Module 1

Digital Rights and Emerging Challenges

Modules on Digital Rights and Freedom of Expression Online in Europe

MEDIA DEFENCE

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

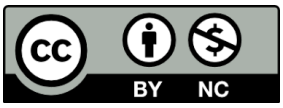

TABLE OF CONTENTS

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 Internet[10] 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] *Yıldırır 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 informatio0n 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 Shtekel 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 date 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] *Tietosuojavaltuutettu 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 Service[43] 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).