of reality	Misrepresents without deceptive intent	Misrepresents with deceptive intent	Truthfully represents but deceives through intent
Examples	Unintentional sharing of false information	Fake news, hoaxes, propaganda	Half-truths, spin, selective disclosure
Impact	Can still have harmful effects	Can have severe consequences	Can mislead without outright lying
Potential harm	Can influence opinions and trust	Damages trust, affects societal opinions	Impacts perceptions and decisions

2.2. International efforts

Several initiatives at both the regional and international levels have sought to deal with the growing problem of misinformation and other forms of harmful information online in recent years.

Of particular note at the international level is the 2017 Joint Declaration on Freedom of Expression and “Fake News”, Disinformation and Propaganda ([2017 Joint Declaration](#)) issued by the relevant freedom of expression mandate-holders of the United Nations ([UN](#)), the African Commission on Human and Peoples’ Rights ([ACHPR](#)), the Organisation for Security and Co-operation in Europe ([OSCE](#)), and the Organisation of American States ([OAS](#)).⁸ The 2017 Joint Declaration noted the growing prevalence of disinformation and propaganda, both online and offline, and the various harms to which they may contribute or be a primary cause.

⁶ Id.

⁷ International Telecommunication Union, ‘Session 5: Disinformation, misinformation, malinformation and Infodemics: Ways to handle’ (accessible [here](#)).

⁸ Joint Declaration on Freedom of Expression and “Fake News”, Disinformation and Propaganda (2017) (accessible [here](#)).

Amidst this evolving digital landscape, the declaration emphasised the transformative role of the internet and digital technologies in enabling access to information and facilitating responses to disinformation while acknowledging the responsibilities of intermediaries in respecting human rights.⁹

Recommendations of the 2017 Joint Declaration

The 2017 Joint Declaration highlighted, however, that efforts to regulate these harms often have negative effects on freedom of expression and, thus, identified the following recommended standards:

- General prohibitions on the dissemination of information based on vague and ambiguous ideas, including “false news” or “non-objective information”, are incompatible with international standards for restrictions on freedom of expression, as set out in paragraph 1(a), and should be abolished.
- Criminal defamation laws are unduly restrictive and should be abolished. Civil law rules on liability for false and defamatory statements are legitimate only if defendants are given a full opportunity and fail to prove the truth of those statements and also benefit from other defences, such as fair comment.
- State actors should not make, sponsor, encourage or further disseminate statements which they know or reasonably should know to be false (disinformation) or which demonstrate a reckless disregard for verifiable information (propaganda).
- State actors should, in accordance with their domestic and international legal obligations and their public duties, take care to ensure that they disseminate reliable and trustworthy information, including about matters of public interest, such as the economy, public health, security and the environment.

The Joint Declaration called on state actors to ensure that they disseminate reliable and trustworthy information, and not to make, sponsor, encourage or further disseminate statements that they know (or reasonably should know) to be false or which demonstrate a reckless disregard for verifiable information.¹⁰

In 2023, the UN Educational, Scientific and Cultural Organisation ([UNESCO](#)) also published Guidelines for the governance of digital platforms: safeguarding freedom of expression and access to information through a multi-stakeholder approach which “outline a set of duties, responsibilities and roles for States, digital platforms, intergovernmental organisations, civil society, media, academia, the technical community and other stakeholders” that will ensure freedom of expression and information.¹¹

⁹ Above n 8.

¹⁰ Above n. 8.

¹¹ UNESCO, ‘Guidelines for the Governance of Digital Platforms: Safeguarding freedom of expression and access to information through a multistakeholder approach,’ (2023) (accessible [here](#)).

5 Principles for Governance Systems

The UNESCO Guidelines emphasise five principles that should underly all governance systems that impact freedom of expression and access to information on digital platforms, based on an extensive consultation process that considered over 10,000 comments from 134 countries:

- Principle 1: Platforms should conduct human rights due diligence
- Principle 2: Platforms must adhere to international human rights standards, including in platform design, content moderation, and content curation;
- Principle 3: Platforms must be transparent;
- Principle 4: Platforms must make information and tools available for users;
- Principle 5: Platforms should be accountable to relevant stakeholders

3. MISINFORMATION, DISINFORMATION AND MAL-INFORMATION

3.1. *The socio-technical context*

In interrogating the root of this problem, it is clear that social media has played a substantial role in the widespread distribution of misleading messages. This can be attributed to the heightened impact of social media compared to traditional platforms due to their speed, broad reach, and personalised features.¹² User-generated content capabilities enable individuals to craft false messages while social interactions online facilitate the dissemination of these messages quickly and widely.¹³ Social media features that enable users to “share,” “repost” and “follow” also amplify the reach of false information within these platforms, with little formal fact-checking or verification of information.¹⁴

Other digital products such as algorithms, which now determine which information is seen and prioritised by audiences, and websites that publish and disseminate such information, also contribute to the challenge.¹⁵

Misinformation has the powerful potential to influence opinions and behaviours in various contexts such as politics and elections.¹⁶ The crisis of sustainability within the traditional media sector, fuelled by the growing dominance of the big tech platforms and the rapid shift away from print news, has also contributed to a generally poor information ecosystem in which misinformation and disinformation are able to thrive.

¹² (ECiHR) has emphasised, ‘Data citizenship: Rethinking data literacy in the age of disinformation, misinformation, and malinformation’ (2020) 9(2) *Internet Policy Review* 5-6 (accessible [here](#)).

¹³ *Id.*

¹⁴ Above n. 12.

¹⁵ Ali Khan and others, ‘The anatomy of “fake news”: Studying false messages as digital objects’ (2022) 37(2) *Journal of Information Technology* 125 (accessible [here](#)).

¹⁶ Above n 1 at p. 18.

This, alongside more insidious practices such as the intentional distribution of disinformation for economic or political gain, has created what UNESCO refers to as a “perfect storm.”¹⁷

UNESCO identifies three causes enabling the spread of misinformation:

1. **Collapsing traditional business models:** As a result of the rapid decline in advertising revenue and the failure of digital advertising to generate profit, traditional newsrooms are bleeding audiences, with media consumers moving to “peer-to-peer” news products offering “on demand-access.” These decreasing budgets lead to reduced quality control and less time for “checks and balances”. They also promote “click-bait” journalism.¹⁸ Importantly there are no commonly agreed ethics and standards on peer-to-peer news.
2. **Digital transformation of newsrooms and storytelling.** As the information age develops, there is a discernible digital transformation in the news industry. This transformation causes journalists to prepare content for multiple platforms, limiting their ability to properly interrogate facts. Often, journalists apply a principle of “social-first publishing” whereby their stories are posted directly to social media to meet audience demand in real-time. This, in turn, promotes click-bait practices and the pursuit of “virality” as opposed to quality and accuracy.¹⁹
3. **The creation of new news ecosystems.** With increasing access to online audiences as a result of the advent of social media platforms, users of these platforms can curate their own content streams and create their own “trust network” or “echo chambers” within which inaccurate, false, malicious, and propagandistic content can spread. These new ecosystems allow misinformation to flourish as users are more likely to share sensationalist stories and less likely to properly assess sources or facts. Importantly, once published, a user who becomes aware that a publication may constitute misinformation is largely unable to “pull back” or correct the publication.²⁰

Rise in online false news in elections in Spain

In the lead-up to Spain's regional and municipal elections in May 2023, false claims about mail ballots and election fraud circulated widely across social media platforms, echoing similar assertions made by former United States President Donald Trump prior to his 2020 election loss.²¹ Debunked videos supposedly displaying election fraud spread on platforms including Facebook and Twitter.²² Other videos circulated on Facebook and TikTok alleging electoral manipulation by the then-outgoing and currently re-elected Prime Minister's party.²³

¹⁷ Id.

¹⁸ Above n 1 at p. 57.

¹⁹ Above n 1 at pp. 57-8.

²⁰ Above n 1 pp. 59-61.

²¹ AP, 'Warning over online misinformation ahead of Spanish election' (2023) *Euronews* (accessible [here](#)).

²² Id.

²³ Above n 21.

Research uncovered numerous instances of election-related misinformation across platforms such as Twitter, Facebook, YouTube, and TikTok in Spain.²⁴ While content types vary, election denialism remains a prevalent theme around the world. Conspiracy groups have been found to orchestrate social media attacks resulting in distrust of independent media and creating barriers to users' access to credible information.²⁵

3.2. Journalism, political advertising, and elections

Journalism faces the threat of being overshadowed by the widespread dissemination of false information which significantly diminishes the impact of the accurate news disseminated by journalists.²⁶ There is also the risk of manipulation, with actors aiming to corrupt journalists or manipulate them beyond the ethical bounds of their profession.²⁷ Journalists, particularly those committed to uncovering inconvenient truths, often become targets of deliberate lies, rumours, and hoaxes designed to discredit their work. This is exacerbated by the instrumentalisation of false concerns by powerful entities, leading to the imposition of stringent laws that could suppress genuine news media.²⁸

In the realm of political advertising and elections, the landscape lacks uniformity at the European Union (EU) level. Although the rights to freedom of expression and free elections could be interrelated, in certain circumstances, they may come into conflict.²⁹ The European Court of Human Rights (ECtHR) has emphasised that the interaction between freedom of expression and the right to free elections can either complement each other or create conflicts based on specific circumstances.³⁰ In fact, the issue predates the era of social media, with the Court emphasising in the 1987 *Mathieu-Mohin and Clerfayt v Belgium* matter that it is the responsibility of state authorities to facilitate the free expression of people's opinions during elections.³¹

False information during elections

In the *Salov v Ukraine* (2005) case, the ECtHR reviewed a scenario involving a newspaper disseminating false information about the alleged death of a presidential candidate.³² Despite the factual inaccuracy, the ECtHR recognised that the information related to the elections influenced the electorate's ability to support a particular candidate.³³ Consequently, the ECtHR maintained that the same principles governing political discourse

²⁴ Above n 21.

²⁵ International Press Institute, 'New report: How conspiracy groups in Spain worked to undermine the media literacy project of the Maldita.es foundation' (2023) (accessible [here](#)).

²⁶ UNESCO, 'Journalism, "Fake News" & Disinformation: Handbook for Journalism Education and Training' (2018) (accessible [here](#)).

²⁷ Id.

²⁸ Above n 26.

²⁹ Paolo Cavaliere, 'The Truth in Fake News: How Disinformation Laws Are Reframing the Concepts of Truth and Accuracy on Digital Platforms' (2022) 3 *European Convention on Human Rights Law Review* 513 (accessible [here](#)).

³⁰ Id.

³¹ (Application no. 9267/81) (1998) para. 54 (accessible [here](#)).

³² (Application no. 65518/01) (2005) para. 111 (accessible [here](#)).

³³ Id.

apply irrespective of the factual accuracy of the information, emphasising that even if the distributor strongly suspected the information's untruthfulness, the European Convention on Human Rights (ECHR) did not prohibit the dissemination of information.³⁴

A guide to anti-misinformation actions around the world

The Poynter Institute, an international resource on journalism, has compiled information about [global efforts to regulate misinformation](#) in various ways, including through laws, and media literacy programmes, amongst other things.³⁵ France passed a law that outlaws election misinformation in 2018, Croatia is reportedly working on a draft bill against hate speech and misinformation, Belarus has passed amendments to media laws that allow prosecution of people who spread false information online, and Russia has also passed an anti-misinformation bill that bans the spread of “unreliable socially-important information.”

The EU Disinfo Lab provides a [similar resource](#) targeted at EU states.

4. HOW TO COMBAT MISINFORMATION, DISINFORMATION AND MAL- INFORMATION

Of particular importance in the European context is the new [EU Digital Services Act](#), which came into force in November 2022 and applies across the EU. The law is targeted at major online intermediaries and platforms, requiring them to put in place systems to control the spread of misinformation as well as hate speech and terrorist propaganda at the risk of large penalties calculated as a proportion of global annual revenue or a ban. It also includes other requirements related to transparency over the spread of certain types of content and the role of their services in this spread, as well as conducting an annual risk assessment.

In addition to legislation, the European Commission has introduced several alternative measures to combat disinformation:³⁶

- The [Communication on “Tackling online disinformation: a European Approach”](#) compiles tools to combat the propagation of disinformation and safeguard EU principles and the [2022 Code of Practice on Disinformation](#) aims to fulfil the objectives outlined in the Communication.
- The [Action Plan on Disinformation](#) aims to enhance the EU's capacity and collaboration in combatting disinformation.
- The [European Democracy Action Plan](#) outlines standards for the responsibilities and the liability of online platforms in combatting disinformation.

³⁴ Above n 32 para. 113.

³⁵ Daniel Funke and Daniela Flamini, ‘A guide to anti-misinformation actions around the world,’ *Poynter* (accessible [here](#)).

³⁶ European Commission, ‘Tackling online disinformation’ (accessible [here](#)).

- The European Digital Media Observatory ([EDMO](#)), an independent observatory, unites fact-checkers, academic researchers specialising in online disinformation, social media platforms, journalist-driven media, and media literacy experts.
- The [Strengthened Code of Practice on Disinformation](#), endorsed on 16 June 2022, brings together diverse stakeholders committed to a broad range of voluntary obligations to counter disinformation.
- The [2018 report](#) of the European Commission High-level Group of Experts on fake news and online disinformation, encourages a multi-dimensional approach to tackling these issues along the lines of five pillars.

Additionally, two expert groups, namely the [Committee of Experts on quality journalism in the digital age](#) and the [Committee of Experts on Human Rights Dimensions of automated data processing and different forms of artificial intelligence](#) have been appointed by the Council of Europe to explore in more detail how member states can promote a favourable environment for “an independent, diverse and pluralistic media environment in which societies can both trust and actively participate in.”³⁷

4.1. *Media and Information Literacy (MIL) strategies and campaigns*

Given the risks inherent in legislation of regulating and criminalising speech, UNESCO proposes MIL strategies and campaigns as an alternative mechanism to detect misinformation and combat its spread, particularly online.³⁸

Defining Media and Information Literacy

MIL is an umbrella and inter-related concept which is divided into:

- **Human rights literacy** which relates to the fundamental rights afforded to all persons, particularly the right to freedom of expression, and the promotion and protection of these fundamental rights.³⁹
- **News literacy** which refers to literacy about the news media, including journalistic standards and ethics.⁴⁰ This includes, for example, the specific ability to understand the “language and conventions of news as a genre and to recognise how these features can be exploited with malicious intent.”⁴¹
- **Advertising literacy** which relates to understanding how advertising online works and how profits are driven in the online economy.⁴²
- **Computer literacy** which refers to basic IT usage and understanding how headlines, images, and, increasingly, videos can be manipulated to promote a particular narrative.⁴³

³⁷ Council of Europe, ‘Information Disorder’ (accessible [here](#)).

³⁸ Above n 1 at p. 70.

³⁹ Id.

⁴⁰ Above n 1 p. 70.

⁴¹ Id.

⁴² Above n 1 p. 70.

⁴³ Id.

- **Understanding the “attention economy”** which relates to one of the causes of misinformation and the incentives to create click-bait headlines and misleading imagery to grab the attention of users and, in turn, drive online advertising revenue.⁴⁴
- **Privacy and intercultural literacy** which relate to developing standards on the right to privacy and a broader understanding of how communications interact with individual identity and social developments.⁴⁵

The EU’s [Digital Education Action Plan \(2021-2027\)](#) also emphasises the importance of developing digital competencies and skills among learners, both in formal and non-formal education settings.⁴⁶ Additionally, the [Digital Competence Framework for Citizens](#), formulated by the European Commission, outlines a comprehensive set of skills essential for all learners, spanning information and data literacy, digital content creation, online safety, and well-being.⁴⁷

Media literacy programmes in countries such as Sweden aim to strengthen citizen resilience against disinformation and propaganda, highlighting the significance of media literacy in combating disinformation.⁴⁸

4.2. *Litigation where justifiable limitations exist*

The International Covenant on Civil and Political Rights ([ICCPR](#)) provides in Article 20 that “[a]ny propaganda for war shall be prohibited by law” and that “[a]ny advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law.”

In addition, Article 4(a) of the International Convention on the Elimination of All Forms of Racial Discrimination ([CERD](#)) requires that the dissemination of ideas based on racial superiority or hatred, incitement to racial discrimination, as well as all acts of violence or incitement to such acts against any race or group of persons of another colour or ethnic origin, must be declared an offence that is punishable by law.

Article 10(2) of the European Convention on Human Rights ([ECHR](#)) guarantees freedom of expression but acknowledges limitations in cases where expressions contribute to social harm. The provision states that:

[freedom of expression] may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence or for maintaining the authority and impartiality of the judiciary.

⁴⁴ Above n 1 p. 47.

⁴⁵ Above n 1 p. 70.

⁴⁶ European Commission, ‘Digital Education Action Plan (2021-2027) (accessible [here](#)).

⁴⁷ European Commission, ‘DigComp 2.2: The Digital Competence Framework for Citizens - With new examples of knowledge, skills and attitudes’ (2022) (accessible [here](#)).

⁴⁸ European Committee of the Regions, ‘Developing a handbook on good practice in countering disinformation at local and regional level’ (2022) at p. 29 (accessible [here](#)).

Efforts to regulate and prohibit misinformation and disinformation continue restrictions on expression, which must, therefore, align with the general requirements on legitimate aims, necessity and proportionality, and serve specific objectives outlined in human rights instruments. Where mis- or disinformation might amount to hate speech, terrorist content, or other forms of speech that can be legitimately prohibited, the relevant provisions under international and regional law will apply.

In instances where misinformation is so egregious that it meets the definitional elements of hate speech, litigation may be a useful and important tool in the protection and promotion of fundamental rights, including the right to equality and dignity.⁴⁹ However, such litigation should be fully considered for unintended consequences and the possibility of jurisprudence which may negatively impact freedom of expression. Depending on the content of the speech and the harm that it causes, the publication of counter-narratives may constitute a useful complementary strategy to litigation.

4.3. **Fact-checking and social media verification**

Alongside MIL strategies and campaigns and litigating misinformation that constitutes hate speech, another effective tool to combat misinformation is fact-checking and social media verification. According to the [Duke Reporters' Lab](#), there are around 125 fact-checking projects debunking false news and misinformation in 37 European countries as of 2023.⁵⁰ In addition, the [European Digital Media Observatory](#), which presents a map with the names and locations of all of Europe's fact-checking organisations, demonstrates a considerable number of organisations dedicated to fact-checking information disseminated online.⁵¹

Fact-checking and verification processes are not new, and were first introduced by US weekly magazines such as *Time* in the 1920s.⁵² However, they have had to adapt to the dynamic online environment and changing trends in the information ecosystem. In general, fact-checking efforts within newsrooms consist of:

- **Ex-ante fact-checking and verification:** increasingly and due to shrinking newsroom budgets, ex-ante (or before the event) fact-checking is reserved for more prominent and established newsrooms and publications that employ dedicated fact-checkers.⁵³
- **Ex-post fact-checking, verification and “debunking:”** this method of fact-checking is becoming increasingly popular and focuses on information published after the fact. It concentrates “primarily (but not exclusively) on political ads, campaign speeches and political party manifestos” and seeks to make politicians and other public figures accountable for the truthfulness of their statements.⁵⁴ Debunking is a subset of fact-

⁴⁹ For a useful discussion on the balancing of rights see Judith Geldenhuys and Michelle Kelly-Louw, 'Hate Speech and Racist Slurs in the South African Context: Where to Start?' (2020) 23 *PER* 12 (accessible [here](#)).

⁵⁰ Duke Reporters' Lab, 'Browse Fact-Checking' (2020) (accessible [here](#)).

⁵¹ European Digital Media Observatory, 'Map of Fact-checking Activities in Europe' (accessible [here](#)).

⁵² Above n 1 at p. 81.

⁵³ *Id.*

⁵⁴ Above n 1 at p. 82.

checking and requires a specific set of verification skills, increasingly in relation to user-generated content on social media platforms.

Fact-checking is central to strategies to combat misinformation and has grown exponentially in recent years due to the increasing spread of false news of misinformation and the need to debunk viral hoaxes.

Regulatory measures concerning journalism and media also play a pivotal role in effectively countering misinformation.⁵⁵ Media self-regulatory bodies use established rules on objectivity, honesty, accuracy, fairness, and rigour of information to deal with disinformation cases.⁵⁶ Examples from different countries, such as Germany, Latvia, Denmark, and Sweden, demonstrate how these jurisdictions deal with factual accuracy, ethical reporting, and correction of erroneous information in media publications.⁵⁷

5. PROPAGANDA

Unlike dis- and misinformation, the spread of propaganda is expressly prohibited in international law, provided that it propagates for war or advocacy of hatred that constitutes incitement.⁵⁸ In these instances, multiple direct legal remedies such as criminal prosecutions and interdictory or injunctive relief may result. However, propaganda does not often meet these thresholds. In these instances, MIL strategies and campaigns and fact-checking, coupled with the publication of counter-narratives or counter-disinformation, are effective remedies.⁵⁹

EU strategy against propaganda

The EU's strategy against propaganda involves three key components: identification, removal, and countering without engaging in counter-propaganda.⁶⁰

1. **Identification:** The EU acts as a coordination platform between Member States, encouraging information sharing and best practices exchange. Europol established a specialised unit in 2015 ([EU IRU](#)) to combat terrorist propaganda online, aiming to detect and track such content.
2. **Content removal:** [Regulation 2021/784](#) has been implemented compelling internet platforms operating in the EU to swiftly remove terrorist content upon authorities' injunctions, preventing its dissemination. Notably, this regulation applies to platforms regardless of their headquarters location.

⁵⁵ Above n 5 at p. 41.

⁵⁶ *Id.*

⁵⁷ Above n 5 at p. 42.

⁵⁸ Article 20 of the ICCPR, read with Article 4(a) of CERD.

⁵⁹ See, for example, the UK Government Communications Services, 'RESIST: Counter-disinformation toolkit' (accessible [here](#)).

⁶⁰ Marie Robin, 'European Policies in the fight to counter propaganda' (2023) *The Research and Studies Centre on Europe* (accessible [here](#)).

3. **Countering Propaganda** The EU emphasises training citizens to resist biased information and supports good-quality journalism and independent media. Platforms such as the Radicalisation Awareness Network ([RAN](#)) focus on producing alternative communications to counter extremist propaganda.

6. CONCLUSION

False news, comprising disinformation, misinformation, and mal-information, poses complex challenges in today's digital realm. Addressing these requires multifaceted approaches. Media and Information Literacy (MIL) strategies, encompassing human rights, media literacy, and privacy awareness, serve as pivotal tools. Complementing this, fact-checking, social media verification, and counter-narratives aid in debunking false content. While legal measures exist, such as litigation for hate speech instances, caution must be exercised to prevent unintended consequences and prevent the stifling of the right to freedom of expression. By combining educational, technological, and legal strategies, combating false news becomes an ongoing endeavour vital to safeguarding the integrity of information dissemination.

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.

Module 7

Defamation and Reputation

*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.....	1
1.1. What is Defamation	1
1.2. Criminal Defamation	2
1.3. Civil Defamation	3
1.4. Can a true statement be defamatory?.....	4
1.5. The Right to Reputation.....	6
1.6. What is the right way to deal with defamation?	7
1.7. Remedies	7
2. TYPES OF DEFAMATORY MATERIAL	10
2.1. Opinion versus fact.....	10
2.2. Humour.....	11
2.3. Statements of others.....	12
2.4. Privileged statements	12
2.5. Whose burden of proof?	13
3. STRATEGIC LITIGATION AGAINST PUBLIC PARTICIPATION.....	13
3.1. SLAPP Suits.....	13
3.2. Insult Laws	15
3.3. Abuse of process.....	16
4. CONCLUSION	17

MODULE 7

1. INTRODUCTION

Defamation is a notorious tactic used to suppress freedom of expression, notably affecting journalists. While defamation laws intend to safeguard individuals from public statements that could tarnish their reputation or dignity, they frequently clash with the right to free expression entrenched in multiple international and domestic legal frameworks. It is, thus, important that a balance is struck between safeguarding fundamental rights and shielding individuals from detrimental statements in terms of legitimate defamation claims.

Europe has witnessed a surge in online defamation cases in recent years due to the ease of posting content on social media platforms and the internet, often without the same level of scrutiny applied in traditional media. Coupled with a lack of comprehensive legislative frameworks addressing online defamation in many countries, this has led to an increase in defamation cases and a degree of uncertainty in applying defamation laws to the online realm.

Navigating online defamation cases poses unique challenges. The internet, lacking clear internationally recognised boundaries, complicates the identification of perpetrators. Moreover, determining the jurisdiction to adjudicate the matter becomes intricate as messages can originate from diverse global locations, involving parties scattered across different jurisdictions.

This module examines defamation laws in Europe and explores recent jurisprudence in which courts strive to strike a balance between conflicting rights. Additionally, it delves into emerging trends and examples specific to Europe, showcasing the evolving landscape of defamation law in the digital era.

1.1. What is Defamation

Definition of defamation

Defamation is a false statement of fact that is harmful to someone's reputation and published "with fault", meaning as a result of negligence or malice.¹

The law of defamation dates back to the Roman Empire, but while the penalties and costs attached to defamation today are not as serious as they once were, they can still have a notorious "chilling effect," with imprisonment or massive compensation awards posing a serious risk to freedom of expression, journalistic freedom, and dissent in many countries.

The foundation for defamation in international law is Article 17 of the International Covenant on Civil and Political Rights ([ICCPR](#)), which protects against unlawful attacks on a person's honour and reputation. Article 19(3) of the ICCPR also refers to the rights and reputation of

¹ Electronic Frontier Foundation, 'Online Defamation Law' (accessible [here](#)).

others as a legitimate ground for limitation of the right to freedom of expression.² Reputation is therefore the underlying basis in any claim of defamation, whether slander or libel.³

Defamation can be an important legal remedy for those who genuinely need it, but it can also be a weapon to quash dissent. There are many real examples where defamation may provide an important defence, for example in the non-consensual distribution of intimate images, a growing trend in the online era that disproportionately affects women. In these cases, defamation may provide recourse for women seeking justice for the non-consensual sharing of images.

However, defamation is also frequently misused, particularly by states and powerful private individuals to stifle free speech, as well as by non-state actors in the context of Strategic Litigation against Public Participation (SLAPP) suits (which will be further discussed in this module).

1.2. Criminal Defamation

Historically, defamation was usually a criminal offence. While some countries still have the offence of criminal defamation on their statute books, it is widely opposed, most notably by the [United Nations](#), the European Union (EU), and the [Council of Europe](#), who have urged states to decriminalise defamation claims to protect the rights to freedom of speech and expression.⁴ For instance, the UN Human Rights Council ([UNHRC](#)) [General Comment No. 34](#) provides that: “States Parties should consider the decriminalisation of defamation and, in any case, the application of the criminal law should only be countenanced in the most serious of cases and imprisonment is never an appropriate penalty.”⁵

In 2007, the [Parliamentary Assembly of the Council of Europe](#) affirmed its commitment to advocate for the decriminalisation of defamation in [Resolution 1577](#) towards the decriminalisation of defamation and the corresponding [Recommendation 1814](#).⁶ The Parliamentary Assembly urged member states of the Council of Europe to promptly eliminate imprisonment for defamation, prevent the misuse of criminal proceedings for defamation, preserve the independence of prosecutors in such cases, precisely define defamation in legislation to avoid arbitrary application and ensure effective civil law protection for the dignity of individuals affected by defamation.⁷

Within the region, currently, only Ireland, Romania, Estonia, the United Kingdom, Ukraine, Norway, Moldova, Macedonia, and Montenegro have completely decriminalised defamation

² International Covenant on Civil and Political Right, 23 March 1976.

³ For a fuller discussion on the law on defamation, see the training manual published by Media Defence on the principles of freedom of expression under international law: Richard Carver, ‘Training manual on international and comparative media and freedom of expression law’, MLDI at pp. 48-64 (2018) (accessible [here](#)). See Vaughan, ‘What’s the difference between libel and slander?’ (accessible [here](#)) for the definitions of libel and slander.

⁴ Human Rights Council, ‘General Comment No. 34’ (2011) (CCPR/C/GC/34 (accessible [here](#)); Council of Europe, ‘Defamation,’ (accessible [here](#)).

⁵ Id.

⁶ Parliamentary Assembly, ‘Towards decriminalisation of defamation’ (2007) Resolution 1577 at para 17.

⁷ Id.

against private persons, although many of these countries still criminalise libel and slanderous statements against the state, state officials, and/or its armed forces.⁸ Bulgaria's Justice Ministry has proposed amendments to its [Penal Code](#) which would replace criminal liability for defamation with an administrative penalty.⁹ In May 2023, the Hungarian Parliament also voted to partially decriminalise defamation committed by members of the press under certain circumstances.¹⁰

Protections against criminal defamation laws

When a criminal defamation law remains enforced, several safeguards should be in place to prevent defamation from being used to stifle freedom of speech and expression:

- The criminal standard of proof — beyond a reasonable doubt — should be fully satisfied.¹¹
- Criminal sanctions should be implemented by states to preserve public order, not to safeguard reputations, especially where the statements made are true.¹²
- It must be ensured that individuals accused of defamation have adequate means for their defence under the law, especially methods that involve verifying the accuracy of their statements whilst considering the broader public interest.¹³
- Penalties should not include imprisonment, nor should they enforce damages that are disproportionate to the injury suffered.¹⁴
- As a less restrictive means, states should not resort to criminal law when a civil law alternative is readily available.¹⁵

1.3. Civil Defamation

Despite widespread agreement that criminal punishment for defamation is no longer acceptable in a democratic society, there is nevertheless a need for some sort of remedy for those who have faced injury to their reputation and dignity following the dissemination of false and damaging statements. If a person is able to prove a civil claim for defamation, and the person responsible for the statement or publication is not able to successfully raise a defence,

⁸ Scott Griffen, 'Defamation Law in the European Union: A Comparative Overview for Journalists, Civil Society and Policymakers' (2015) p. 6 (accessible [here](#)); European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 2023 Communication on EU Enlargement policy' (2023) at p. 44 (accessible [here](#)); Danielsen, 'Defamation and Privacy Law in Norway' *Norway Media Guide* (accessible [here](#)).

⁹ Gigov, 'Justice Ministry proposes less severe penal sanctions for defamation' (2022) (accessible [here](#)).

¹⁰ Committee to Protect Journalists, 'CPJ welcomes Hungary vote to partially decriminalize defamation' (2023) (accessible [here](#)).

¹¹ Inter-American Court of Human Rights, *Kimel v Argentina*, (2008) (accessible [here](#)).

¹² *Castells v Spain* App No 11798/85, A/236, (1992) 14 EHRR 445, IHRL 2936 (ECHR 1992) at para 38.

¹³ *Id.*

¹⁴ Above n 6.

¹⁵ See for example: European Court of Human Rights, *Amorim Giestas and Jesus Costa Bordalo v. Portugal*, Application No. 37840/10 (2014) at para 36 (accessible [here](#) in French).

the person who has suffered reputational harm is typically entitled to monetary compensation in the form of civil damages. While civil defamation claims may serve the intended purpose of restoring reputation or honour, they can be misused and cause a “chilling effect” on the full enjoyment and exercise of freedom of expression.

Safeguards should, thus, equally be applied when addressing civil defamation matters to ensure that administrative remedies are not similarly used to stifle freedom of speech and expression. The Parliamentary Assembly of the Council of Europe has called on Member States to establish reasonable and proportionate maximum amounts for damages and interest in defamation cases to safeguard the viability of media defendants and provide legal safeguards against disproportionate awards.¹⁶

Libel tourism

Libel tourism is the practice of filing defamation lawsuits in jurisdictions that are deemed likely to provide favourable judgments, often chosen based on legal fees being contingent on the outcome (“no win, no fee”) or the potential cost of the legal process acting as a deterrent to the defendant. It is a cause for concern as it can be misused to intimidate and silence the media, journalists, and academics, particularly those critical or investigative in nature.¹⁷

In 2012, the Council of Europe adopted a [Declaration](#) addressing libel tourism which states that:

The prevention of libel tourism should be part of the reform of the legislation on libel/defamation in member States in order to ensure better protection of the freedom of expression and information within a system that strikes a balance between competing human rights... Further, if there is a lack of clear rules as to the applicable law and indicators for the determination of the personal and subject matter jurisdiction, such rules should be created to enhance legal predictability and certainty, in line with the requirements set out in the case law of the Court. Finally, clear rules as to the proportionality of damages in defamation cases are highly desirable.¹⁸

1.4. Can a true statement be defamatory?

In most states in Europe, truth is generally a defence for defamatory statements, with some exceptions.¹⁹ The ECtHR has held that truth is an absolute defence to a suit of defamation, provided that it can be proved.²⁰ If a factual statement can be proven to be true, it cannot be

¹⁶ Parliamentary Assembly, ‘Towards decriminalisation of defamation’ (2007) Resolution 1577 para 17.

¹⁷ Above n 18 at paras 5-10.

¹⁸ Council of Europe, ‘Declaration of the Committee of Ministers on the Desirability of International Standards Dealing with Forum Shopping in Respect of Defamation, “Libel tourism” To Ensure Freedom of Expression’ (2012) at paras 11-12 (accessible [here](#)).

¹⁹ Above n 8 at p. 8.

²⁰ Tarlach McGonagle, ‘Freedom of Expression and Defamation: A study of the case law of the European Court of Human Rights,’ Council of Europe (2016) (accessible [here](#)) at p. 43.

See, for example, [Bergens Tidende and Others v Norway](#) (2001).

defamatory, and the defendant will generally be absolved of liability.²¹ It follows naturally that any practices that unreasonably restrict the ability of defendants to establish the truth of their allegations should be avoided.²²

This is bolstered by [General Comment No. 34, which](#) states that “all such laws including penal defamation laws, should include defences such as the defence of truth.”²³

This principle arises from the notion that an individual's reputation should be based on truth, not on false or undeserved grounds. Although accuracy in reporting facts is crucial, in journalistic scenarios, especially during breaking news, absolute accuracy may be challenging, requiring some flexibility.²⁴ In [Observer and Guardian v the United Kingdom](#) (1991), the European Court of Human Rights (ECtHR) acknowledged the time-sensitive nature of news and the potential loss of its value if publication is delayed.²⁵ In this regard it is relevant and important that journalistic practices integrate fact-checking procedures, encouraging access to credible sources and documents that could serve as evidence in potential defamation claims.²⁶

The defence of truth applies solely to ascertainable facts, as statements of opinion or value judgments are not subject to factual proof.²⁷

Untrue statements

On the other hand, a statement that cannot be proven to be true should not always be automatically considered defamatory, as it depends on whether it was made in good faith, without intent to defame, or whether it may be covered by other possible defences such as reasonable publication.

General Comment No. 34 states that:

At least with regard to comments about public figures, consideration should be given to avoiding penalising or otherwise rendering unlawful untrue statements that have been published in error but without malice...[A] public interest in the subject matter of the criticism should be recognised as a defence.²⁸

The importance of truth is discussed in the case of [Kosova and Apostolov v North Macedonia](#) (2022) in the ECtHR, which held that North Macedonia violated the applicant's freedom of expression when its domestic courts found against the editor-in-chief of a weekly magazine and a journalist in a civil defamation suit, holding that the articles published were

²¹ Article 19, ‘Defining Defamation: Principles on Freedom of Expression and Protection of Reputation’ Principle 7 (accessible [here](#)).

²² *Id.*

²³ Above n 5 at p. 12.

²⁴ *Id.*

²⁵ *Observer and Guardian v United Kingdom, The Observer Ltd and ors and ‘Article 19’ (the International Centre against Censorship) (intervening) v United Kingdom* (Application no. 13585/88) (1992) para 60.

²⁶ Above n 8 at p. 44.

²⁷ *Id.*

²⁸ Above n 5.

of public interest capable of contributing to public debate and that the journalists could not be criticised for failing to ascertain the truth of the statements which emanated from a source. It also criticised the large amount of the award for having a chilling effect on the media.

As is implicit above, the element of truth is closely related to that of the public interest. In the case of [Udovychenko v Ukraine](#) (2023), the ECtHR discussed the public interest in the context of a woman who had given a witness statement to police implicating certain individuals in a road accident. She was subsequently sued by those individuals for defamation, with the domestic courts finding against her. The ECtHR held that the penalties imposed were disproportionate because her statement related to a matter of public interest and she had acted in good faith in making it.

1.5. The Right to Reputation

The right to protection against attacks on reputation is firmly established in international law. Article 12 of the [Universal Declaration of Human Rights](#) provides that: “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”²⁹ This is echoed in identical words in Article 17 of the ICCPR which states that: “No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.”³⁰

This is mirrored within the European system in Article 8 of the European Convention on Human Rights ([ECHR](#)), which protects the right to respect for private and family life, read with Article 10(2) which provides that the right to freedom of expression may be constrained for the protection of the reputation of others.

However, as indicated, a balance often needs to be found between offending statements which constitute an attack on a person’s reputation and the justifiable limitations on the right to freedom of expression and any associated rights.

²⁹ UN General Assembly, ‘Universal Declaration of Human Rights, Resolution 217 A (III)’ (1948) ([accessible here](#)).

³⁰ Article 17(1) of the ICCPR.

A balancing act

When examining the necessity of an interference in a democratic society in the interests of the 'protection of the reputation or rights of others', the Court may be required to verify whether the domestic authorities struck a fair balance when protecting two values guaranteed by the Convention which may come into conflict with each other in certain cases, namely, on the one hand, freedom of expression protected by Article 10 and, on the other, the right to respect for private life enshrined in Article 8.³¹

1.6. What is the right way to deal with defamation?

When a person is found to have been defamed, they are entitled to a remedy. However, the remedies imposed are often punitive and disproportionate. We have already seen that sentences of imprisonment for criminal defamation are widely regarded as disproportionate due to their impact on freedom of expression.³² Heavy fines have also been subject to scrutiny by the courts as a disproportional and unjustifiable restriction of the right to freedom of expression.

Whenever possible, redress in defamation cases should, therefore, be non-pecuniary (non-financial) and aimed directly at remedying the wrong caused by the defamatory statement, such as through publishing an apology or correction.

Monetary awards — the payment of damages — should only be considered when other less intrusive means are insufficient to redress the harm caused. Compensation for harm caused (pecuniary damages) should be based on evidence quantifying the harm and demonstrating a causal relationship with the alleged defamatory statement.

1.7. Remedies

The following remedies apply to civil defamation matters:

Damages

In, *Tolstoy Miloslavsky v the United Kingdom* (1995), the ECtHR determined that compensation for defamation should reasonably relate to the harm caused to one's reputation.³³ Other factors that could influence the proportionality of damages and fines are the inclusion of "success fees" for legal teams, the potential threat to the economic stability of the applicant company, or the risk of closing a media outlet.³⁴ For example, in *Timpul Info-Magazin and Anghel v Moldova* (2008), a severe fine resulted in the closure of a newspaper, which the ECtHR acknowledged could suppress open discussion on matters of public concern, essentially silencing a dissenting voice.³⁵

³¹ *Axel Springer AG v Germany*, judgment of the Grand Chamber of the ECtHR (2012) at paras 83-84 (accessible [here](#)).

³² Above n 5.

³³ *Tolstoy Miloslavsky v United Kingdom* (1995) 20 EHRR 442 at para 69 (accessible [here](#)).

³⁴ Tarlach McGonagle, 'Freedom of expression and defamation: A study of the case law of the European Court of Human Rights' (2016) at pp. 51-52 (accessible [here](#)).

³⁵ *Timpul De Dimineata v Moldova* App no.16674/06 (2006) (accessible [here](#)).

Further, the proportionality of civil damages should not be solely evaluated in monetary terms. In *Reznik v Russia* (2013), despite a negligible monetary penalty of 20 Russian roubles, the initiation of defamation proceedings against the President of the Moscow City Bar was deemed capable of significantly chilling his freedom of expression due to the importance of his position.³⁶

Public apology

This remedy encourages defendants to show acknowledgement and to be accountable, making it a better-suited remedy to address the emotional requirements of offended parties compared to monetary compensations.³⁷ Consequently, apologies could foster a sense of reconciliation in strained relationships and prompt forgiveness from the victims, thereby facilitating a healing process.³⁸

Right to reply

The right of reply stems from the necessity to contest misleading information and ensure a diversity of viewpoints, particularly in areas of broad interest such as literature and politics.³⁹ In *Melnychuk v Ukraine* (2005), a newspaper declined to publish an author's reply to a critical book review, citing the inclusion of "vulgar and offensive language" about the reviewer. Despite communicating the reasons for refusal and offering the opportunity to edit the response, the applicant declined. The ECtHR highlighted that the right to freedom of expression does not grant unrestricted access to media for airing opinions and that:

Newspapers and other privately owned media must be free to exercise editorial discretion in deciding whether to publish articles, comments and letters submitted by private individuals. However, there may be exceptional circumstances in which a newspaper may legitimately be required to publish, for example, a retraction, an apology or a judgment in a defamation case.⁴⁰

Injunction

Injunctions play a crucial role in regulating or restricting certain activities, often related to the publication or dissemination of allegedly defamatory material. An injunction, in this context, is a court order that prohibits an individual or entity from publishing or further disseminating specific information deemed defamatory.⁴¹

These injunctions might take different forms:

- **Interim Injunctions:** These are provisional measures issued during the early stages of legal proceedings and are aimed at preventing imminent harm or maintaining the status quo until the case is resolved.⁴²

³⁶ *Reznik v Russia* -4977/05 (2013) (accessible [here](#)).

³⁷ Wannes Vandebussche, 'Rethinking non-pecuniary remedies for defamation: The case for court-ordered apologies' (2021) *Journal of International Media & Entertainment Law* 155 (accessible [here](#)).

³⁸ *Id.*

³⁹ Above n 34 at p. 53.

⁴⁰ *Melnychuk v Ukraine* (App no 28743/03) (2001) p. 6 (accessible [here](#)).

⁴¹ David Adria, 'Freedom of speech, defamation, and injunctions' (2013) 55(1) *William & Mary Law Review* 6-7 (accessible [here](#)).

⁴² Above n 34 at pp. 54-55.

- **Permanent Injunctions:** These are issued as part of the final judgment in a defamation case and prohibit certain actions permanently, such as prohibiting the continued publication or dissemination of defamatory material. They are typically issued after the court has determined that the material in question is indeed defamatory.⁴³

Courts must strike a balance between protecting an individual's reputation and ensuring the right to freedom of expression.⁴⁴ This balance is crucial in determining the proportionality of the injunctions issued in defamation cases. Courts often assess whether the injunctions imposed are necessary and proportionate to the harm caused by the alleged defamation, ensuring they do not unduly restrict freedom of speech.

Recent defamation matter against journalist

On 2 May 2023, the Court of General Jurisdiction in Yerevan, Armenia, issued an order to freeze assets amounting to 9 million Dram (€21,890) belonging to journalist Davit Sargsyan and his publisher employer, 168 Hours.⁴⁵ This followed a civil defamation lawsuit filed by Yerevan's Deputy Mayor, Tigran Avinyan, in response to a video report released by Sargsyan on 5 February 2023. The report alleged a steady increase in Avinyan's family wealth through political influence since Prime Minister Nikol Pashinyan's assumption of power in 2018. Avinyan contested the assertion that these facts amounted to corruption, although he did not challenge their accuracy.

Sargsyan defended his report on Facebook, stating that he based his claims on previously published materials that Avinyan had not earlier refuted and that he believed the lawsuit aimed to silence him by inflicting substantial financial harm. Head of the Committee to Protect Freedom of Speech, Ashot Melikyan, noted that this marked the first instance where a media outlet faced the maximum 9 million Dram penalty following legal amendments that tripled the fines for insult and defamation in 2021. Aramazd Kiviryan, a lawyer representing 168 Hours, expressed concern over the freeze, highlighting its significant impact on the outlet's operations and noting that while it intended to petition for the freeze's removal, its continuation until the court's final verdict, which might take years, posed a substantial challenge.

On 16 May 2023, Avinyan's lawyer announced an application to lift the freeze, clarifying that their intent was not to bankrupt any media outlet or create financial hardships. However, the substantive proceedings are ongoing.

The case comes in the midst of a rising number of lawsuits filed against journalists and the media in Armenia based on insult and defamation.⁴⁶

⁴³ Above n 34 at p. 55.

⁴⁴ Dominika Bychawska-Siniarska, *A handbook for legal practitioners* (2017) at p. 44 (accessible [here](#)).

⁴⁵ More insight on the matter is accessible at Safety of Journalists Platform, 'Assets of Journalist Davit Sargsyan and Outlet 168 Hours Frozen in Defamation Proceedings' (accessible [here](#)).

⁴⁶ Marianna Danielyan, 'The Number Of Lawsuits Against Journalists In Armenia Has Increased,' *media.am* (2023) (accessible [here](#)).

2. TYPES OF DEFAMATORY MATERIAL

2.1. *Opinion versus fact*

We have addressed factual statements that may be defamatory. However, it is important to differentiate expressions of opinion from factual statements. [General Comment No. 34](#) states that defamation laws, particularly penal defamation laws, “should not be applied with regard to those forms of expression that are not, of their nature, subject to verification,”⁴⁷ such as opinions and value judgments. It also notes that “[a]ll forms of opinion are protected, including opinions of a political, scientific, historic, moral or religious nature.”

To distinguish fact from opinion, the following should be considered:⁴⁸

- **Statements of facts:** Statements claiming facts need to be proven true by the author or publisher in court, while opinions require a demonstration of a sufficient factual basis.
- **Verifiability:** Facts are objectively verifiable information, and if challenged as false, the burden lies on the speaker to prove their accuracy. Opinions, on the other hand, are subjective viewpoints based on available information. They cannot be objectively proven as true or false. However, critical opinions should have some basis in reality. The level of factual basis varies with the seriousness of the allegation. Severe claims demand more robust and reliable factual support.

Opinions are generally protected under the defence of “honest comment” or “fair comment,” allowing individuals to express their views on matters of public interest, even if those opinions are strong or biased.⁴⁹ However, when statements are presented as factual assertions and are proven false, leading to harm or damage to someone’s reputation, they can be subject to defamation claims.

The requirements for an honest comment defence were outlined by the United Kingdom Supreme Court in [Spiller v Joseph](#) (2010) which identified the requirements as follows:⁵⁰

1. The comment must be on a matter of public interest.
2. The comment must be recognisable as comment, as distinct from an imputation of fact.
3. The comment must be based on facts that are true or protected by privilege.
4. The comment must explicitly or implicitly indicate, at least in general terms, the facts on which it is based.
5. The comment must be one which could have been made by an honest person, however prejudiced he might be, and however exaggerated or obstinate his views.
6. The comment must not have been published maliciously.

⁴⁷ Above n 5 at p. 12.

⁴⁸ Human Rights Guide, ‘Distinction: fact or opinion’ (accessible [here](#)).

⁴⁹ Withersworldwide, ‘Social network activities and their legal implications in the EU: defamation and data protection’ (2021) (accessible [here](#)).

⁵⁰ [2010] UKSC 53 at para. 83 (accessible [here](#)).

Case law analysis

In the context of the UK, the *Waterson v Lloyd and Carr* (2013) case presented a critical examination of where the line between fact and opinion lies within defamation law.⁵¹ In this case, a Member of Parliament (MP) initiated a libel claim against the Eastbourne Liberal Democrats, due to the distribution of two campaign newsletters during the 2010 General Election. These newsletters, designed to resemble local newspapers, labelled the MP as an “Expenses Scandal” MP both in headlines and internal articles. The Eastbourne Liberal Democrats defended their actions by invoking the defence of honest comment, asserting that the statements were expressions of opinion rather than factual allegations.

Two of the judges in the England and Wales Court of Appeal viewed the statements made as expressions of opinion or comment, emphasising that they primarily centred on the MP's expense claims without expressly insinuating any unlawful behaviour. One dissenting judge argued for a clearer distinction between broader MP expense scandals and the specific facts of the MP's claims. This dissent underscored the potential impact of language nuances in differentiating between statements of fact and expressions of opinion within defamation cases.

The case highlighted the ongoing challenge in defamation law regarding the demarcation between factual assertions and opinions or comments, particularly in the politically charged arena.

2.2. Humour

The ECtHR has held that satire is “a form of artistic expression and social commentary and, by its inherent features of exaggeration and distortion of reality, naturally aims to provoke and agitate.”⁵² While humour, especially satire, is recognised as a form of expression and social commentary deserving protection, its subjective and elusive nature makes drawing a clear line between harmful speech and protected expression challenging.⁵³

In the case of *Petrina v Romania* (2008), the ECtHR found that allegations broadcast on a television programme and in a humorous magazine had violated the subject's freedom of expression because, although the publication was satirical in nature, the articles themselves had been liable to offend the applicant as they had no factual basis, and because they directly concerned him in his personal rather than professional capacity, resulting in speech that overstepped the boundaries of reasonableness.⁵⁴ In contrast, in *Sousa Goucha v Portugal* (2004), the Applicant, an openly gay TV host, filed a complaint for defamation and insult after he was described in a television comedy show as “The best Portuguese female TV host.”⁵⁵ The

⁵¹ [2013] EWCA Civ 136 [2013] EMLR 17 (accessible [here](#)).

⁵² *Vereinigung Bildender Künstler v Austria* (2007) 68354/01 at para 33 (accessible [here](#)).

⁵³ Alberto Godioli and others, ‘Laughing Matters: Humor, Free Speech and Hate Speech at the European Court of Human Rights’ (2022) 35 *International Journal of Semiotics of Law* 2242 (accessible [here](#)).

⁵⁴ European Court of Human Rights, ‘Factsheet: Protection of reputation,’ (2023) (accessible [here](#)).

⁵⁵ Application No 36109/03 (2008) (accessible [here](#)).

ECtHR held that there had been a fair balance between the Applicant's right to protection of his reputation and the media's right to freedom of expression and found no violation of the Applicant's rights.

The matter of *Nikowitz and Verlagsgruppe News GmbH v Austria* (2007) provides further guidance from the ECtHR on the pertinent characteristics of a satirical article in the context of a defamation suit.

2.3. Statements of others

A point of consideration, particularly for journalists, is the extent to which they are liable for the potentially defamatory statements of others since a central part of their work is reporting on the words of others. The ECtHR has found that a journalist is not automatically liable for the opinions stated by others and is not required to "systematically and formally" distance themselves from "the content of a statement that might defame or harm a third party,"⁵⁶ provided they have not repeated potentially defamatory statements as their own, endorsed, or agreed with them.

Principle 15 of the *Principles on Freedom of Expression and Protection of Reputation* notes that "individuals should not face legal responsibility for accurately reporting the statements of others" and "no one should be held accountable under defamation laws for a statement they did not create, edit, or publish, and when they had no knowledge or reason to believe that their actions contributed to spreading a defamatory or otherwise unlawful statement."⁵⁷

With increased social media use, it is notable that individuals may, however, be responsible for statements made by others if they actively participate in or endorse the publication of defamatory content.

2.4. Privileged statements

Privileged statements are those reported from places which are covered by different forms of privilege. For example, statements reported from legislative or judicial proceedings typically have absolute privilege. This means that neither the statement's author nor the media reporting it can be held liable for defamation. Some other types of statements reported from public meetings, documents, or materials in the public domain may also enjoy qualified privilege.

Absolute privilege grants individuals the clear right to make statements in certain situations, regardless of their truth or intent.⁵⁸ However, the same statement by the same person may be protected by absolute privilege in one context and not in another.⁵⁹ For instance, a defamatory statement made during testimony at a trial would be absolutely privileged, while the same statement made outside the trial could lead to a successful defamation lawsuit.

⁵⁶ *Nenkova-Lalova v Bulgaria* Application No. 35745/05 (2012) (accessible [here](#)).

⁵⁷ Article 19, 'Defining Defamation: Principles on Freedom of Expression and Protection of Reputation' (2017) (accessible [here](#)).

⁵⁸ Charles Crain, 'Privileges and Defenses in Defamation Cases' (accessible [here](#)).

⁵⁹ *Id.*

Other forms of communication also fall under qualified privilege. This privilege protects those acting in good faith who make statements to fulfil a duty or serve a positive purpose and may apply to other fora such as other legislative bodies and quasi-judicial institutions.⁶⁰ Unlike absolute privilege, qualified privilege does not shield individuals if they abuse it.⁶¹

Case law on privilege

- *Keller v Hungary* (2006): In declaring the application inadmissible, the ECtHR stated that the public insinuations made against a minister did not benefit from the privilege afforded to parliamentary debate because some of them were made outside of Parliament itself.
- *Reynolds v Times Newspapers* (1999): the Judicial Committee of the House of Lords in the UK dismissed an appeal in a defamation case, holding that although the defence of qualified privilege is available to the media, there is no generic defence for the communication of political information, and defined what has come to be known as the “Reynolds test.”
- *Gordon v The Irish Race Horse Trainers Association* (2020): the High Court of Ireland elaborated on the defence of qualified privilege and when it is defeated by express malice.

2.5. Whose burden of proof?

A general principle of law is that the burden of proof lies with the person who brings the suit or makes the “claim.” However, with defamation, this principle is generally reversed, and the responsibility lies with the defendant — the person who made the allegedly defamatory statement — to prove that the statement did not damage the claimant’s reputation and would rely on one of the abovementioned grounds of justification.⁶²

3. STRATEGIC LITIGATION AGAINST PUBLIC PARTICIPATION

3.1. SLAPP Suits

Other legal methods are also increasingly used to silence critics and journalists. One such example is Strategic Lawsuits Against Public Participation (SLAPP), which aim to intentionally bury critics under expensive and often baseless legal claims to intimidate and silence them. Usually, the objective in these cases is not a positive judgment, but rather to leverage the threat of financial damage — typically against persons and organisations that cannot reasonably pay for the damages sought in the lawsuit. Libel and defamation are often used as

⁶⁰ Above n 58.

⁶¹ Id.

⁶² Council of Europe, ‘Defamation and freedom of expression’ (2003) at p. 3 (accessible [here](#)).

the underlying complaints in SLAPP suits. In Europe, the number of SLAPP suits has been steadily rising in recent years, reaching 161 in 2022.⁶³

In acknowledging these risks, in 2023, the Legal Affairs Committee of the European Parliament voted in support of new rules designed to ensure EU-wide safeguards against unjustified SLAPP suits, building on a series of existing resolutions aimed at preventing the legal harassment of journalists and activists.⁶⁴ This included broadening the definition of cross-border cases to include situations where the subject matter of the case is pertinent to more than one country and can be accessed electronically.⁶⁵ It also builds on the European Commission's existing recommendations for domestic cases that particularly address legal support for those targeted.

The proposed measures include the option for those targeted by a SLAPP to seek early dismissal of their case, placing the burden of proof on the claimant to demonstrate that their case is not blatantly unfounded.⁶⁶ Claimants would also be responsible for covering all legal expenses, while victims of SLAPPs would have the right to seek compensation for damages, including harm to their reputation and defamation cases would only be admissible in the defendant's national court.⁶⁷ On 30 November 2023, the EU Council and Parliament agreed on and passed the new directive.⁶⁸

The rise of anti-SLAPP laws

Several countries around the world have sought to address the surge of SLAPP suits against journalists and activists by passing dedicated anti-SLAPP legislation. This includes, for example, the United States, Australia, and Canada.⁶⁹ As the Reporters Committee for Freedom of the Press states:⁷⁰

Under most anti-SLAPP statutes, the person sued makes a motion to strike the case because it involves speech on a matter of public concern. The plaintiff then has the burden of showing a probability that they will prevail in the suit — meaning they must show that they have evidence that could result in a favorable verdict. If the plaintiff cannot meet this burden and the suit is dismissed through anti-SLAPP proceedings, many statutes allow defendants to collect attorney's fees from the plaintiff.

In 2023, the UK also introduced an anti-SLAPP law giving judges the power to dismiss lawsuits they deem to be attempting to silence those speaking out justifiably on economic

⁶³ The CASE, 'SLAPPs,' (accessible [here](#)).

⁶⁴ European Parliament, 'Anti-SLAPP: EU protection against legal actions that silence critical voices' 27 June 2023 (accessible [here](#)).at p. 64.

⁶⁵ *Id.*

⁶⁶ Above n 64 at p. 56.

⁶⁷ *Id.*

⁶⁸ Nathalie Weatherald, 'EU institutions strike deal on Anti-SLAPP Directive,' Euractiv (2023) (accessible [here](#)).

⁶⁹ Linda Maria Ravo and others, 'Protecting Public Watchdogs Across the EU: A Proposal for an EU Anti-SLAPP Law,' A call for action signed by multiple non-governmental organisations from across Europe (accessible [here](#)).

⁷⁰ Reporters Committee for Freedom of the Press, 'Understanding Anti-SLAPP law,' (accessible [here](#)).

crime.⁷¹ The law defines what constitutes a SLAPP and provides a cost protection scheme for cases that proceed. However, it is limited only to those covering economic crimes.

International human rights bodies have also increasingly begun to recognise SLAPPs. For example, the 2022 UN Human Rights Council Resolution on the safety of journalists made commitments acknowledging the growing risks of SLAPPs and called on governments to “take measures to protect journalists and media workers from strategic lawsuits against public participation, where appropriate, including by adopting laws and policies that prevent and/or alleviate such cases and provide support to victims.”⁷² This has also been recognised by several reports of the special mandates.⁷³

The ECtHR has made some progress toward recognising SLAPPs, including in the case of *OOO Memo v Russia* (2022), in which it explicitly referred to “the growing awareness of the risks that court proceedings instituted with a view to limiting public participation bring for democracy.”

3.2. Insult Laws

Insult laws aim to safeguard the “esteem and character” of individuals, even public officials, and are, unlike defamation laws, usually oblivious to whether the statements are true.⁷⁴ Several insult laws are still at play across the continent and continue to pose risks for journalists and others critical of the government. Poland stands out as a country in which insult cases remain common, while across the rest of the continent they are rare despite remaining laws which often aim to protect heads of state.⁷⁵

Regional courts have increasingly argued that public officials should enjoy *less* protection from criticism than others. Because of their status, access to the media, and power, public officials can often use their office to try to curtail freedom of expression and prosecute critics.⁷⁶ Additional protections for those who criticise them may therefore be warranted, to counter this imbalance of power. In addition, there is a real need for those serving in public office to be open to criticism and public input. As the ECtHR has found in *Oberschlick v Austria* (1997):

A politician inevitably and knowingly lays himself open to close scrutiny of his every word and deed by both journalists and the public at large, and he must display a greater degree of tolerance, especially when he himself makes public statements that are susceptible of criticism.⁷⁷

⁷¹ Lucy Nash, ‘UK introduces first anti-SLAPP law – but critics say it doesn’t go far enough,’ The Bureau of Investigative Journalism (2023) (accessible [here](#)).

⁷² A/HRC/RES/51/9 (accessible [here](#)).

⁷³ Global Freedom of Expression: Columbia University, ‘How are courts responding to SLAPPs? Analysis of selected court decisions from across the globe,’ (2023) (accessible [here](#)) at p. 10.

⁷⁴ Joel Simon and others, ‘Weaponizing the Law: Attacks on Media Freedom’ (2023) at p. 16 (accessible [here](#)).

⁷⁵ Antonia Zimmerman, ‘European countries where insulting the head of state can land you in prison,’ Politico (2021) (accessible [here](#)).

⁷⁶ *Id.*

⁷⁷ Application No. 11662/85 (1991) at para 59 (accessible [here](#)).

The Office of the High Commissioner for Human Rights ([OHCHR](#)) has also called for the abolition of the offence of “defamation of the State,”⁷⁸ and some jurisdictions have refused to allow elected and other public authorities to sue for defamation.⁷⁹ The ECtHR has limited such suits to situations which threaten public order, implying that governments cannot sue in defamation simply to protect their honour.⁸⁰

3.3. Abuse of process

Lastly, those seeking to silence critics and journalists may abuse court processes to meet their objectives.⁸¹ Even when the legal framework does not offer specific safeguards against SLAPPs, there may be other legal mechanisms available for dismissing such cases.⁸² These mechanisms could include provisions addressing the “abuse of process” or prohibiting frivolous litigation.⁸³ Some courts have started to entertain defendants’ requests for case dismissals using these provisions, although their application has been inconsistent.⁸⁴

Practical steps on defamation

- **If you have been a victim or survivor of the non-consensual distribution of intimate images**, you may be able to use defamation as a remedy.
 - If you are able to show that the distribution of the images harmed your reputation, you may have success in a defamation case.
 - The challenge with using civil defamation as a remedy is that the images may technically be ‘true,’ or even taken with the victim’s consent. However, if it can be shown that there existed an associated implication about the subject of the images (e.g. that reflects on their character) which can be proven false, a defamation claim is more likely to have success.
- **If someone has posted slanderous comments about you online**, and you are also a user of the same social media platform, you may have recourse with that social media company.
 - Most social media companies have defamation reporting processes,⁸⁵ which may enable you to have the comments taken down. However, they are unlikely to provide further recourse beyond removing the offending content.
- **If you have been targeted by a SLAPP suit** that uses defamation charges to silence or intimidate you may:

⁷⁸ OHCHR, Concluding Observations of the Human Rights Committee: Serbia and Montenegro, CCPR/CO/81/SEMO (12/08/2004) at para 22 (accessible [here](#)).

⁷⁹ OHCHR, ‘Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression,’ E/CN.4/2000/63 (2000) (accessible [here](#)).

⁸⁰ *Id.*

⁸¹ Global Freedom of Expression, ‘How are courts responding to SLAPPs? Analysis of selected court decisions from across the globe,’ (2023) (accessible [here](#)).

⁸² *Id.*

⁸³ *Above n 81.*

⁸⁴ *Id.*

⁸⁵ For Facebook, see [here](#). For X (formerly ‘Twitter’), see [here](#).

- Approach a reputable public interest law firm or human rights lawyers for assistance. Sometimes, lawyers may be able to act *pro bono* (free of charge) or rely on legal defence funds for their fees.
- **If you live in a country that has defamation laws that infringe on regional and international human rights**, you may be able to do something about it:
 - Consider whether you have access to other regional or international human rights courts, such as the European Court of Human Rights or the Court of Justice of the European Union. There may be jurisprudence in your country opposing the use of disproportionate penalties for defamation.

4. CONCLUSION

While defamation laws aim to shield individuals from infringements on their rights to dignity and privacy, their frequent abuse tends to subdue and penalise dissenting voices. The ongoing shift towards decriminalising defamation signifies a progressive step but necessitates a comprehensive execution of judicial verdicts. Concurrently, the elimination of criminal penalties associated with other insult laws becomes imperative. This module has also underscored the importance of instituting legal safeguards against alternative coercive tactics such as the use of Strategic Lawsuits Against Public Participation (SLAPP) suits.

A holistic approach encompassing not only the decriminalisation of defamation but also the eradication of punitive measures, coupled with protective measures against silencing methodologies, is needed to fortify the terrain of unfettered expression and dissent.