Module 3

Content Based Restrictions and Intermediary Liability

Modules on Digital Rights and Freedom of Expression Online in Europe

MEDIA DEFENCE

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

TABLE OF CONTENTS

MODULE 3

1. INTRODUCTION

Content based restrictions[1] 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 Directive[3] (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. 3.3 Providers of Hosting Services

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 Directive[18] 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* (adoptemajd 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 disapplied 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 Nimes 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. Swedena*[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).