Radboud University

The revision of the European framework for the liability and responsibilities of hosting service providers

Towards a better limitation of the dissemination of illegal content

Raphaël Gellert and Pieter Wolters

Radboud Business Law Institute

iHub

Radboud University

Date 7 April 2021
Reference 202006043
Prepared by R.M. Gellert and P.T.J. Wolters
Acknowledgements The authors would like to thank prof. dr. B.P.F. Jacobs, prof. mr. dr. F.J. Zuiderveen Borgesius, prof. mr. dr. M.I. Fedorova, dr. M. Kleemans, prof. mr. dr. A.A. Quaedvlieg, mr. M.D. Reijneveld, mr. W.Y. Hu and the steering committee of the Ministry of Economic Affairs and Climate Policy for their valuable assistance and contributions.

Relation

Digital Economy Department, Directorate Business & Innovation (B&I)
Ministry of Economic Affairs and Climate Policy
Bezuidenhoutseweg 73
P.O. BOX 20401
2500 EK The Hague
The Netherlands
T (+)31 70 379 89 11

Radboud University
Houtlaan 4
6525 XZ Nijmegen
+31 (0)24 361 61 61

P.O. Box 2345
4567 AE Nijmegen
The Netherlands
www.ru.nl/law

Table of contents

1. Introduction

1.1. Introduction

Twenty years after its creation, the European framework for the liability and responsibilities of internet intermediaries is in need of revision. This is not just a conclusion of a limited number of theoretical academics or disgruntled rights holders. It is widely shared by policy makers, academics and various kinds of stakeholders.[1] However, the opinions about *how* the framework should be revised are not as uniform. The various policy makers, academics and stakeholders suggest various solutions, representing diverging priorities and ideas about the proper role of online intermediaries in our digitalised information society.

The core of the European framework is formed by the e-Commerce Directive of 8 June 2000. This Directive, which is discussed in more depth in Chapter 2, exempts online intermediaries from liability for disseminating (either as 'mere conduit' or by 'caching' or 'hosting') illegal online content that they are unaware of. This exemption has been introduced to stimulate the development of the digitalised information society (Section 2.2.2). Free from the threat of liability, online intermediaries have thrived and developed all kinds of services. This in turn has allowed all kinds of parties, including consumers, professionals and public entities, to use the internet to disseminate information, communicate effectively and develop all kinds of (economic) activities. Consequently, it has facilitated the exercise of fundamental rights, and in particular freedom of expression and freedom of information.[2]

The increased role of online intermediaries also has downsides.[3] Content providers can use the intermediaries to effectively and anonymously disseminate various kinds of illegal content. For example, an online content-sharing service provider (such as Youtube) may host copyright-protected videos without permission from the copyright holder, an online marketplace can offer products that infringe on trademarks or facilitate vendors that perform unfair commercial practices, social media can be used to spread hate speech and a search engine could lead to websites that violate someone's privacy.

In these situations, the injured parties or victims are often left without effective redress. The 'primary' perpetrator, the person that used the intermediary to disseminate the illegal content, is often anonymous, otherwise impossible to sue or unable to pay damages.[4] The intermediary that facilitated this dissemination is exempted from liability by the e-Commerce Directive. As such, the e-Commerce Directive favours the development of the internet and the interests of intermediaries over the effective protection of victims of illegal online content.

This is not to say that the protection of victims is entirely overlooked. The e-Commerce Directive is designed to strike a balance between the various interests.[5] Most importantly, the exemption from liability for hosting service providers only extends to illegal online content that they are unaware of. After the illegal online

---

[1] The various opinions of academics and stakeholders will be presented throughout this report. The most prominent developments from policy makers are presented *infra*.

[2] Cf DSA proposal, recital 1; Commission, 'Online Platforms and the Digital Single Market' 2-3; Commission, 'Tackling Illegal Content Online' 2; Commission, 'Impact Assessment Digital Services Act', box 1.

[3] Commission, 'Impact Assessment Digital Services Act', points 34-43, 60-63. See also Section 1.5.

[4] See also Section 2.1.

[5] Case C-360/10 *SABAM* [2012] ECLI:EU:C:2012:85, para 51; e-Commerce Directive, recital 41; Frosio and Mendis 563.

content is discovered, for example after a notification, the provider should remove it. Through this mechanism, victims are able to remedy situation *ex post*.

Since the creation of the e-Commerce Directive in 2000, the information society has become far more developed. New kinds of hosting service providers or 'platforms' have greatly facilitated the online exchange of information in ways that were not envisaged by the e-Commerce Directive.[6] They have made it easier to disseminate various kinds of illegal online content. Furthermore, these platforms are no longer merely neutral conduits. Through their design, policy decisions and the use of algorithms, they exercise a great influence on the dissemination of content. Furthermore, the platforms frequently moderate the hosted content through (semi-)automated monitoring and by responding to notifications.[7] This raises questions about whether and under what conditions the platforms have, or should be considered to have, 'actual knowledge' or 'awareness' about the illegal online content.

These developments have put pressure on the exemption from liability and the resulting balance between the various interests. There is a strong sense that online intermediaries, and especially platforms, should do more to stop the dissemination of illegal online content through their services.[8] It is considered unfair that these platforms greatly benefit from the dissemination of (both legal and illegal) user-provided content, but cannot be held accountable if this dissemination causes harm to others. At the same time, the core principles of the e-Commerce Directive are still regarded as sound.[9] Good-faith intermediaries should not be held liable for any dissemination of illegal online content by their users.

This pressure has resulted in two distinct but connected legal developments. First, the *scope* of the exemption from liability has widened to (at least potentially) include these new intermediaries. This development is not discussed in this report (see Sections 1.2.1 and 1.3). Secondly, the *content* of the exemption has diminished, in particular in relation to these platforms. New rules have increased the responsibilities of online intermediaries, including responsibilities to *ex ante* prevent the dissemination of illegal online content.[10] These new responsibilities are the result of diverging national implementations of the e-Commerce Directive, case law of the Court of Justice (Chapter 2) and new European rules that impose various obligations in relation to specific types of illegal content or hosting service providers (Chapter 3).

The resulting legal framework has become fragmented, inconsistent, unclear and complex (Chapter 4).[11] It is different in each member state and contains variations depending on the type of online content and hosting service provider. Furthermore, it does not solve all underlying problems and creates a tension between the various involved interests.[12] On the one hand, online intermediaries still do not do enough to effectively limit the dissemination of illegal online content.[13] On the other hand, various stakeholders warn that increased moderation by intermediaries may result in a reduction of the online freedom of expression and

---

[6] DSA proposal 1, 8-9; Commission, 'Impact Assessment Digital Services Act', points 16-29; Van Hoboken and others, *Hosting intermediary services and illegal content online* 6; Dinwoodie 47; De Streel and others 11, 23, 41, 57.

[7] Section 2.3. See also the definition of 'content moderation' in DSA proposal, art 2(p).

[8] DSA proposal, recital 3; Commission, 'Digital Single Market Strategy' 12; Adviesraad Internationale Vraagstukken 16, 47; Elkin-Koren and Perel 669-671; Frosio 11-14, 21; Montagnani 299.

[9] DSA proposal 1-2, 8, recital 16; Commission, 'Impact Assessment Digital Services Act', box 1; European Parliament, 'Improving the single market', points 2, 6; Montagnani 298; De Streel and others 11, 57-58.

[10] Commission, 'Tackling Illegal Content Online' 10-11; Stalla-Bourdillon 287; Adviesraad Internationale Vraagstukken 7-8; Frosio 13-14; Frosio and Husovec 613-615, 628; Frosio and Mendis 547, 564-565; Geiger and Izyumenko 583; Montagnani 309.

[11] DSA proposal, recital 2; Commission, 'Impact Assessment Digital Services Act', box 1, points 91-92, 97; Stalla-Bourdillon 280; Adviesraad Internationale Vraagstukken 12, 49; Montagnani 296, 309-310.

[12] Commission, 'Tackling Illegal Content Online' 10-11; Frosio 13; Section 1.5.

[13] DSA proposal 9, 11; Montagnani 298.

freedom of information.[14] Finally, these responsibilities may affect the economic viability of certain newer and smaller intermediaries.[15]

For these reasons, a revision of the European framework for the liability and responsibilities of internet intermediaries is necessary. The various interests should be balanced anew. However, policy makers, academics and stakeholders have different perspectives on the best way to balance these interests and the way in which this balance can best be achieved. On 15 December 2020, the European Commission presented its proposal for a revision of the framework in the Digital Services Act ('DSA proposal').

The Dutch Ministry of Economic Affairs and Climate Policy has requested this report in order to prepare itself for the substantive aspects of this revision. To this end, it formulated several questions about the liability and responsibilities of hosting service providers, including platforms. These questions will be answered, in a slightly modified form, in this report.

The report first analyses the existing framework for the liability and responsibilities of hosting service providers. Chapter 2 describes the liability exemption in the e-Commerce Directive, with a particular focus on the criterion of 'actual knowledge or awareness'. Chapter 3 gives an overview of the other relevant legislative and self-regulatory initiatives. These chapters provide an answer to the following questions:

1. When does a hosting service provider have 'actual knowledge' or 'awareness' as referred to in Article 14 of the e-Commerce Directive?
2. What role and responsibilities in relation to the limitation of the dissemination of illegal online content do hosting service providers have according to the various legislative and self-regulatory initiatives?

Next, Chapter 4 analyses the existing framework. Specifically, it focusses on the gaps in the existing European framework and answers the following question:

3. Can any gaps be discerned in the European framework for the liability and responsibilities of hosting service providers?

Finally, Chapter 5 provides recommendations to address the gaps identified in Chapter 4 and evaluates possible legal solutions to stimulate hosting service providers to limit the dissemination of illegal online content through their services without unduly affecting fundamental rights and other concerned interests. Notably, this means that Chapter 5 is not focussed on an analysis of the DSA proposal *per se*, although it does address the proposed solutions. It answers the following question:

4. How can new rules best encourage hosting service providers to limit the dissemination of illegal online content?

[14] DSA proposal 11; Van Hoboken and others, *WODC-onderzoek* 57.

[15] DSA proposal 11.

1.2. Terminology

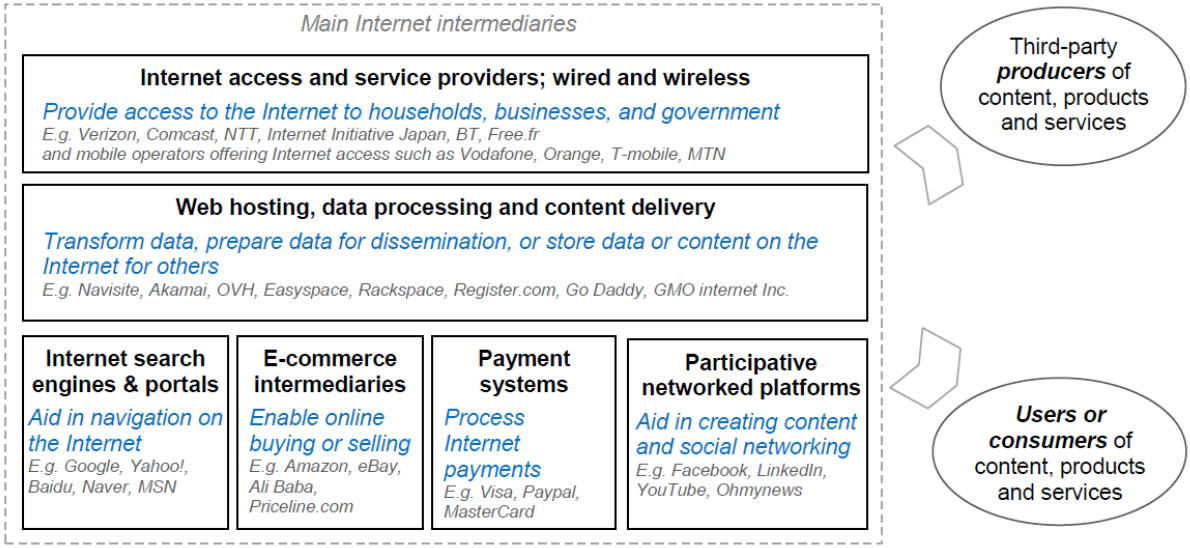
1.2.1. Internet intermediaries; hosting service providers; platforms; users; content providers

This report is focussed on online content that is disseminated by users through 'internet intermediaries' and the revision of the liability of intermediaries in the upcoming Digital Services Act. The concept of 'internet intermediary' can refer to any organisation that facilitates the transmission of online content through the internet. The OECD provides the following definition:

"'Internet intermediaries' bring together or facilitate transactions between third parties on the Internet. They give access to, host, transmit and index content, products and services originated by third parties on the Internet or provide Internet-based services to third parties."[16]

Examples of intermediaries are Internet Service Providers, data processing and web hosting providers, domain name registrars, search engines and portals, e-Commerce intermediaries, internet payment systems and participative network platforms.[17] Figure 1 provides an overview of the various kinds of intermediaries. They can be distinguished in various legally relevant categories.

Figure 1. Stylised representation of Internet intermediaries' roles. Source: OECD 9



First, it is possible to distinguish between the various kinds of electronic communications intermediaries and other types of intermediaries. Article 2 of the European Electronic Communications Code (Recast) Directive provides the European definitions for 'electronic communications network' (1), 'electronic communications service' (4), 'number-based' (6) and 'number-independent' (7) 'interpersonal communications service' (5) and 'public electronic communications network'. Furthermore, Article 4 of the

[16] OECD 9. For a detailed analysis of the concept 'internet intermediary', see also Dinwoodie 37-57.

[17] OECD 9-14. See also Van Hoboken and others, *WODC-onderzoek* 23; Dinwoodie 39, 47.

NIS Directive defines 'internet exchange point (IXP)' (13), 'DNS service provider' (15) and 'top-level domain name registry' (16).

Next, the e-Commerce Directive and the DSA proposal exempt the providers of 'mere conduit', 'caching' and 'hosting' 'information society services' from liability.[18] Article 2(f) of the DSA proposal limits the concept of 'intermediary service' to these three types of services. There has been a lot of discussion about the scope of these exemptions, and of the exemption for hosting services in particular. More concretely, the discussion has focussed on the limitation of this exemption to intermediaries that are 'neutral', 'merely technical', 'automatic' and 'passive'. This issue is not addressed in this report. Instead, we assume that a wide range of intermediaries can benefit from the exemption for hosting providers, including relatively 'active' intermediaries such as social media, search engines and online market places. For a more detailed analysis of this question, we refer to the report by Batura.[19] Current European rules define and regulate certain types of hosting service providers such as 'online content-sharing service providers', 'online marketplaces' and 'online search engines'.[20]

The discussion about the liability and responsibility of intermediaries has mainly focussed on new kinds of hosting services or 'platforms'. For this reason, our report is limited to hosting service providers, including platforms. There is currently no fixed definition of 'platform' or a sharp delineation from other intermediaries. However, Article 2(h) of the DSA proposal defines an 'online platform' as "a provider of a hosting service which, at the request of a recipient of the service, stores and disseminates to the public information, unless that activity is a minor and purely ancillary feature of another service and, for objective and technical reasons cannot be used without that other service, and the integration of the feature into the other service is not a means to circumvent the applicability of this Regulation." 'Dissemination to the public' is defined in article 2(i). It means "making information available, at the request of the recipient of the service who provided the information, to a potentially unlimited number of third parties". Article 25 of the DSA proposal defines 'very large' online platforms.

Under these definitions, a platform refers to a hosting service that uses the internet to connect the 'users' (or 'recipients') and to facilitate the exchange user-provided content to a potentially unlimited number of third parties. Instead of merely hosting content, an online platform also plays a more involved role in the dissemination of content that is provided by the 'content providers'.[21] For most platforms, the value of the service strongly depends on 'network effects'. For example, the value of an online marketplace depends on the offers by third-party vendors and the consumers that use the marketplace. The value of a social media service depends on the provided content and the users to whom this content can be disseminated.

---

[18] e-Commerce Directive, arts 2(a), (b), 12, 13, 14; DSA proposal, arts 3-5; Chapter 2. 'Information society service' is defined in Directive 2015/1535, art 1(b). About the relation between the concepts of 'internet intermediary' and 'information society service' in the context of the e-Commerce Directive, see also Dinwoodie 42.

[19] Batura. About the requirement to be neutral, merely technical, automatic and passive, see eg e-Commerce Directive, recital 42; Joined Cases C-682/18 and C-683/18 *Youtube* [2020] ECLI:EU:C:2020:586, Opinion of AG Saugmandsgaard Øe; Sartor 26-27; Husovec, *Injuctions Against Intermediaries in the European Union* 54-55; Kulk, *Internet intermediaries and copyright law* 112-113; Wolters 811; Dinwoodie 43-44, 53.

[20] NIS Directive, art 4(17), (18); CDSMD, art 2(6), 17; Modernisation Directive, arts 3(1)(b), 4(1)(e). See also Section 3.3.4.1. See also the service providers defined in NIS Directive, art 4(13), (15), (16), (19). Internet exchange points, DNS service providers, top-level domain name registries and cloud computing services. These services may also be able to benefit from the exemptions of liability. See also DSA proposal, recital 27.

[21] See also DSA proposal, recital 13.

1.2.2. Illegal online content; victims

'Online content' comes in all kinds of shapes and forms.[22] It can include all kinds of digital information that is disseminated through the internet.[23] It can consist of text in various forms, but also includes audio, video, pictures, e-books and software applications. For this reason, we adopt a broad definition of 'content'. The concept can refer to any kind of (digital) information.

Some intermediaries (internet service providers, electronic communication services) can be used to disseminate all kinds of online content in any form. Others are specialized in certain kinds of online content that is shaped in a certain way. For example, although they can both be used to share text messages, Facebook is used to share 'posts' to a content provider's network while a news website only allows 'reactions' to news articles. Whatsapp is used to share messages to a limited amount of people, while Twitter can be used to 'tweet' to the whole world. Furthermore, Amazon, eBay, Funda and Google each present advertisements in strongly diverging ways. However, all of these intermediaries are used to disseminate digital information through the internet and thus online content.

In this report, 'illegal' online content refers to content that violates the law in any way. This broad interpretation is in line with Article 2(g) of the DSA proposal, which defines 'illegal content' as "any information[,] which, in itself or by its reference to an activity, including the sale of products or provision of services is not in compliance with Union law or the law of a Member State, irrespective of the precise subject matter or nature of that law".[24] Illegal content can thus refer to online content that violates the law under all circumstances (for example, child pornography, Section 3.3.2), but also to content that is only 'unlawful' under certain circumstances (for example, because it violates someone else's privacy or because the recipient is a minor, Section 3.2.2).[25] Content can be illegal because the dissemination infringes on an exclusive right (for example, an intellectual property right), or simply because it is not compliant with the law (for example, a violation of a duty to provide proper information in consumer law).[26] Content can also be illegal because the underlying purpose is illegal. For example, even though a picture of a gun may not be illegal, an offer to sell a gun can be. Similarly, a request for information can constitute an illegal phishing-attack and thus be illegal content.

Many different types of illegal online content exist.[27] For example, illegal online content includes child pornography, unfair commercial practices and other infringements of consumer law, slander, 'hate speech'[28], infringements of copyright and trademarks and violations of privacy. The legality of online content depends on both national and European law. European law harmonises the illegality of certain kinds of online content, but does not prohibit member states from imposing other restrictions.[29]

We refer to the individuals or organisations that are harmed by the illegal content as the 'victims'. Because illegal content can take many shapes and forms, the same is true for the victims. A victim can be a consumer, a victim of child pornography or a rights holder whose content is disseminated without its

---

[22] For other definitions, see Adviesraad Internationale Vraagstukken 22; Kulk and Snijders 46.

[23] Cf the definition of 'digital content' in Digital Content and Digital Services Directive, art 2(1), recital 19.

[24] See also DSA proposal, recital 12.

[25] In this regard, translated to the situation in The Netherlands, 'illegal content' includes both '*strafbare*' and '*onrechtmatige*' content.

[26] Cf Hilty and Moscon 441-442.

[27] For more examles, see eg Dinwoodie 49-50; Hilty and Moscon; Van Hoboken and others, *WODC-onderzoek* 19-22.

[28] For a definition, see eg Kulk and Snijders 51.

[29] Section 4.2.2; De Streel and others 16-18.

permission. Notably, the victim of illegal content can also be a user (Section 1.2.1) of the platform, but this is not necessary. For example, a victim of hate speech may be targeted by reactions on his or her pictures, but also by posts on a platform of which it is not a user.

'Illegal' online content should be distinguished from content that can be undesirable or harmful but is ultimately permissible.[30] As a rule, freedom of expression and freedom of information require that users are free to spread online content. Illegality is the exception. For example, information may be false without being illegal disinformation,[31] a message may be insulting or even racist without being illegal slander or discrimination and 'obscene' nudity may be shown to consenting adults. Although these types of online content *can* be illegal under certain circumstances, they may be permissible in other contexts. Undesirable or harmful online content that is not illegal is not covered by this report.[32]

1.2.3. Liability and responsibilities of hosting service providers

This report does not address all possible responsibilities of hosting service providers. For example, a provider is responsible for the safety of its employees and is liable for a violation of this obligation. These kinds of responsibilities are not discussed in this report. Instead, it only focusses on liability and responsibilities in relation to (the limitation of the dissemination of) illegal online content. When we refer to the 'liability and responsibilities', we specifically refer to the liability for disseminating user-uploaded illegal online content and the responsibilities to limit this dissemination.

1.3. Delineation

The scope of this report is limited in various ways. As discussed in Section 1.2.1, this report does not address the question what types of intermediaries can benefit from the exemptions from liability of the e-Commerce Directive. Instead, we assume that a wide range of intermediaries can benefit from the exemption for hosting service providers. Next, this report is limited to hosting service providers including platforms. It does not address the responsibilities of other intermediaries, including mere conduit and caching.

Furthermore, this report focusses on the *obligations* and liability of intermediaries. It does not address the separate but connected question whether these and how these obligations and liability can be *enforced* effectively.[33] For example, it does not address the question whether a (national) civil procedure provides effective redress. For the same reason, this report does not address enforcement problems in relation to intermediaries that simply do not respond to (European) law, for example because they do not have a European establishment.

However, this report does address enforcement and procedural aspects insofar as they directly affect the obligations of online intermediaries. For example, a victim of online hate speech can enforce its rights by notifying the hosting service provider. Such a notification can trigger various obligations, including an obligation to remove the content.[34]

---

[30] See also Kulk and Snijders 47.

[31] See also High Level Expert Group on Fake News and Online Disinformation 10; De Streel and others 10.

[32] See also DSA proposal 9.

[33] About this issue, see Van Hoboken and others*, WODC-onderzoek*.

[34] Eg Sections 2.3.1.3, 3.2.2, 3.2.3, 3.3.3, 3.3.3.4.1 and 3.3.4.2.

Finally, the underlying objective of this report is to prepare the Ministry of Economic Affairs and Climate Policy for the revision of the *European* e-Commerce Directive in the *European* Digital Services Act. For this reason, the report focusses on the European framework. National (case) law is only included to a limited extent, and only when it provides insight about the European framework or its revision.

1.4. Methodology

The questions of this report are primarily of a legal nature. They require a description of (questions 1 and 2) and the identification of the gaps in (question 3) the current legal framework for the liability and responsibilities of hosting service providers. These questions are primarily answered by using descriptive and doctrinal legal research and close reading of legal sources such as treaties, statutes, preparatory documents, case law, guidelines by regulators and supervisory authorities and legal literature.

For question 3, a 'gap' is described as a situation in which the current framework is unjustifiably inconsistent or when the various involved interests are insufficiently safeguarded by the current legal rules. In both of these situations, the gaps are identified primarily by the previous analysis of the existing rules.

Like cases should be treated alike. This maxim of justice holds especially true in the digital single market, where online intermediaries (and other businesses) should be able to offer their services throughout the European Union. As a starting point, the rules for intermediary liability should be the same in all member states, for all types of illegal content and for all types of hosting service providers. This is not to say that no relevant differences between the member states, types of illegal content and service providers can exist. Relevant differences may form a justification for divergent rules. However, a gap exists when legal differences are not justified by relevant differences.[35]

Gaps may also exist because the existing rules provide insufficient safeguards for the various involved interests discussed in Section 1.5. The legal framework for intermediary liability is designed to protect and balance various interests. However, an analysis of the existing legal framework can reveal that a particular interest is, generally or in relation to a specific type of online content or hosting service, insufficiently safeguarded by the current legal rules.

Question 4 also requires an estimation of the effectiveness of the proposed and other potential new legal norms. For this reason, it is important to consider other perspectives as well. It also calls for insight into the existing possibilities for the limitation of the dissemination of illegal content. For this reason, this report also contains an empirical component. It includes semi-structured interviews and an expert meeting with several stakeholders, including (representatives of) victims of illegal content, intermediaries and non-governmental organisations. The interviews are processed anonymously in this report. Instead of the name or organisation of the interviewee, we refer to a broader category such as 'a representative from an online intermediary'.

It is important to note that these interviews and expert meeting complement but do not *replace* the traditional legal research. The various stakeholders have an interest in the revision of the legal framework. Although it is important to take their experiences, insights and interests into account, our answers are not dictated by the wishes or interests of (some of these) stakeholders. Instead, question 4 requires a balancing of the various involved interests discussed in Section 1.5.

---

[35] See also De Streel and others 12, 41, 53, 76, 80.

1.5. Involved interests

Both the eCommerce Directive and the DSA proposal are aimed at the creation of a balance of the various involved interests.[36] The creation of such a balance requires a thorough understanding of these interests. This is also necessary for the answer to question 4. This question is aimed at finding the best rules to encourage hosting service providers to limit the dissemination of illegal online content. In this report, we understand the 'best' rules as the rules that best balance the effective limitation of the dissemination of illegal online content with other concerned interests. The following subsections give an overview of the involved interests.

1.5.1. Protecting victims of illegal content

The liability and responsibilities of intermediaries are primarily imposed to protect the victims of illegal content. Many types of illegal online content exist (Section 1.2.2). Consequently, there are important differences between the various victims of illegal content. For example, the victims of hate speech require a different protection than the rights holders of illegally shared copyrighted works. Furthermore, users to whom content is shared may also be victims when they are exposed to shocking or otherwise inappropriate content. Moreover, terrorist content is not always aimed at individual victims. It is (also) aimed at the entire society. Finally, some types of illegal content violate fundamental rights such as the rights to privacy and data protection.[37]

These differences may require specific rules for certain situations. Generally though, victims of illegal online content can be protected in several ways:

1. By proactively preventing the dissemination of illegal content *ex ante*. Online intermediaries can be required to check (or filter out) illegal content before or shortly after it is uploaded.
2. By reactively removing the illegal content *ex post*, after a notification by the victim or another organisation. Submitting a notification can be cumbersome and complicated, especially for non-professional victims. This is amplified because the same illegal content may appear multiple times and on multiple platforms.
3. By discouraging the dissemination of illegal online content by users. This can be done by the intermediaries (for example by banning, suspending or fining users), the government (criminal sanctions) or the victims themselves (private law liability of content providers).
4. By giving victims effective redress possibilities, either against the content providers or against the intermediary. Such redress can undo (a part of) the harm that is caused by the illegal online content. Furthermore, it discourages users from disseminating illegal content (see also under 3) and encourages the intermediaries to take responsibility (see also under 1 and 2).

In sum, victims of illegal online content can be protected by imposing proactive monitoring obligations and effective, fast and user-friendly notice and action procedures and by creating effective sanctions against providers of illegal content and the intermediaries that facilitate this dissemination.

---

[36] N 5; DSA proposal, recital 34, 41.

[37] Eg Geiger, Frosio and Izyumenko 143; Van Hoboken and others, *WODC-onderzoek* 39-41. See also Adviesraad Internationale Vraagstukken 46-47.

1.5.2. Preserving freedom of expression and freedom of information; related fundamental rights

The protection of victims by the removal of online content comes at the expense of the freedom of expression and freedom of information of the content providers. The limitation of these freedoms is not necessarily undesirable. Generally speaking, the fact that the content is illegal can justify a limitation of these rights. There is no fundamental reason to protect the online dissemination of such content through online intermediaries.[38]

However, the removal of illegal online content is often imprecise and leads to 'collateral censorship'. For various reasons, explained in more detail in Section 2.2.2, intermediaries may also remove permissible online content. This restricts the online exchange of information and thus leads to a restriction of the fundamental rights of freedom of expression and freedom of information.

The removal of online content can also affect other fundamental rights. First, these restrictions do not affect everyone equally. Certain types of communication may be more prone to collateral censorship than others. For this reason, removal of permissible online content may disproportionally affect certain groups. For example, the (permissible) posts by religious young Muslims may be removed due to an incorrect designation as terrorist content, the political messages and memes shared by right-wing young men may be incorrectly labelled as a violation of copyright or hate speech and a conservative country's hostile stance against LGBTQ-content may cause it to be removed due to incorrect or abusive notices, even when it is not illegal.[39] For this reason, the removal of permissible online content could also affect other fundamental rights. It can cause discrimination and infringe on political rights. Furthermore, certain types of collateral censorship may be more damaging to the society as a whole. For example, the removal of news also affects the freedom of the press.[40]

In principle, the fundamental rights of freedom of expression and freedom of information can be protected by only removing online content that is undoubtedly or 'manifestly' (see Section 2.3.2) illegal.[41] Furthermore, there should be safeguards in place to prevent the unjustified removal of permissible content.[42] For example, the users whose content is removed should be able to undo this removal through a counter-notice procedure that is at least as effective and user-friendly as the original notice and take down procedure (Section 1.5.1). Furthermore, human oversight should complement and correct automated monitoring systems (see also Section 2.3.1.2).

This conclusion does come with two important caveats. First, some or even most people will only express themselves online if they feel sufficiently secure. This may not be the case if a social media post leads to insults or bullying, even if these reactions are ultimately not illegal.[43] More generally, different platforms can

---

[38] Commission, 'Tackling Illegal Content Online' 2; European Parliament, 'Improving the single market', point 6; Adviesraad Internationale Vraagstukken 32-33; Elkin-Koren and Perel 671. Cf the concept of 'internet exceptionalism': some authors put more emphasis on the 'free' character of 'cyberspace', even at the expense of other legally protected interests. For example, see Barlow; Svantesson 692-693. See also Wolters 799 for more examples of internet exceptionalism in law.

[39] DSA proposal, recital 57; Hern.

[40] Cf Geiger, Frosio and Izyumenko 143; De Streel and others 83.

[41] See also Adviesraad Internationale Vraagstukken 30, 45-46; Geiger, Frosio and Izyumenko 140-147; Van Hoboken and others, *WODC-onderzoek* 41-44; De Streel and others 77.

[42] Commission, 'Impact Assessment Digital Services Act', points 51-52, 54; Commission, 'Tackling Illegal Content Online' 3, 20.

[43] Cf Commission, 'Impact Assessment Digital Services Act', point 62.

cater to different people and different types of content.[44] For this reason, content moderation practices by online platforms that go beyond the removal of manifestly illegal online content may actually stimulate the online exchange of information and thus facilitate freedom of speech and freedom of expression. Most, but not all, of the interviewed representatives of online intermediaries indicated that they apply stricter standards than imposed by law. At the same time, these moderation practices should be non-discriminatory, transparent and consistently applied.[45]

Secondly, the online platforms that impair freedom of expression and freedom of information are also the ones that facilitated these fundamental rights through their services. Although limits may exist when platforms become so ubiquitous that they *de facto* become unavoidable and their services are the only way to effectively disseminate information (Section 1.5.3), platforms are free to shape their services as they see fit (Section 2.2.2.2) and content providers are ultimately free to ignore certain platforms and exchange information through other channels.

For this reason, freedom of expression and freedom of information benefit from the existence of a pluriform system of online platforms. The removal of permissible but borderline content by some platforms may be justified, but only as long as content providers have another effective way to disseminate their ideas and the moderation practices do not lead to an infringement of other fundamental rights.

1.5.3. Maintaining the rule of law and judicial oversight

The removal of online content does not only affect the fundamental rights of individual content providers of the intermediary services. Such removal can also affect society as a whole by undermining democratic values such as the rule of law and the effectiveness of judicial oversight.

By holding intermediaries liable for failing to remove illegal content, they are forced to judge whether certain content is permissible. It is broadly argued that intermediaries should not be the ones to make these complex decisions.[46] However, it is important to note that both removing and retaining online content constitutes a 'decision' about its availability. Either allowing or removing online content that is possibly but not manifestly illegal does not in itself lead to a better protection of the rule of law (see also Section 2.3.2).

The fact that intermediaries are forced to decide whether content is permissible is not necessarily a bad thing. Intermediaries facilitate the dissemination of illegal content. It is therefore only justified that they also carry the *responsibility* to separate illegal and permissible online content, especially after receiving a specific notification about the illegality of certain content. At the same time, the ultimate *power* to make the distinction should not lie with the intermediaries: it should lie with judges.

In theory, both content providers and victims can go to a judge when they disagree with an intermediaries decision to (not) remove certain content.[47] In practice, not many content providers or victims use this opportunity. The costs and efforts of suing an intermediary in court generally outweigh the benefits.[48] Enforcement through a court is often only realistic for certain types of victims such as repeat players like the

---

[44] For example, an interviewed representative of a digital rights organisation commented that a dog forum should be free to remove cat content.

[45] Commission, 'Impact Assessment Digital Services Act', points 54, 57.

[46] Eg Joined Cases C-682/18 and C-683/18 *Youtube* [2020] ECLI:EU:C:2020:586, Opinion of AG Saugmandsgaard Øe, para 187; Stalla-Bourdillon 290; Frosio 26; Kuczerawy 527; Van Hoboken and others, *WODC-onderzoek* 79; De Streel and others 45; Svantesson 693.

[47] Cf e-Commerce Directive, art 18.

[48] Eg Walree and Wolters 351, with references to further literature.

holders of copyright. This is amplified by the 'Streisand effect': an attempt to remove information may lead to its further dissemination.

Although the decision-making of these intermediaries is partly justified by their freedom to shape and offer their services as they see fit, it becomes problematic when these services become so ubiquitous that their services are the only way to effectively disseminate information.[49] As one interviewed representative of a digital rights organisation commented, the sheer size of a handful of platforms has given them enormous power over the public debate, irrespective of the way in which they practice content moderation. This problematic nature is further amplified because the decisions are often inconsistent, not transparent (partly) made through automated means and because courts only have limited opportunities to supervise and correct them.[50] These circumstances lead to a situation in which big (non-European) private companies and their algorithms become the *de facto* judges about the permissibility of online content.[51]

The possible measures to mitigate the negative effects of this kind of 'private ordering' are similar to the measures to protect freedom of expression and freedom of information (Section 1.5.2). The rule of law can be strengthened by measures that ensure effective judicial oversight by giving content providers and victims a real opportunity to have judicial recourse. Moreover, transparency obligations can ensure that the courts have a real opportunity to judge the 'private ordering' by the intermediaries.

1.5.4. The economic interests of hosting service providers

The liability and responsibilities of hosting service providers come at the expense of their economic viability and their right to freedom of business.[52] Hosting service providers benefit from freedom to shape their business as they see fit, free from both obligations to remove illegal online content (Section 1.5.1) *and* from interference with the way they decide to remove content for their own reasons (Sections 1.5.2 and 1.5.3).

The importance of these economic interests depend on the valuation of the services themselves. Hosting service providers play an important role in the development of our information society. They facilitate freedom of expression and information, effective communication and the development of all kinds of economic activities. The costs of liability and responsibilities can negatively impact their development and availability and (consequently) the development of the internet and the information society. They could cause the providers to abandon or limit their hosting services or start charging a (higher) price.

This rationale for the exemption from liability of the e-Commerce Directive (Section 2.2.2) has become less important. Since the creation of the e-Commerce Directive in 2000, the information society has become far more developed. Some hosting service providers have become highly mature and profitable. Although these services are still important, they could also be economically viable without this kind of protection or stimulation.

---

[49] About this issue, see eg Commission, 'Impact Assessment Digital Services Act', points 85-86; Yannopoulos 46, 53-56; Adviesraad Internationale Vraagstukken 11, 41-42; Geiger, Frosio and Izyumenko 138-139; Van Hoboken and others, *WODC-onderzoek* 57; Kuczerawy 527; McGonagle 479-480; De Streel and others 80-81; Taddeo 134-136. See also Sections 1.1, 1.5.2, 2.2.2.2; DMA proposal.

[50] Commission, 'Impact Assessment Digital Services Act', points 78-82, 88; Yannopoulos 46; Elkin-Koren and Perel; Frosio and Husovec 625-627. See also n 123; Section 2.3.2.

[51] DSA proposal, recital 56; n 46, 49. This issue is not limited to intermediary liability, it is also an issue of competition law. The risk of platforms becoming the *de facto* judges of what is allowed is smaller when no single platform is dominant.

[52] About this right, see DSA proposal, recital 41; Geiger, Frosio and Izyumenko 148-149.

At the same time, the economic interests may still play a role in the formulation of new responsibilities. Generally, the economic interests can be protected by only imposing responsibilities that can be fulfilled at a reasonable cost.[53] First and foremost, this means that the responsibilities of hosting service providers should be proportional.[54] The benefits should outweigh the costs of their fulfilment. Furthermore, the responsibilities should be clear, harmonised and consistently applied throughout Europe.[55] Finally, the responsibilities should be formulated in a technology-neutral manner. This allows hosting service providers to find new ways to more effectively and efficiently meet their responsibilities.[56]

However, even proportional responsibilities can threaten the economic viability of certain beneficial hosting service providers. Furthermore, liability and responsibilities that may be proportional for certain (large, mature) intermediaries, may be too costly for other (small, new) hosting service providers that lack the capacity to efficiently limit the dissemination of illegal content. A differentiated approach may be necessary to stimulate innovation and protect smaller hosting service providers. Under this approach, small and new intermediaries would be subject to fewer responsibilities.[57]

At the same time, it may not always be justified to 'punish' large hosting service providers for their success and efficiency by imposing more responsibilities. Similarly, the fact that an intermediary is not profitable, new and small does not justify the dissemination of illegal content by itself.[58] It is necessary to find a balance between the stimulation of innovation by small hosting service providers and the protection of other interests.

---

[53] DSA proposal 8, 13, recital 4.

[54] European Parliament, 'Improving the single market', point 10.

[55] Commission, 'Online Platforms and the Digital Single Market' 4; Commission, 'Impact Assessment Digital Services Act', points 70-71, 75-76; European Parliament, 'Improving the single market', points 10, 12.

[56] DSA proposal, recital 4; European Parliament, 'Improving the single market', point 14.

[57] DSA proposal 2, 11, 13, recital 35, 43; Joined Cases C-682/18 and C-683/18 *Youtube* [2020] ECLI:EU:C:2020:586, Opinion of AG Saugmandsgaard Øe, para 194-195; Commission, 'Impact Assessment Digital Services Act', points 70-71; Adviesraad Internationale Vraagstukken 45-46; De Streel and others 54-55; Van Hoboken and others*, WODC-onderzoek* 25.

[58] Cf an interviewed representative from an organisation fighting against online abuse that considered dealing with illegal content as an inherent cost of the intermediary business. If it is too burdensome for a particular intermediary, it should not be in the intermediary business in the first place.

2. Liability of hosting providers

2.1. Introduction

An internet intermediary may be held liable for facilitating the dissemination of illegal online content. This is a kind of 'secondary liability',[59] as illustrated by Figure 2. The 'primary' unlawful act is committed by the content provider. However, the victim may not be able to enforce a remedy against this content providers, for example because it cannot be identified or sued or because it lacks the funds to pay damages.[60] For this reason, the victim may prefer to hold the intermediary liable.

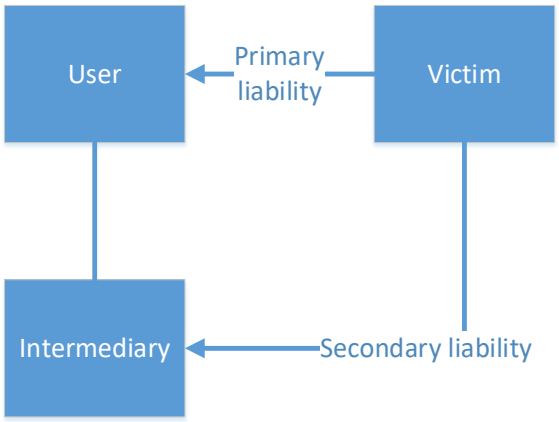


Figure 2. Primary and secondary liability

If the mere fact that a user disseminated the content through the services of the intermediary is sufficient to trigger secondary liability, the liability is 'strict'. However, as discussed below, the e-Commerce Directive only allows secondary liability for 'negligence' under certain circumstances. The liability can only be triggered if the hosting service provider has taken insufficient steps to remedy the unlawful act of the content providers, specifically by removing the online content after becoming aware of the illegal nature.[61]

This chapter analyses the secondary liability of 'hosting' service providers under the framework of the e-Commerce Directive. First, it provides a general overview of Article 14 of the e-Commerce Directive, the central provision of this framework (Section 2.2). Article 14 exempts hosting service providers from liability for hosting illegal online content. However, this exemption does not apply if the hosting service provider has 'actual knowledge' or 'awareness' of the illegal content. For this reason, the scope of the exemption largely depends on the circumstances under which such knowledge or awareness exists. By analysing this criterion (Section 2.3), this chapter will provide an answer to question 1 (Section 2.4): *When does a hosting service provider have 'actual knowledge' or 'awareness' as referred to in Article 14 of the e-Commerce Directive?* Furthermore, it provides a part of the answer to question 2: *What role and responsibilities in relation to the*

[59] Joined Cases C-682/18 and C-683/18 *Youtube* [2020] ECLI:EU:C:2020:586, Opinion of AG Saugmandsgaard Øe, para 138; Sartor 8-9; Husovec, 'Remedies First, Liability Second'; Rosati. About the facilitation of this dissemination, see Section 1.1.

[60] See also Geiger and Izyumenko 566; Van Hoboken and others, *WODC-onderzoek* 35.

[61] Frosio and Mendis 545.

limitation of the dissemination of illegal online content do hosting service providers have according to the various legislative and self-regulatory initiatives?

2.2. Article 14 of the e-Commerce Directive

Article 14 of the e-Commerce Directive states that a provider of hosting services is not liable for hosting illegal content. The provision creates an exemption from private law liability, but also from administrative or criminal sanctions.[62]

The exemption of Article 14 applies in two situations. First, it applies if the provider does not know about the illegal content. Pursuant to Article 14(1)(a), the exemption of liability applies if the provider does not have 'actual knowledge' of the illegal activity or information and is not 'aware' of facts or circumstances from which the illegal activity or information is apparent. Secondly, pursuant to Article 14(1)(b), the exemption can also apply after the provider obtains such knowledge or awareness, but only if it acts 'expeditiously' to remove or disable access to the information. In other words, a hosting service provider is not liable for illegal content that it doesn't know about, but it can have an obligation to remove this content after it becomes aware of its existence (a 'notice and take down' obligation, see below Section 2.3.1.3).

2.2.1. The role of Article 14 in the European legal framework

Before further analysing its exact legal consequences, it is necessary to properly understand the role of Article 14 of the e-Commerce Directive in the European legal framework. Most importantly, Article 14 contains a *prohibition*. It prohibits member states from imposing liability on hosting service providers for hosting illegal content. Instead, member states have an obligation to ensure that the providers cannot be held liable under national law.

Article 14 applies to all types of illegal content and all hosting service providers. However, it only prohibits *member states* from imposing liability for *the dissemination of illegal online content*. However, they may still be held liable by *European law* or for a violation of *other obligations* such as monitoring obligations. As discussed in Chapter 3, European law imposes various obligations that limit the scope of the exemption of Article 14 in relation to specific types of illegal content or hosting service providers.

The conditions of Article 14(1)(a) and (b) limit the scope of the exemption. The exemption from liability does not apply if the hosting service provider is aware of the illegal content and does not act expeditiously to remove it. This does not automatically mean that a hosting service provider is liable under those circumstances or that it has a notice and take down obligation. It only means that member states are *allowed* to impose such liability or obligations.[63] As long as no other European rules state otherwise,[64]

---

[62] Commission, 'First report' 12; Yannopoulos 45; De Streel and others 21. Cf the Dutch implementation in both Article 54a of the Criminal code and Article 6:196c of the Civil code. Note that the article does distinguish between the various kinds of liability. Awareness can only lead to a claim for damages, whereas actual knowledge is required for other kinds of liability. See also Section 2.3.1.3.

[63] See also Joined Cases C-682/18 and C-683/18 *Youtube* [2020] ECLI:EU:C:2020:586, Opinion of AG Saugmandsgaard Øe, para 134; Van Eecke and Truyens ch 6, 9; Stalla-Bourdillon 282; Hilty and Moscon 440; Kuczerawy 530; De Streel and others 21. Member states even have some freedom to impose more far reaching obligations, such as an obligation to also remove identical or equivalent content. Section 2.3.1.1. See also Section 3.3.4.1.

[64] Cf Copyright in the Digital Single Market Directive, art 17(4), that holds 'content-sharing service providers' liable for unauthorised acts of communication of copyright-protected works.

member states could also decide that hosting service providers are not liable for hosting illegal content. This report concerns the revision of the European e-Commerce Directive by the Digital Services Act. For this reason, we will focus on the European law and do not include an extensive analysis of the liability of hosting service providers under member state law.

2.2.2. Rationale

Hosting service providers, and internet intermediaries in general, play an important role in the development of the internet and the exercise of fundamental rights. Most notably, they facilitate freedom of expression and information, effective communication and the development of all kinds of economic activities. Liability for illegal content would interfere with this role in various ways.[65]

First, such liability would hinder the operations and economic viability of hosting service providers. This rationale is discussed in more detail in Section 1.5.4.

More fundamentally, liability would induce hosting service providers to limit content providers from using their services to disseminate illegal content. Such limitation is not necessarily undesirable (Section 1.5.2). However, liability could also induce them to *excessively* constrain the behaviour of content providers. It could cause hosting service providers to become overly cautious and remove or preventively filter online content that is permitted or even valuable. The likelihood and magnitude of this 'collateral censorship' depend on various factors.[66]

2.2.2.1. Uncertainty

First, collateral censorship is more likely to occur when the permissibility of online content is unclear. With hosting services, the online content is primarily uploaded by users and immediately disseminated. At this moment, it is impossible for hosting service providers to know whether the content is permissible.[67] Holding hosting service providers (strictly) liable for hosting illegal online content could induce them to monitor the online content before allowing its dissemination. Such monitoring would hinder effective communication and limit the freedom of expression. For this reason, Article 14 of the e-Commerce Directive provides an exemption for illegal content that the hosting service provider is unaware of.

The risk of collateral censorship is smaller if, in accordance with Article 14 of the e-Commerce Directive, the hosting service provider can only be held liable if it knows about the illegal character and (negligently) fails to remove it. Under this system, the providers are not stimulated to preventively verify the legality of the uploaded content.

However, collateral censorship can also arise due to factual uncertainty and legal unclarity. When online content is clearly permissible, an intermediary is not likely to remove it for fear of liability. However, it can be difficult to distinguish between permitted and illegal online content. For example, the line between an infringement of copyright and a permissible parody or between unfounded slander and legitimate critical journalism will not always be clear.[68] Furthermore, for many types of illegal content, this line may be drawn

---

[65] About the rationale of the exemption from liability, see also eg e-Commerce Directive, recital 40; Sartor 10-15; Stalla-Bourdillon 288; Ullrich, 'Standards for Duty of Care?'; Yannopoulos 47-48; Elkin-Koren and Perel 670-671; Frosio and Mendis 546-547; Geiger, Frosio and Izyumenko 145-146; Kuczerawy 525-526; Kulk, 'Platformaansprakelijkheid' 132; Montagnani 296; De Streel and others 19; Section 1.1.

[66] See also Sartor 6.

[67] Although this knowledge could be acquired, in part, through technical means. See also Section 2.3.1.2.

[68] Eg Verbiest and others 14-15; Yannopoulos 50; Adviesraad Internationale Vraagstukken 22-23, 30, 43; Geiger, Frosio and Izyumenko 146; Kulk and Snijders 50; McGonagle 483; Montagnani 304; De Streel and others 40, 43, 52.

differently in each member state.[69] In those circumstances, a hosting service provider may decide to take down online content that is permissible under the law.

2.2.2.2. Diverging consequences

By itself, uncertainty can lead to both under- and over-removal. However, the difference between the consequences induces hosting service providers to err on the side of caution. For them, the risks of permitting online content that is ultimately deemed illegal outweigh the adverse effects of removing lawful content.[70]

A failure to remove illegal online content can directly affect hosting service providers through liability. In contrast, the effects of removing permitted content are indirect. Although the removal of permitted content could affect the use and popularity, and therefore the profitability, of the service,[71] it typically does not have any direct legal consequences. In principle, hosting service providers are free to ward off certain kinds of online content, even if they are ultimately not illegal. For example, a provider has the right to remove (legally permissible) personal insults, racially charged or otherwise offensive statements, political statements or nudity. Even if such removal could lead to liability under member state law,[72] the intermediary's terms and conditions generally prohibit the dissemination of such content through the service and limit the liability *vis-a-vis* the user.[73] Although limits may exist when hosting service providers become so ubiquitous that they *de facto* become unavoidable (Section 1.5.2) for certain kinds of content or when their practices lead to discrimination or otherwise violate fundamental rights or other mandatory rules such as consumer or competition law, hosting service providers are typically free to shape their services as they see fit and thus prohibit certain kinds of permissible content.[74] Furthermore, the adverse effects can be limited by reinstating the online content after a complaint and review. In contrast, a provider is unable to contract with all potential victims of illegal online content and the adverse effects of such content are typically not undone by its removal.[75]

2.2.2.3. Synthesis

The exemption from liability of article 14 e-Commerce Directive is primarily motivated by a desire to avoid collateral censorship. By exempting hosting service providers from liability for hosting illegal content which they are unaware of, they are no longer induced to preventively constrain the behaviour of content providers. The providers can only be held liable if they violate their obligations after learning about the illegal nature of the online content. However, diverging consequences could still lead to collateral

---

[69] Verbiest and others 14-15; Montagnani 304; De Streel and others 40, 51, 56-57, 61; Section 4.2.2.

[70] Eg Joined Cases C-682/18 and C-683/18 *Youtube* [2020] ECLI:EU:C:2020:586, Opinion of AG Saugmandsgaard Øe, para 189; Commission, 'Impact Assessment Digital Services Act', box 1; Frosio 26; Keller; Kuczerawy 527; Kulk and Snijders 61-62; McGonagle 483; De Streel and others 23. Cf Van Hoboken and others, *WODC-onderzoek* 79, who claim that uncertainty leads to underremoval. This diverging conclusion may be caused due to the fact that their report focusses on the effective protection of victims.

[71] De Streel and others 44. This also depends on the type of service and the way it markets itself. For example, a 'family-friendly' social media network (eg Facebook) may want to remove more borderline but ultimately permissible content than a 'minimal intervention' message board (eg 8kun). Van Hoboken and others, *WODC-onderzoek* 26.

[72] For example, because a hosting service provider could be held liable for impairing a user's right to freedom of expression or because it could classify as breach of contract. Verbiest and others 16; Klos. See also n 49.

[73] Yannopoulos 50; Adviesraad Internationale Vraagstukken 31; Frosio 26; Van Hoboken and others, *WODC-onderzoek* 52; Kulk and Snijders 49, 62, 65; De Streel and others 10, 14, 40, 43, 61. Generally speaking, the hosting service provider prohibits content in accordance with the *most restrictive* national laws. This allows it to apply the same moderation practices throughout an entire region such as the European Union. Svantesson 693. See also n 69.

[74] DSA proposal, recital 38; Commission, 'Impact Assessment Digital Services Act', point 51; Van Hoboken and others, *WODC-onderzoek* 54; Klos.

[75] See also Yannopoulos 49; Keller; Hilty and Moscon 441; Van Hoboken and others, *WODC-onderzoek* 26, 36.

censorship, especially when factual uncertainty and legal unclarity can make it difficult to distinguish between permitted and illegal online content.

2.3. Actual knowledge or awareness

Pursuant to Article 14 of the e-Commerce Directive, a hosting service provider is not liable for illegal content that it does not know about, but it can have an obligation to remove this content after it becomes aware of its existence. For this reason, it is important to understand when a provider has actual knowledge or awareness as referred to in Article 14 of the e-Commerce Directive. It affects both the existence of an obligation to remove illegal content and the moment when this obligation should be performed.

This issue can be further divided in three subquestions:

1. *How* is the hosting service provider supposed to acquire this knowledge (Section 2.3.1)?
2. *What* knowledge is required to trigger 'actual knowledge' or 'awareness' (Section 2.3.2)?
3. *When* is the threshold for 'actual knowledge' or 'awareness' met (Section 2.3.3)?

The e-Commerce Directive is vague about the exact meaning of actual knowledge or awareness.[76] It does not provide a clear and harmonised answer to these questions. Instead, Article 14(3) allows member states to establish procedures governing the removal or disabling of access to information. Furthermore, Article 16 encourages national and European codes of conduct. For this reason, it is not possible to give a universal *European* description of the criteria of 'actual knowledge' and 'awareness'. Instead, this Section will describe the criteria in a way that best matches the rationale and European interpretation of Article 14 and the various implementations in member states. Furthermore, it will address the most important points to be addressed in the upcoming Digital Services Act (Section 2.3.4). A selection of the national laws is discussed in more detail in Section 3.4.

2.3.1. How can the knowledge be acquired?

In order to properly understand the criterion of 'actual knowledge' or 'awareness', it is necessary to understand the channels through which a hosting service provider can obtain such knowledge or awareness. The channels can be roughly divided into two categories. First, a hosting service provider can obtain this knowledge by monitoring the hosted online content (Sections 2.3.1.1 and 2.3.1.2). Secondly, it can be notified by a third party (Sections 2.3.1.3 and 2.3.1.4). Pursuant to the Court of Justice in *eBay*, actual knowledge or awareness can be acquired through both of these channels. It is not limited to knowledge that is acquired through some specific channel.[77]

2.3.1.1. Monitoring the hosted information; no general obligation to monitor

Hosting service providers come in various shapes and forms.[78] With some services, the hosted content is confidential and only visible to authorised users (e.g. Google Docs, Dropbox). For those services, the hosting service provider may not have the right[79] to monitor the information. In contrast, platforms are typically

---

[76] Van Eecke and Truyens ch 6, 19, 25.

[77] Case C-324/09, *eBay* [2011] ECLI:EU:C:2011:474, para 121-122. Cf Section 2.3.1.3; Verbiest and others 44, 71. This rule is confirmed in DSA proposal, recital 22.

[78] See Section 1.2.1; Batura.

[79] Cf De Streel and others 52, 56. Cf the Terms and Conditions of iCloud, permitting Apple to screen and remove content from iCloud at its own discretion. <https://www.apple.com/ie/legal/internet-services/icloud/en/terms.html> accessed 1 December 2020.

designed to display the hosted information to all or specific kinds of viewers (e.g. publicly available websites, social media, online market places). For those services, the hosting service provider can also monitor the hosted content.

A provider can have several legitimate reasons to monitor the hosted content. First, it may want to remove online content that is illegal or that otherwise violates the terms and conditions of the service. Secondly, the provider may want to 'censor' content that is undesirable but not necessarily illegal without removing it outright. For example, it can demonetize or deprioritise the content or warn the viewers, for example by stating that it may contain disinformation.[80] Finally, the provider may want to process the content to improve the service in some other way. For example, an internet referencing service (e.g. Google Ads) or an online marketplace may want to change the order of the displayed ads based on their content and quality.[81] Under these scenarios, the monitoring is not motivated by a desire to avoid liability, but by a desire to improve and protect the online service.[82] Without the monitoring, the hosting service provider would not have acquired knowledge of the illegal content and thus would not be liable.

Monitoring could lead to actual knowledge or awareness about illegal content and can thus trigger an obligation to remove this content (Section 2.3.1). However, the fact that a hosting service provider monitors the hosted information does not necessarily mean that knowledge or awareness about any existing illegal content is acquired or that it is no longer 'neutral', 'merely technical', 'automatic' and 'passive'.[83] Monitoring is not complete and may not detect all kinds of illegal content. For example, an automatic monitoring system that detects child pornography may not detect illegal hate speech. For these reasons, monitoring does not mean that a hosting service provider can no longer benefit from the exemption from liability.

Monitoring could also be imposed by a legal obligation. For example, a duty of care to limit the dissemination of copyright-protected works could lead to an obligation to monitor the uploaded content.[84] If such obligations would be permissible, member states could impose a duty to preventively check all hosted files for any illegal content. Under such an obligation, a hosting service provider should always be aware of the illegal content and could never escape liability under Article 14(1)(a) of the e-Commerce Directive. Even if a hosting service provider could claim that it had no 'actual knowledge' about the illegal online content, and thus escape liability pursuant to Article 14(1)(a), it could still be held liable for a violation of the duty to monitor the hosted files. After all, if it had properly performed this obligation, it would have known about the illegal content. Article 14 only prohibits liability for the stored information. It does not prohibit member states (see also Section 2.2.1) from holding hosting service providers liable for failing to comply with other obligations.

Far reaching monitoring obligations can therefore undermine the effectiveness of Article 14 of the e-Commerce Directive and even render it meaningless. For this reason, Article 15 prohibits such duties. It states that a member state is not allowed to impose a general obligation to monitor the hosted online content or to actively seek facts or circumstances that indicate illegal activity. For example, the European Court of Justice ruled that a member state cannot order a hosting service provider to install a permanent

---

[80] Sartor 22; Elkin-Koren and Perel 671; Frosio and Husovec 617; Frosio and Mendis 556; Kulk and Snijders 50.

[81] Cf Joined Cases C-236/08 to C-238/08 *Google France/Louis Vuitton Malletier* [2010] ECLI:EU:C:2010:159, para 26, 114-115; Case C-324/09, *eBay* [2011] ECLI:EU:C:2011:474. For other examples, see Sartor 22. See also n 83

[82] Van Hoboken and others, *Hosting intermediary services and illegal content online* 39; Frosio and Husovec 625-627. See also Van Hoboken and others, *WODC-onderzoek* 54; Kulk and Snijders 48. Cf Frosio and Mendis 555, who claim that the decision to implement monitoring is at least partially motivated by a desire to avoid law suits.

[83] E-Commerce Directive, recital 40; Commission, 'Tackling Illegal Content Online' 10-13; Van Hoboken and others, *Hosting intermediary services and illegal content online* 41-42. Cf Section 1.2.1; Section 5.2.2.

[84] Cf Copyright in DSM Directive, art 17(4)(b); Section 3.3.4.1.

preventive filtering system at its own expense that applies to all content and which is capable of identifying copyright-protected works.[85]

This does not mean that no monitoring obligations exist. First, Article 15 of the e-Commerce Directive only applies to member states. The *European Union* may still and does indeed impose various monitoring obligations. These obligations are discussed in Chapter 3. Secondly, the e-Commerce Directive only prohibits a *general* obligation to monitor. Member states can still impose *specific* monitoring obligations, injunctions, requirements and duties of care.[86] It is therefore necessary to distinguish between general and specific obligations. Existing literature and interviewed stakeholders representing both intermediaries and victims emphasise that this delineation is not always clear.[87]

Glawischnig-Piesczek v Facebook demonstrates that the delineation should be approached teleologically.[88] The purpose of Articles 14 and 15 of the e-Commerce Directive is to prevent censorship and to strike a balance between the various interests (Sections 1.1 and 2.2.2). A member state is therefore not allowed to impose excessive monitoring obligations. Such an excessive obligation would exist if the hosting service provider is required to carry out an independent assessment of potentially illegal content. In contrast, there is no reason not to prevent the dissemination of illegal content if this can be done efficiently through automated search tools and technologies. A member state is therefore allowed to order a hosting service provider to search for and remove online content that is identical to content that was previously declared illegal. It can even extend this order to slightly different but equivalent content, but only as long as this does not require an independent assessment of the potentially equivalent content.[89] *Glawischnig-Piesczek v Facebook* therefore also illustrates that the delineation between general and specific monitoring obligations could change over time. If more sophisticated automated monitoring technologies become available, the responsibilities of hosting service providers can also be increased without creating a 'general' obligation to monitor or undermining the rationale of Article 14 of the e-Commerce Directive.[90] This also suggests that other obligations, such as a duty to prevent the removed content from being reuploaded (notice and stay down), may also be permissible as long as they can be performed efficiently and automatically.[91]

Just like Article 14, Article 15 is formulated as a *prohibition* (see also Section 2.2.1) of general monitoring obligations. It does not impose any specific monitoring obligations itself. This is left to the member states and various other European instruments for specific types of illegal content. For this reason, the existing obligations are different in each member state and for each type of illegal content (see also Section 4.2.3.3).

2.3.1.2. Monitoring in practice

Intermediaries use various techniques to automatically monitor the hosted information and detect illegal content and content that violates their terms and conditions (see also Section 2.2.2.2). Although most removed online content is detected through this monitoring, the automated mechanisms are (currently) not able to filter out all illegal content. This section gives a few examples and simple explanations of the more

---

[85] Case C-360/10 *SABAM* [2012] ECLI:EU:C:2012:85.

[86] See also e-Commerce Directive, art 14(3), recitals 45-48.

[87] About this issue, see also Stalla-Bourdillon 287 (claiming that Article 15 has become an empty shell); Ullrich, 'A risk-based approach towards infringement prevention on the internet' 229-232; Frosio and Mendis 546; Montagnani 310.

[88] Case C-18/18 *Glawischnig-Piesczek v Facebook* [2019] ECLI:EU:C:2019:821. About this teleological approach, see also Sartor 26; Stalla-Bourdillon 289, 291. About this case, see also Kulk, 'Platformaansprakelijkheid' 135.

[89] Case C-18/18 *Glawischnig-Piesczek v Facebook* [2019] ECLI:EU:C:2019:821, in particular paras 45-46.

[90] Sartor 26, 29-30; Ullrich, 'A risk-based approach towards infringement prevention on the internet' 230-231. Cf Joined Cases C-682/18 and C-683/18 *Youtube* [2020] ECLI:EU:C:2020:586, Opinion of AG Saugmandsgaard Øe, para 194-195, stating that such an obligation should only be imposed on hosting service providers that have the capacity to install such filters. Cf Section 1.5.4.

[91] DSA proposal 3-4. See also Sections 3.3.4.1 and 3.3.7.2.

common techniques, based on the interviews with representatives of online intermediaries and existing literature.[92] Furthermore, several representatives of online intermediaries emphasized that these practices are constantly changing and evolving.

First, it is possible to detect illegal online content that has been previously deemed illegal or that is included in a database of copyrighted or otherwise illegal works. This can be done by using 'hashes'. When a piece of content is deemed illegal and removed, for example because it infringes on copyright or contains child pornography, the 'hash' or 'hash value' of this content is stored in a database. When other content is uploaded, its hash can be compared with the values in the data base. If the value of the newly uploaded content matches a hash in the database, it is almost certainly[93] identical as the previously removed content and automatically removed. Similarly, if an intermediary removes a URL of a website that contains illegal information, the URL is also stored in a database.[94] Content providers can circumvent this monitoring through hash codes by slightly changing the content. Even minor changes lead to different hash values. However, new technologies also allow the detection of near-duplicates, for example by analysing various parts of the online content separately or by using a 'sketch' of the content.[95]

Next, techniques can be used to detect new illegal content. For example, it is possible to automatically flag 'prohibited' words that indicate illegal content. Machine learning can also be used to detect illegal content. For example, an algorithm can be trained to detect deep fakes by feeding it both real and manipulated videos and images. Similarly, hate speech can be detected by feeding an algorithm both illegal hate speech and permissible communication. Moreover, algorithms can also consider other factors, such as the behaviour of the account. For example, a new user that posts 20 messages in one hour to a single user can indicate a pattern of harassment.[96]

All of these techniques are also used semi-automatically, in combination with manual monitoring. A platform can use the techniques to automatically flag online content that *may* be illegal while using a human moderator to make the final decision.[97] Furthermore, several representatives of intermediaries stated that they use automated monitoring to put potentially illegal content on top of the queue, prioritising it for a human moderator. This hybrid system can also function as a protection of freedom of expression, freedom of speech and the rule of law by making sure that the automated systems (continue to) function fairly.

2.3.1.3. Notifications by third parties

Since a hosting service provider has no obligation to preventively monitor the hosted online content and automated techniques are not (yet) able to detect all illegal content, 'actual knowledge' or 'awareness' is often triggered by a third party (for example, a user of a platform or the holder of an IP-right) that notifies the hosting service provider of the illegal nature. For this reason, the obligation to remove illegal online content is frequently referred to as a 'notice and take down' (or more general: 'notice and action') obligation. However, 'actual knowledge' or 'awareness' is not limited to information that is obtained due to a notice. A hosting service provider is also unable to benefit from Article 14(1) of the e-Commerce Directive if it obtained the knowledge through another channel, such as voluntary monitoring (Section 2.3.1).

---

[92] See also Frosio and Husovec 622-625; Frosio and Mendis 556-557; Van Hoboken and others, *WODC-onderzoek* 54; Kulk, 'Platformaansprakelijkheid' 132-133; Kulk and Snijders 50, 53-54; De Streel and others 10, 44-45, 48-49.

[93] There is a small chance that different online content share a hash value.

[94] About the adoption of these measures by large platforms, see <https://gifct.org/joint-tech-innovation/> accessed 18 November 2020.

[95] Eg Charikar 380; Leskovec, Rajaraman and Ullman 73-134.

[96] Example given by one of the interviewees. See also Nguyen and others; Kulk and Snijders 53-55.

[97] See also Van Hoboken and others, *WODC-onderzoek* 54; Kulk, 'Platformaansprakelijkheid' 133; Kulk and Snijders 53, 56; De Streel and others 10, 40, 44-45, 64.

In *eBay*, the Court of Justice confirmed that a notification represents a factor which must be used to determine whether there was actual knowledge or awareness. However, notifications do not automatically preclude the exemption of Article 14 of the e-Commerce Directive because they may be insufficiently precise or inadequately substantiated.[98] This suggests that, *a contrario*, specific, detailed and adequately substantiated notifications generally do lead to such knowledge. This is further discussed in Sections 2.3.2, 5.2.5 and 5.3.1.4

Article 14 of the e-Commerce does not explicitly impose an obligation on hosting service providers to facilitate or respond to such notifications (and the subsequent takedowns).[99] This obligation is imposed for specific situations by other European rules, but also generally by various national laws and codes of conduct. The details of these national obligations vary from member state to member state.[100] For example, some member states place formal requirements on the notifications, only obligating hosting service providers to remove content when the notification contains certain information and/or is made by a competent authority.[101] In The Netherlands, criminal liability is only possible when a hosting service provider ignores an order from a public prosecutor, while private law liability may also be imposed when the actual knowledge or awareness is acquired through another channel.[102]

These formal requirements lead to a divergence between the liability that is allowed by the e-Commerce Directive and the liability that is actually imposed by the member states. Although the e-Commerce Directive allows liability for actual knowledge that is acquired through any channel (Section 2.3.1.1), various member states limit this liability to situations in which the knowledge is acquired through a notification that fulfils certain requirements.

2.3.1.4. Notice and take down in practice

Although no general European Notice and take down obligation exists (Section 2.3.1.3, but see also Section 4.2.3.2), (almost) all major online platforms implemented a procedure to facilitate notifications. This section gives a generalised description of how these systems work, based on existing literature and the interviews with both representatives of online intermediaries and other stakeholders.[103] Again (Section 2.3.1.2), several representatives of intermediaries emphasized that these practices are constantly changing and evolving.

Typically, these procedures allow a user to 'flag' illegal content by clicking a dedicated button and subsequently selecting the reason for the perceived illegality. If the notified content is indeed illegal, the platforms remove it. The effectiveness of a notice and take down procedure depends on its accessibility, which varies from platform to platform.[104] A streamlined user-friendly system can lead to more notifications and thus more removal of online content, but it could also lead to more unsubstantiated complaints.[105] The platforms typically have specific channels or procedures for law enforcement agencies and other privileged or 'trusted' flaggers.[106] They give special priority to the notifications of certain parties, including 'high accuracy' or otherwise dependable reporters such as NGOs or government agencies. Although most

---

[98] Case C-324/09, *eBay* [2011] ECLI:EU:C:2011:474, para 122.

[99] Kuczerawy 528, 530; Section 2.2.1.

[100] Commission, 'Impact Assessment Digital Services Act', points 93-99; Verbiest and others 41-47; Kuczerawy 530; Sections 3.4 and 4.2.3.2.

[101] Verbiest and others 14-15, 36, 42-46. See also Stalla-Bourdillon 291.

[102] Cf Dutch Criminal code, art 54a; Dutch Civil code, art 6:196c; Klos, par 1.

[103] Frosio and Mendis 556; De Streel and others 40, 46-51; Kulk and Snijders 49

[104] De Streel and others 40, 48-49, 51.

[105] De Streel and others 40, 47-48.

[106] On the usefulness of trusted flagging systems, see Husovec, 'The Promises of Algorithmic Copyright Enforcement' 81.

interviewees indicated that these systems generally work very well, a representative from an association of ISPs emphasised that this success can come at the expense of other notifications.

Although an interviewed representative from a consumer interest organization emphasised that large differences exist between the various platforms, most platforms are relatively fast. They claim to usually remove terrorist-related content and child pornography within one hour and other illegal content within 24 hours after the notification.[107] The content is therefore removed before the content providers have a chance to contest the notification. Furthermore, the content providers are not always notified or given a clear explanation about the reasons for the removal. Although most platforms do allow them to appeal against the removal of their online content through a 'counter-notice' procedure, the interviewed representatives of intermediaries insisted that these procedures only rarely lead to a reversal of the decision. Furthermore, one interviewee stated that it had temporarily disabled this option after the corona-pandemic made it more difficult to employ a sufficient number of moderators.

Several interviewed representatives of intermediaries emphasised that the biggest challenge of notice and take down, and monitoring generally, is the scale. Hosting service providers are faced with vast numbers of notifications. They are constantly looking for more efficient ways to process these notifications. Several interviewees emphasised that this is particularly hard for smaller intermediaries that lack the necessary expertise. Another noted that the unstructured nature of the online content on the platform caused challenges.

2.3.2. What knowledge is required?

The e-Commerce Directive is vague about what kind of knowledge is required to trigger 'actual knowledge' or 'awareness'. In *eBay*, the Court of Justice clarified that the knowledge should contain two elements: the online content and its illegality.[108]

First, the hosting service provider should have *specific knowledge about the online content* for which it is held liable. A hosting service provider cannot be assumed to know about all hosted content. Otherwise, Article 14 of the e-Commerce Directive would provide no protection. Furthermore, unless the service is specifically designed to facilitate the dissemination of illegal content,[109] a provider cannot be held liable because of the abstract knowledge that its service may be used for this purpose.[110]

Secondly, the hosting service provider should have actual knowledge or awareness *about the illegal nature* of this content. In most member states, a hosting service provider can only be held liable if the illegal nature is sufficiently clear or 'manifest'.[111] This approach prevents collateral censorship, but it also allows hosting service providers to escape or delay their responsibilities by claiming that the illegality of certain content is

---

[107] See also De Streel and others 44, 47, 49.

[108] Case C-324/09, *eBay* [2011] ECLI:EU:C:2011:474, para 122. About the distinction between these elements, see also Sartor 25.

[109] *Piratebay* B 13301-06 (Stockholms tingsrätt 2009); Joined Cases C-682/18 and C-683/18 *Youtube* [2020] ECLI:EU:C:2020:586, Opinion of AG Saugmandsgaard Øe, para 191; Van Hoboken and others, *Hosting intermediary services and illegal content online* 38-39; Frosio and Mendis 552.

[110] Case C-324/09, *eBay* [2011] ECLI:EU:C:2011:474, para 122; Joined Cases C-682/18 and C-683/18 *Youtube* [2020] ECLI:EU:C:2020:586, Opinion of AG Saugmandsgaard Øe, para 171-176, 182-184; Verbiest and others 37; Van Hoboken and others, *Hosting intermediary services and illegal content online* 38.

[111] Joined Cases C-682/18 and C-683/18 *Youtube* [2020] ECLI:EU:C:2020:586, Opinion of AG Saugmandsgaard Øe, para 187, 190; Verbiest and others 38-41; Stalla-Bourdillon 290; Klos, par. 1. Cf Gedragscode Notice-and-Take-Down 2018, art 6 (only imposing an obligation to remove 'unequivocally unlawful' content).

unclear. In contrast, more recent provisions such as § 3(2) such as the German NetzDG impose an obligation to remove any illegal content.[112]

In this respect, a distinction should be made between various types of uncertainty. Generally, ignorance of the law cannot be used as an excuse, '*ignorantia juris non excusat*'.[113] A hosting service provider is supposed to know whether online content is illegal or not, even if the law is unclear. Although this approach is consistent with the general principles of law, it is broadly argued that hosting service providers should not be the ones to make these complex decisions (Section 1.5.3). Ultimately though, this issue primarily depends on a trade-off between the removal of illegal content and the risk of collateral censorship. Liability for online content whose liability is hard to determine may induce hosting service providers to err on the side of caution (Section 2.2.2.2). In contrast, factual uncertainty should be an excuse.[114] For example, a hosting service provider could escape liability for hosting copyrighted content as long as it cannot know that someone else holds the copyright.[115]

Although liability requires knowledge about the illegal nature of the online content, other obligations may also exist without this knowledge. Most notably, specific knowledge about the online content and adequately substantiated and detailed information[116] of why it may be illegal can trigger an obligation to analyse the permissibility.[117] For example, a hosting service provider may be obligated to inform the notifier that it has insufficient information to determine the legality of the flagged content and to provide it with an opportunity to give more detailed information. Under such a system, even a notification that does not immediately and clearly demonstrate the illegal nature can still lead to a take down, or at least to an opportunity to provide more details that clarify the illegality.

The length of the period in which this obligation should be performed depends on various circumstances, such as reason for the illegality (shorter in case of very harmful illegal content such as child pornography[118]) and the difficulty of analysing the permissibility of the content (longer if it has to be done manually, if more information from the notifier is required or if the illegal nature is not clear-cut). The hosting service provider only loses the benefits of Article 14 of the e-Commerce Directive if fails to remove the manifestly illegal content after this period.

Finally, it is important to note that knowledge cannot trigger liability by itself. Pursuant to Article 14(1)(b), a hosting service provider can only be held liable if it does not act 'expeditiously' after obtaining this knowledge. In this sense, the required knowledge about the illegal nature and the meaning of 'expeditiously' are interconnected. The timeframe for 'expeditious' removal should be considered longer if actual knowledge is accepted more easily. For example, if a hosting service provider is presumed to have actual knowledge directly after receiving a sufficiently specific and detailed notification,[119] it will still have a short period to analyse the permissibility. In contrast, there is no reason to delay the removal if actual knowledge only exists when the hosting service provider is certain about the illegal character of online content. In both

---

[112] Note that uncertainty about the illegal nature does affect the period for the analysis of the permissibility. A provider 24 hours for obviously illegal content, '*offensichtlich rechtswidrigen Inhalt*', and seven days in other situations.

[113] About this principle, see generally Matthews; Husak.

[114] Cf NetzDG, § 3(2)3a) (granting extra time if the illegality depends on the truthfulness of factual statements).

[115] Cf Joined Cases C-682/18 and C-683/18 *Youtube* [2020] ECLI:EU:C:2020:586, Opinion of AG Saugmandsgaard Øe, para 188-189.

[116] Cf Case C-324/09, *eBay* [2011] ECLI:EU:C:2011:474, para 122; Stalla-Bourdillon 291; Verbiest and others 16.

[117] Joined Cases C-682/18 and C-683/18 *Youtube* [2020] ECLI:EU:C:2020:586, Opinion of AG Saugmandsgaard Øe, para 185. Specific and detailed notifications are also required for a 'notice and stay down' obligation. Cf Sections 2.3.1.3, 3.3.4.1; Kuczerawy 541-542.

[118] Cf Gedragscode Notice-and-Take-Down 2018, addendum 1, art 4 (imposing an obligation to remove within 24 hours).

[119] Cf Verbiest and others 44-46, about Finnish and French law.

interpretations, a hosting service providers does not (always)[120] have to immediately remove online content after receiving a notification.

2.3.3 When is the knowledge acquired?

Article 14(1) of the e-Commerce Directive only applies if there is 'actual' knowledge or awareness. 'Actual' implies that the threshold is high; it implies that hosting service providers can only be held liable if the knowledge or awareness is sufficiently 'real'. This issue encompasses several aspects. First, it is necessary to know *who* should have the actual knowledge (Section 2.3.3.1). Secondly, the threshold depends on whether 'objective' or 'subjective' knowledge is required (Section 2.3.3.2).

2.3.3.1. Who should have actual knowledge?

First, it is necessary to distinguish between 'computer' and 'human' knowledge. When a hosting service provider obtains information about potential illegal content, this information is typically first acquired through automated means. An automated monitoring technique detects (potentially) infringing content or a notification is issued through an online form (Sections 2.3.1.2 and 2.3.1.4). Under German law, such automated means do not lead to actual knowledge. Actual knowledge implies *human* knowledge.[121] Although this interpretation corresponds with the high threshold that is implied by 'actual', it should not mean that a hosting service provider can avoid liability by failing to transform this computer knowledge into human knowledge. The providers should at least have a (due diligence) duty to process notifications that are sufficiently specific and detailed (Sections 2.3.1.1, 2.3.1.3 and 2.3.2).

Next, hosting service providers can be large organisations, consisting of many employees. A hosting service provider does not have actual knowledge of everything that is known by any of its employees. For example, it should not be considered to have actual knowledge about the fact that one of its 10.000 knows about the dissemination of illegal content by one of its family members. It is not necessary here to provide an overview of the various national rules on imputation of knowledge to legal entities.[122] However, it is important to note that hosting service providers can make sure that knowledge finds its way to the responsible employees. Most notably, by facilitating an accessible notice and takedown procedure (see Section 2.3.1.4), hosting service providers can make sure that information about illegal online content is shared with the correct employees. With such a system in place, a provider could be excused if a letter to the office gets misplaced or an e-mail ends up in an employee's junk-filter. In contrast, a hosting service provider that does not facilitate notifications could be held to a stricter standard. Naturally, actual knowledge will also exist when the provider is informed through another relatively formal channel, such as a court summons.

Again (Section 2.3.2), the meaning of actual knowledge and 'expeditiously' are interconnected. If actual knowledge is presumed to exist when there is 'computer knowledge' or when the illegal content has been notified through other means than the dedicated notice and take down procedure, the period during which the hosting service provider should act 'expeditiously' should be considered longer.

---

[120] This may be different under certain circumstances. For example, removal should be faster if a hosting service provider receives many notifications in a short timeframe. For example, consider the live-streaming of a terrorist attack in Christchurch. See eg 'Christchurch attacks: Facebook curbs Live feature' (*BBC*, 15 May 2019) <www.bbc.com/news/technology-48276802> accessed 11 November 2020. Alternatively, a hosting service provider may be obligated to respond faster when a 'trusted flagger' notifies the provider. See Section 5.3.1.6.

[121] Verbiest and others 36-37; Van Eecke and Truyens ch 6, 18. Cf Stalla-Bourdillon 281.

[122] For a detailed analysis of the Dutch rules, see Katan.

2.3.3.2. 'Objective' or 'subjective' knowledge

According to Article 14(1) of the e-Commerce Directive, the obligation to remove illegal content is only triggered when the hosting service provider has *actual* knowledge about the illegal activity or information or if it *is* aware of facts or circumstances from which the illegal activity or information is apparent. A grammatical interpretation suggests that only real and existing ('subjective') knowledge of the illegal content triggers the exception to the exemption of liability. Under this interpretation, no liability can be imposed because a provider *should have* had ('objective') knowledge about the illegal content.[123]

This grammatical interpretation would make it very hard to hold hosting service providers liable. Generally, 'real' knowledge is hard to prove by others. For this reason, despite the use of the word 'actual', a hosting service provider can also be liable if it should have known about the specific illegal online content. Pursuant to the Court of Justice in *eBay*, a provider can be held to have 'awareness' if it knows about such facts or circumstances on the basis of which a diligent economic operator should have identified the illegality.[124] Still, the use of the terms 'actual knowledge' and 'is aware' suggest that this objective knowledge should not be presumed easily.[125]

2.3.4. Synthesis

The previous subsections show that various aspects about the meaning of actual knowledge or awareness under Article 14 of the e-Commerce Directive are unclear and implemented differently in the various member states. For this reason, it is not possible to give a universal *European* description of the criteria of 'actual knowledge' and 'awareness'. However, it is possible to formulate various aspects that could be clarified in the Digital Services Act:

a) Does actual knowledge only exist if the illegal nature is clear or 'manifest' (Section 2.3.2)?
b) Can ignorance of the law prevent the existence of actual knowledge if the law is unclear (Section 2.3.2)?
c) Does actual knowledge always require *human* knowledge? Or can actual knowledge also exist before the information is processed (Section 2.3.3.1)?
d) Under what circumstances should the knowledge of employees be imputed to the hosting service provider? Is this imputation harmonised? Is it affected by the existence of a notice and take down procedure (Section 2.3.3.1)?

The answer to these questions depends in part on the other obligations that can be imposed on hosting service providers. A member state cannot impose a general monitoring obligation (Section 2.3.1.1). However, the following question remains:

e) What kinds of monitoring obligations may be imposed on hosting service providers (Section 2.3.1.1)?

Actual knowledge cannot trigger liability by itself. A hosting service provider can only be held liable if it does not act 'expeditiously' after obtaining this knowledge. In the end, the secondary liability of hosting service providers depends on three interconnected factors: the obligations to analyse the permissibility of online content, the threshold for actual knowledge and the timeframe for 'expeditious' removal. For this reason,

---

[123] Joined Cases C-682/18 and C-683/18 *Youtube* [2020] ECLI:EU:C:2020:586, Opinion of AG Saugmandsgaard Øe, para 179; Van Hoboken and others, *Hosting intermediary services and illegal content online* 38.

[124] Case C-324/09, *eBay* [2011] ECLI:EU:C:2011:474, para 120. See also Joined Cases C-682/18 and C-683/18 *Youtube* [2020] ECLI:EU:C:2020:586, Opinion of AG Saugmandsgaard Øe, para 180. This rule is confirmed in DSA proposal, recital 22

[125] Cf Verbiest and others 37, discussing the requirement of *gross* negligence in German and Dutch law.

the questions should not be answered in isolation. If actual knowledge is accepted more easily, the timeframe for 'expeditious' removal should be longer (Sections 2.3.2 and 2.3.3.1). Conversely, if the threshold for actual knowledge is higher, hosting service providers should under certain circumstances have an obligation to analyse the permissibility of the online content (Sections 2.3.1.3 and 2.3.2). This leads to the following questions:

f) Under what circumstances does a hosting provider have an obligation to analyse the permissibility of (specific) online content? Specifically, when does a notification trigger such an obligation?
g) How much time after receiving information or acquiring actual knowledge or awareness can a hosting service provider take before it no longer acts 'expeditiously'?

2.4. Conclusion

The e-Commerce Directive plays a central role in the European framework for the liability and responsibility of hosting service providers. Article 14 provides an important exemption from liability. Member states (see Section 2.2.1) can only hold hosting service providers liable for hosting illegal content if those providers have actual knowledge or awareness of this content and fail to remove it expeditiously. This exemption stimulates the development of the internet and the information society and thus freedom of expression and information, effective communication and the development of all kinds of economic activities (Section 2.2.2).

This chapter provides an answer to question 1 (Section 2.4): *When does a hosting service provider have 'actual knowledge' or 'awareness' as referred to in Article 14 of the e-Commerce Directive?* The exact meaning of actual knowledge or awareness is one of the key factors that determine the scope of this exemption.[126] However, the e-Commerce Directive only provides limited clarification. It does not provide a clear and harmonised answer to these questions. Instead, it gives a lot of freedom to the member states (Section 2.3). Although the Court of Justice has given some guidance, questions and diverging implementations still remain. The Digital Services act could be used to clarify and harmonize these issues.

First, actual knowledge can be acquired through various channels. Most notably, they can be acquired through monitoring by the hosting service provider and through a notification of a rightsholder or other third party. Although some member states only hold the service providers liable for actual knowledge that is received through a specific channel, the e-Commerce Directive does not impose this restriction (Sections 2.3.1.1 and 2.3.1.3). Secondly, actual knowledge or awareness requires knowledge about two elements: the online content and its illegality (Section 2.3.2). However, it is not clear whether and under what conditions a provider can be held liable for online content that is not clearly or 'manifestly' illegal. Finally, not much is known about the threshold for actual knowledge or awareness. Although the Court of Justice has clarified that 'objective' knowledge can be actual knowledge (section 2.3.3.2), it has not answered the questions whether actual knowledge can be 'computer' knowledge and how knowledge should be imputed (Section 2.3.3.1).

This chapter also provides a part of the answer to question 2: *What role and responsibilities in relation to the limitation of the dissemination of illegal online content do hosting service providers have according to the various legislative and self-regulatory initiatives?*

The e-Commerce Directive does not only prevent member states from imposing liability in certain situations (Section 2.2.1). It also provides some clarity about the duties of care that can be imposed, including about duties that can lead to actual knowledge. Notably, Article 14(3) allows member states to impose notice and

[126] The other is the question what kinds of intermediaries qualify as a hosting service provider and under what circumstances. This question is discussed in Batura. See also Section 1.2.1.

take down obligations. This obligation has been implemented differently in the various member states (Section 2.3.1.3). Article 15 provides an important limit to the permissible duties of care by prohibiting general monitoring obligations. In contrast, member states may still impose specific monitoring obligations and specific duties of care (Sections 2.3 and 2.3.1.1). The delineation between general and specific monitoring obligations is not always clear and may change over time. The Digital Services act could be used to clarify this delineation and harmonize the monitoring obligations.

Finally, actual knowledge can only lead to liability when a hosting service provider does not act 'expeditiously' after obtaining this knowledge. The obligations to analyse the permissibility of online content, the existence of actual knowledge and the timeframe for 'expeditiously' are interconnected. For this reason, the issue of actual knowledge should not be clarified in isolation, but in combination with these other factors (Section 2.3.4).

The e-Commerce Directive forms an important part of the European framework. It provides a baseline that applies to all hosting service providers for all types of content. However, many other rules have imposed specific obligations for specific hosting service providers or specific forms of online content. These obligations are discussed in Chapter 3.

3. Overview of the legal framework

3.1. Introduction: describing the legal framework

This chapter provides an overview of the legal framework concerning the liability of hosting service providers by looking at the e-Commerce Directive (ECD) and the various other instruments that complement it by imposing additional obligations on hosting service providers. It looks at various types of instruments with a specific focus on the EU level. This chapter also addresses national legislation where relevant. In any case, the focus of the description of the legislative framework is on the obligations of the hosting service providers.

The European legal framework for the liability of hosting service providers can be characterised as asymmetric. Some rules have a horizontal scope, meaning that they apply to all types of content (or at least various types of content). Other rules are of a vertical nature. That is, they create obligations for a specific type of content and/or for a specific type of hosting service provider. On top of that, one has to make a distinction between binding instruments such as Directives and Regulations, and non-binding instruments such as soft-law (e.g., Recommendations), self-regulation (codes of conduct, codes of practice, Memoranda of Understanding, initiatives, etc.). The important role of soft-law and self-regulation results from the original ECD's support for self-regulation (Article 16, see also Section 2.3), and from the European Commission's explicit strategy to rely thereupon.[127]

This chapter starts with a description of the horizontal instruments (Section 3.2). Next, it discusses the vertical instruments (Section 3.3). Finally, it addresses various national rules (Section 3.4).

3.2. European Horizontal instruments

3.2.1. The e-Commerce Directive

There are some rules that are horizontal, that is, that apply to all hosting service providers and to all types (or various types) of content. The basic rule is Article 14 ECD, which provides for a regime of liability limitation concerning any type of illegal content. This provision is discussed in more detail in Chapter 2.

3.2.2. The Audiovisual media services Directive

A second instrument is the Audiovisual media services Directive (AVMSD), which was revised in 2018. Contrary to the ECD it is only partially horizontal in that it does not apply to all content, and, in the context of the limitation of the dissemination of illegal content online, only targets specific hosting service providers,

[127] Commission, 'Tackling Illegal Content Online' 4.

namely Video Sharing Platform services (VSPs).[128] VSPs must take two types of measures. The first type of measures must protect the general public from three specific types of illegal content under EU law (terrorist content, child pornography, and racism and xenophobia), as well as from incitement to violence or hate speech based on the illegal grounds of the EU Charter of Fundamental Rights (EUCFR), namely sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation.[129] The second type of measures must specifically protect minors from content which may impair their physical, mental or moral development.[130]

The Directive also lists a number of additional, specific measures that VSPs must take. These measures include transparent and user-friendly mechanisms to report and flag content;[131] systems allowing VSPs to explain to users what effect has been given to the reporting and flagging;[132] easy-to-use systems whereby users can rate the content offered;[133] establishing and operating transparent, easy-to-use and effective procedures for the handling and resolution of users' complaints.[134] The Directive explicitly explains that these measures are without prejudice to Articles 12 to 15 of the e-Commerce Directive.[135]

3.2.3. European Commission's 2018 Recommendation on Measures to Effectively Tackle Illegal Content Online

The third horizontal instrument is the European Commission's 2018 Recommendation on Measures to Effectively Tackle Illegal Content Online ("Recommendation"). Even though not binding, this Recommendation is considered an important policy document insofar as it builds upon and specifies the vision for the responsibilities of hosting service providers embedded in the European Commission's 2017 Communication on Tackling Illegal Content Online. This Communication lays down the European Commission's "new vision" for intermediary liability, which differs from the one embodied in the ECD. Instead of a reactive approach to illegal content underpinned by limited liability, the "new approach" argues that "what is illegal offline is also illegal online", and thus fosters an enhanced responsibility for hosting service providers (and in particular online platforms) who are in the best position to fight against illegal content.[136] This new vision therefore relies upon more anticipative actions by hosting service providers so

---

[128] AVMSD, art 1(1aa) defines the Video-Sharing Platform service as "a service as defined by Articles 56 and 57 TFEU, where the principal purpose of the service or of a dissociable section thereof or an essential functionality of the service is devoted to providing programmes, user-generated videos, or both, to the general public, for which the Video-Sharing Platform provider does not have editorial responsibility, in order to inform, entertain or educate, by means of electronic communications networks (...) and the organisation of which is determined by the Video-Sharing Platform provider, including by automatic means or algorithms in particular by displaying, tagging and sequencing". Beyond this specific context the AVMSD has a material scope going beyond VSPs, since it includes television broadcast, and on-demand audiovisual media services, see AVMSD, art 1(a)(i).

[129] AVMSD, art 28b (1)(b) and (c).

[130] AVMSD, art 28b (1)(a). This article defines content as "programmes, user-generated videos and audiovisual commercial communications".

[131] AVMSD, art 28b(3)(d)

[132] AVMSD, art 28b(3)(e)

[133] AVMSD, art 28b(3)(g).

[134] AVMSD, art 28b(3)(i).

[135] AVMSD, art 28b(1). See also Kukliš. The AVMSD is not considered a *lex specialis* as such, rather it complements what the e-Commerce Directive says within its scope of application, see Commission, Impact Assessment Digital Services Act, point 11.

[136] Commission, 'Tackling Illegal Content Online' 2.

that illegal content can be removed as fast and efficiently as possible. Such vision hinges upon a number of procedures and organisational measures such as close cooperation with competent authorities or trusted flaggers, but also on procedural safeguards (e.g., codified notice and take down procedures, information to content providers, enhanced transparency, safeguards in case of automated tools, etc.).[137]

According to the Commission, the provisions of the Recommendation build upon Article 14 e-Commerce Directive and embody its vision as to what hosting service providers should do in the face of illegal content, and it should constitute the bottom line of any regime for combatting illegal content.[138] Because of the importance of the Recommendation as an embodiment of the European Commission's vision of the e-Commerce Directive, its most relevant provisions are highlighted in the following paragraphs.

First, it provides for a notification system, which also includes the possibility of counter notices. The notice mechanism should be user-friendly (including by electronic means),[139] and should allow for notices that are sufficiently substantiated (e.g., reason for believing the content is illegal and indication on how to identify/locate the content).[140] Notifiers can provide their contact details but they should also have the possibility to remain anonymous.[141] In case the hosting service provider is aware of the notifier's contact information, it should confirm the reception of the notice and inform the latter of the decision taken concerning the notified content.[142]

The counter notification system of the Recommendation works as follows. If the hosting service provider decides to remove and/or disable the content, it should inform the content provider about this decision without undue delay, including the motivations underlying this decision and the possibility to contest such decision.[143] Once informed, content providers should have the possibility to contest the removal decision within a reasonable period of time. They can do so through a (user-friendly) counter-notice addressed to the hosting service provider.[144] Hosting service providers must take due account of the counter notice, which can therefore lead them to reverse (without undue delay) their decision on the removal of content.[145] This provision does however mention that the illegality of the content is not the sole criterion for the decision to remove the content. Hosting service providers have the discretion to remove the content that may not necessarily be illegal, if they consider that it violates their terms of service (see also Section 2.2.2.2). In any case, the hosting service provider should inform both the initial notifier and the counter-notifier of its final decision concerning the content.[146] It also provides for specific protection against notice trolling ("notices or counter-notices that are submitted in bad faith and other forms of abusive behaviour"), without providing

---

[137] Commission, 'Tackling Illegal Content Online' 20. See also Commission, 'Tackling Illegal Content Online' 3: "This Communication lays down a set of guidelines and principles for online platforms to step up the fight against illegal content online (…) It aims to facilitate and intensify the implementation of good practices for preventing, detecting, removing and disabling access to illegal content so as to ensure the effective removal of illegal content, increased transparency and the protection of fundamental rights online."

[138] Commission, 'Tackling Illegal Content Online'20.

[139] Recommendation on measures to effectively tackle illegal content online, point 5.

[140] Recommendation on measures to effectively tackle illegal content online, point 6.

[141] Recommendation on measures to effectively tackle illegal content online, point 7.

[142] Recommendation on measures to effectively tackle illegal content online, point 8.

[143] Recommendation on measures to effectively tackle illegal content online, point 9. A derogation to the previous provisions is provided in cases where the content is manifestly illegal and it relates to serious criminal offences (such as involving threats to life or to the safety of persons). The same derogation applies when public authorities request so for reasons of public security, and in particular as far as the investigation and prosecution of crimes is concerned, see point 10.

[144] Recommendation on measures to effectively tackle illegal content online, point 11.

[145] Recommendation on measures to effectively tackle illegal content online, point 12.

[146] Recommendation on measures to effectively tackle illegal content online, point 13.

much more details however.[147] Finally, the Recommendation encourages the use of out of court settlements in case of conflict over the removal of content.[148]

The recommendation couples the notification system with a trusted flaggers system by encouraging the setting up of fast-track notification procedures for trusted flaggers,[149] the publication of the conditions under which one can become a trusted flagger.[150] The latter include requirements in terms of expertise, diligence, and alignment with EU values.[151]

In addition to the notification system, the recommendation also encourages hosting service providers to take proactive measures including the use of automated tools for the detection of illegal content.[152] Resorting to proactive measures should be appropriate and proportionate, and the use of automated means should equally be appropriate and proportionate as well as subject to appropriate safeguards.[153] These safeguards require the hosting service provider to act in a diligent and proportional way,[154] to have some human oversight and verification "where appropriate", and to have a detailed assessment of the context.[155] The recommendation also requires both "adequate transparency concerning the take down policies",[156] as well as regular (possibly annual) reports on these take down policies.[157]

The Recommendation emphasises the need for cooperation. The cooperation is centred around three principles. Both member States and hosting service providers should establish points of contact.[158] In addition to the already discussed provisions on notices, fast-track procedures should be established for notices stemming from competent authorities.[159] Next, members states are encouraged to establish legal obligations pursuant which hosting service providers should provide competent authorities with any evidence of alleged criminal offences involving a threat to the life or safety of individuals, which they obtained whilst removing content.[160] The Recommendation also provides for cooperation amongst hosting service providers in the form of best practices sharing, including technological solutions. Such cooperation can take the form of codes of conduct, memoranda of understanding and other voluntary arrangements, and is explicitly intended for hosting service providers who operate on a smaller scale/of a smaller size and which have therefore fewer resources.[161]

On top of these general (horizontal) measures, the Recommendation also provides for specific rules for terrorist content online that are adapted to the specific characteristics of such content. They include specific transparency or cooperation measures (see also Section 3.3.1).[162]

---

[147] Recommendation on measures to effectively tackle illegal content online, point 21.
[148] Recommendation on measures to effectively tackle illegal content online, points 14-15.
[149] Recommendation on measures to effectively tackle illegal content online, point 25.
[150] Recommendation on measures to effectively tackle illegal content online, point 26.
[151] Recommendation on measures to effectively tackle illegal content online, point 27.
[152] Also when processing notices and counter notices, see Recommendation on measures to effectively tackle illegal content online point 19.
[153] Recommendation on measures to effectively tackle illegal content online, point 18.
[154] Recommendation on measures to effectively tackle illegal content online, point 19.
[155] Recommendation on measures to effectively tackle illegal content online, point 20.
[156] Recommendation on measures to effectively tackle illegal content online, point 16.
[157] Recommendation on measures to effectively tackle illegal content online, point 17.
[158] Recommendation on measures to effectively tackle illegal content online, point 22.
[159] Recommendation on measures to effectively tackle illegal content online, point 23.
[160] Recommendation on measures to effectively tackle illegal content online, point 24.
[161] Recommendation on measures to effectively tackle illegal content online, point 28.
[162] Recommendation on measures to effectively tackle illegal content online, points 40-42.

3.3. European vertical instruments

The EU legal framework contains a number of vertical instruments that contain specific rules for specific types of illegal content. The description therefore follows the type of content and mixes binding and non-binding instruments.

3.3.1. Terrorist content online

In the field of terrorist content online two instruments are relevant. The first one is the Directive on combatting terrorism (CTD). Article 21 CTD contains obligations directed at member states rather than at hosting service providers. It orders them to remove online content constituting a public provocation to commit a terrorist offence.[163] In case such removal is not possible, member states may block access to the content in question.[164]

These obligations have been transposed in various ways. As of September 2018, only 15 member states transposed the Directive, mainly through two types of measures.[165] On the one hand, they have adopted criminal procedural law provisions allowing prosecutors or Courts to order companies to remove the content or block the website within 24 to 48 hours. On the other hand, they have allowed law enforcement authorities to issue deletion orders and/or provided for (voluntary) referral procedures (from competent authorities to hosting service providers).

On top of the CTD, a Regulation on preventing the dissemination of terrorist content online (TERREG) has now been agreed upon by the European Parliament and the Council of the EU.[166] In contrast to the CTD, the agreed upon TERREG directly imposes obligations on hosting service providers.

The final compromise text imposes rules on "reasonable and proportionate duties of care" in order to address the dissemination of terrorist content.[167] It also includes a number of organisational measures (including cooperation with law enforcement authorities). The most relevant ones are detailed requirements for removal order procedures from competent authorities to hosting service providers (including a 1 hour removal delay and the establishment of a contact point for receiving such orders);[168] transparency measures (in the terms and conditions and annual transparency reports);[169] informing content providers of removal decisions, and the possibility for the latter to contest such decision before the hosting service provider through an internal complaint mechanism as well as to challenge the removal order from the competent authority;[170] cooperation between competent authorities, and between authorities and hosting service providers;[171] and notably a provision on proactive measures (now referred to as 'specific measures'

---

[163] CTD, art 21(1).

[164] CTD, art 21(2). In both cases, such measures must be transparent, provide adequate safeguards, in particular ensure that the restrictions are proportionate and limited to what is necessary, that users are adequately informed, and that they have the possibility of a judicial redress (CTD, art 21(3)).

[165] Commission, 'TERREG impact assessment' 116.

[166] See <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2372> accessed 04 February 2021.

[167] TERREG, art 1(1)(a).

[168] TERREG, art 4(2)

[169] TERREG, art 8.

[170] TERREG, art 9a, 10, 11.

[171] TERREG, art 12 and 13.

and including technical means to "identify and expeditiously remove or disable access to terrorist content")[172] and a related one including the required safeguards.[173]

Finally, the European Commission has created the EU Internet Forum against terrorist propaganda online in 2015. This Forum consists of representatives from the European Commission, member states and a number of hosting service providers such as Facebook, Twitter, Google, Microsoft, Dropbox, JustPaste.it and Snap. The Forum offers a framework for cooperation in the fight against terrorist content online. Its goals are to provide coordinated responses and facilitate private-public cooperation.[174]

3.3.2. Child sexual abuse material

Directive 2011/93/EU contains measures for combating the sexual abuse and sexual exploitation of children and child pornography (CSAED). Article 25 CSAED contains obligations directed at member states rather than at hosting service providers. It orders the member states to remove webpages that contain or disseminate child pornography,[175] and gives them the possibility to block access thereto.[176]

As far as the removal of content is concerned, two main types of measures have been adopted.[177] First, member states have implemented notice and take down procedures which rely upon national hotlines. Users can report the illegal content to these hotlines through national hotlines. INHOPE is an organisation which receives support from the European Commission and acts as the umbrella organisation for the national hotlines. The national hotlines work on the basis of memoranda of understanding with the corresponding national law enforcement authorities (LEAs). The latter determine the procedure to follow concerning the handling of users' reports.[178] In general, the follow-up on a notification will contain the following steps: determination of the hosting location, analysis of content, informing the hosting provider in view of the removal of content.[179]

Further, member states have adopted a number of criminal law provisions. These allow the seizing of material where relevant for criminal proceedings (e.g., material that is used to commit an offence), or may directly concern the removal of Child sexual abuse material (e.g., "prompt removal" orders, or within 12 hours).[180]

As far as the blocking of content is concerned, about half of the member states have also adopted blocking measures such as the blacklisting of websites. The blacklisting of a website typically involves a request from a competent authority (e.g., LEA) to the relevant intermediary, namely the service provider (ISP).[181]

---

[172] TERREG, art X(2).

[173] TERREG, art X(3).

[174] See, https://ec.europa.eu/commission/presscorner/detail/en/ip_19_6009, and also Commission, 'Consumer Protection Cooperation Action on Facebook's Terms of Service'.

[175] CSAED, art 25(1).

[176] CSAED, art 25(2). With such measures being transparent, providing adequate safeguards, in particular ensuring that the restrictions are proportionate and limited to what is necessary, that users are adequately informed, and that they have the possibility of a judicial redress.

[177] Commission, 'Assessing the implementation' 7.

[178] Commission, 'Assessing the implementation' 7. See also, INHOPE.

[179] Commission, 'Assessing the implementation' 7–8.

[180] Commission, 'Assessing the implementation' 8–9.

[181] Commission, 'Assessing the implementation' 10.

There are various initiatives in the field of child sexual abuse material. First, the Alliance to better protect minors online, created in 2017 under the auspices of the European Commission, groups together companies (service and hosting providers) and associations representing the rights of minors.[182] The goal of the Alliance is to protect minors from various types of online harms (e.g., violent content, cyberbullying, sexual extortion, etc.).[183] The goal of the Alliance is to complement the signatories' existing arsenal and to foster collaboration with other stakeholders (civil society, competent authorities, academia, etc.).[184] To that end, signatories aim to empower minors online (e.g., promoting reporting tools); to enhance collaboration with relevant stakeholders; and to raise awareness.[185]

Next, the WePROTECT Global Alliance was created in 2016 and includes states, international organisations, civil society, and technology companies. Its goal is to fight against the sexual exploitation of children online.[186] Its activities consist mostly in awareness-raising types of actions (e.g., securing high-level commitment, supporting comprehensive national action).[187]

3.3.3. Hate Speech

The only binding instrument is the 2008 Counter-Racism Framework Decision, which is binding on member states and requires them to criminalise two specific type of hate speech: "all conduct publicly inciting to violence or hatred directed against a group of persons or a member of such a group defined by reference to race, colour, religion, descent or national or ethnic origin". It is mentioned here insofar as it constitutes the only EU binding instrument on the topic, but it does not contain as such obligations for hosting service providers.

In 2016, at the initiative of the European Commission, some of the main platforms (Facebook, Microsoft, Twitter and YouTube) agreed upon a Code of Conduct on Countering Illegal Hate Speech online, with such hate speech as defined in the Counter-Racism Framework Decision ("The Code").[188]

The Code contains a number of procedural mechanisms. They include a system of notices based on the hosting service provider's terms and conditions (thus prohibiting so-called illegal hate speech).[189] Hosting service providers must review notifications within 24 hours.[190] Further, hosting service providers should provide publicly available information on how to submit a notice.[191]

Next, The Code explicitly relies upon civil society organisations to flag hateful content. Hosting service providers can support this trusted flagging system by providing training and support to the flaggers in order to ensure the quality of the notifications.[192] The Code of Conduct also foresees support from EU institutions

[182] See, Alliance to Better Protect Minors Online 5.
[183] Alliance to Better Protect Minors Online 1.
[184] Alliance to Better Protect Minors Online 2-3.
[185] Alliance to Better Protect Minors Online 4.
[186] WePROTECT Global Alliance 2.
[187] WePROTECT Global Alliance 8.
[188] Code of Conduct on Countering Illegal Hate Speech Online.
[189] Code of Conduct on Countering Illegal Hate Speech Online 2.
[190] Code of Conduct on Countering Illegal Hate Speech Online 2.
[191] Code of Conduct on Countering Illegal Hate Speech Online 2.
[192] Code of Conduct on Countering Illegal Hate Speech Online 2–3.

in order to ensure sufficient diversity concerning the civil society organisations that are selected as trusted flaggers.[193]

The Code requires hosting service providers to provide regular training to their staff, including on societal developments.[194] It also states that hosting service providers should educate and raise awareness about the type of content allowed under their terms of service.[195]

The EU Code of Conduct on countering illegal hate speech online expects hosting service providers to cooperate and share best practices.[196] It also provides for cooperation between hosting service providers and the European Commission with a view of promoting counter narratives against hate speech.[197] Hosting service providers should also cooperate with civil society organisations in order to create best practices for the training on how to counter hate speech, possibly with help from the European Commission.[198]

3.3.4. Intellectual property rights (IPR)

3.3.4.1. Copyright

In terms of copyright, the relevant instrument is the Copyright in the Digital Single Market Directive (CDSMD). It provides for a specific liability regime for online content-sharing service providers.[199] These hosting service providers are directly liable for hosting copyright infringing material,[200] unless they can show best effort to obtain authorization and best effort to take down content upon notification by the rights holder including efforts to make sure that the material cannot be re-uploaded (notice and stay down).[201]

Beyond issues of liability, the CDSMD also contains a number of organisational mechanisms. The Directive requires complaint mechanisms both at the internal level (where automated decisions can be contested based upon human review), and at the external level through an out of court or judicial redress mechanism.[202]

3.3.4.2. Counterfeit goods from an IPR perspective

As far as the IPR dimension of counterfeit goods is concerned,[203] no binding instrument that creates obligations for hosting service providers exists.[204] The only trace of an instrument adopted at EU level that does provide obligations for hosting service providers pertains to the 2011 Memorandum of Understanding

---

[193] Code of Conduct on Countering Illegal Hate Speech Online 2–3.
[194] Code of Conduct on Countering Illegal Hate Speech Online 3.
[195] Code of Conduct on Countering Illegal Hate Speech Online 3.
[196] Code of Conduct on Countering Illegal Hate Speech Online 3.
[197] Code of Conduct on Countering Illegal Hate Speech Online 3.
[198] Code of Conduct on Countering Illegal Hate Speech Online 3.
[199] See, CDSMD, art 17(3).
[200] CDSMD, art 17(3).
[201] CDSMD, art 17(4).
[202] CDSMD, art 17(4).
[203] We note that the term 'counterfeit goods' is an umbrella term that goes beyond IPR issues, see for instance OECD/EUIPO. Section 3.3.7 deals with other relevant aspects.
[204] Because this report focuses on the obligations for intermediaries, it does not address the broader IPR framework applicable to goods such as patents or trademarks, see for instance, OECD/EUIPO 69.

on the sale of counterfeit goods via the internet (which was updated in 2016 in order to include key performance indicators as a way to measure its success).[205]

The Memorandum's goal is to improve NTD measures, to promote proactive measures taken both by hosting service providers and rights holders[206] and to increase cooperation among relevant actors.[207] For this reason it contains certain requirements for the NTD procedure (e.g. efficient and effective procedures, contain the necessary information, submitted in good faith, examine without undue delay, exchange of information among hosting service providers on this matter);[208] proactive measures (both from the rights holders and the hosting service providers, including the transfer of rights holders' information to hosting service providers);[209] provisions on effective enforcement of IPR through adequate sanctions;[210] and various measures on cooperation (e.g., disclosed relevant information on sanctions to competent authorities, providing for cooperation with consumers to report counterfeit goods and identify sellers, or general cooperation between rights holders and hosting service providers).[211] It also provides for particularly close cooperation between rights holders and hosting service providers (in particular as far as proactive measures are concerned such as through the exchange of keywords).

3.3.4.3. Additional IPR instruments (1): the enforcement Directive and the InfoSoc Directive

Under the Enforcement Directive (and more in particular Article 11), it is possible for judicial authorities to issue injunctions against hosting service providers in case of IPR violations.[212] Similarly, the InfoSoc Directive contains specific rules for the enforcement of copyright infringements. More in particular, its Article 8(3) obliges member states to ensure that rights holders can apply for injunctions against hosting service providers when a third party uses their services in a way that infringes upon their copyrights (irrespective of whether the hosting service provider is directly liable for such infringement). According to van Hoboken and others, this provision has been key in shaping the ECD's safe harbour system as it is currently implemented.[213]

3.3.4.4. Additional IPR instruments (2):Memorandum of understanding on online advertising and intellectual property rights on the online advertising market

In June 2018, a memorandum of understanding on online advertising and intellectual property rights on the online advertising market was signed with the European Commission adopting a facilitating role in that regard.[214]

---

[205] See <https://ec.europa.eu/growth/industry/policy/intellectual-property/enforcement/memorandum-understanding-sale-counterfeit-goods-internet_en> accessed 20 December 2020. See also Memorandum of understanding on the sale of counterfeit goods via the internet.

[206] Even though the memorandum talks about rights owners, this report refers to rights holders for purposes of consistency. See, Memorandum of understanding on the sale of counterfeit goods via the internet 2.

[207] De Streel and others 31

[208] Memorandum of understanding on the sale of counterfeit goods via the internet, para 11-19.

[209] Memorandum of understanding on the sale of counterfeit goods via the internet, para 21-27.

[210] Memorandum of understanding on the sale of counterfeit goods via the internet, para 28-35.

[211] Memorandum of understanding on the sale of counterfeit goods via the internet, para 29-34.

[212] On this topic see Revolidis.

[213] Van Hoboken and others, *Hosting intermediary services and illegal content online* 43.

[214] See <https://ec.europa.eu/growth/industry/policy/intellectual-property/enforcement/memorandum-of-understanding-online-advertising-ipr_en> accessed 10 February 2021.

The goal of the memorandum of understanding is to minimise the placement of advertising on websites that offer goods that infringe IPR (e.g., copyright violations of counterfeit goods) on a commercial scale.[215] Signatories include advertisers (i.e., responsible for the placement of advertising), advertising intermediaries (i.e., involved in buying, selling or brokering the sale or purchase of advertising space), and also associations representing the interests of IP rights holders.[216]

The memorandum of understanding lays down obligations for advertisers and advertising intermediaries. It requires them for instance to take reasonable measures to minimise the placing of ads on relevant websites or to use tools for content verification before agreeing to broker advertising space.[217] After the first year of implementation, the memorandum is subject to a bi-annual review.[218]

3.3.5. Consumer protection

3.3.5.1. Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices

In the area of consumer protection, platforms may be used for unfair commercial practices. This issue is not regulated specifically, but in 2016 the European Commission issued a guidance document on the application of Directive 2005/29/EC on unfair commercial practices (UCPD) to platforms.[219] This "UCPD guidance" makes it clear that the rules of the UCPD apply to the online environment, and more specifically to the new business models created by online commercial platforms.[220] The UCPD applies to a platform when it qualifies as a trader under Article 2(b) UCPD. The guidance refers to various examples where a platform will qualify as a trader such as charging a commission on transactions between suppliers and consumers, providing additional paid services or even drawing revenues from targeted advertising.[221]

Once a platform qualifies as a trader it should comply with the rules on professional diligence pursuant to Article 5(2) UCPD. It should also comply with the transparency requirements enshrined in Articles 6 and 7 UCPD. The latter require that the platform abstain from misleading actions in cases where it acts as an intermediary for the promotion, sale or supply of a product to a consumer.[222] For example, an online platform should design its website in a way that enables third-party traders to present information to consumers in a way that is compatible with the UCPD. Notably, it should enable traders to make it clear to consumers that they, and not the platform, act as sellers.[223] This also means that it is prohibited for a platform to use a brand name as a key word when in fact the platform is not selling the products from the brand at stake.[224]

Among other hosting service providers that might need to take content curation measures pursuant to the UCPD (with the caveat that they qualify as a trader pursuant to the Directive), one can also mention search engines who should clearly distinguish natural search results from search results for which they have

---

[215] See Memorandum Of Understanding on Online Advertising and Intellectual Property Rights 1.

[216] Memorandum Of Understanding on Online Advertising and Intellectual Property Rights 1.

[217] Memorandum Of Understanding on Online Advertising and Intellectual Property Rights, para 4, 6.

[218] Memorandum Of Understanding on Online Advertising and Intellectual Property Rights, para 21.

[219] Commission, 'Guidance on the implementation/application of Directive 2005/29/EC on Unfair Commercial Practices' 109–137.

[220] Commission, 'Guidance on the implementation/application of Directive 2005/29/EC on Unfair Commercial Practices' 127–128; Montagnani 307.

[221] Commission, 'Guidance on the implementation/application of Directive 2005/29/EC on Unfair Commercial Practices' 110

[222] Montagnani 307.

[223] Commission, 'Guidance on the implementation/application of Directive 2005/29/EC on Unfair Commercial Practices' 114.

[224] Commission, 'Guidance on the implementation/application of Directive 2005/29/EC on Unfair Commercial Practices' 116.

received compensation[225] and platforms hosting user reviews which should take steps to verify the reliability of the reviews posted.[226]

3.3.5.2. Modernisation Directive

The so-called Omnibus or Modernisation Directive clarifies transparency requirements for online traders or online marketplaces. It also creates new information duties such as providing information concerning the method for ranking search results (e.g., key variables used to determine what is displayed to users), and the identity of the seller (consumer or professional trader) is explicitly labelled as essential information.[227] Note that the scope of the Directive is limited to traders (or businesses) to consumers relations[228] and that the Directive will be enforced starting on 28 May 2022.[229]

3.3.5.3. Joint Action of the consumer protection cooperation network authorities

The Consumer Protection Cooperation (CPC) is a network of national consumer enforcement authorities in EU and EEA countries operates under the steering of the European Commission in view of enforcing infringements of consumer protection legislation.[230]

As such, some of its coordinated actions are relevant in the context of the fight against illegal content online and the role of hosting service providers.[231] Several actions were taken against Facebook for instance. The latter was required to clarify under which conditions users are notified that their content has been taken down. It also agreed to inform users of their right to appeal take down decisions.[232]

3.3.6. Platform to business

The platform to business (or P2B) Regulation contains specific obligations for hosting service providers in relation to businesses. It contains a number of interesting provisions such as those concerning the terms of service transparency (drafted in plain and intelligible language, changes should be notified),[233] or the obligation to put in place an internal complaint-handling mechanism,[234] as well as the obligation to designate in the terms of service two or more mediators.[235] However, as far as the limitation of illegal content online is concerned this Regulation is of no direct relevance.

---

[225] Commission, 'Guidance on the implementation/application of Directive 2005/29/EC on Unfair Commercial Practices' 120–121.

[226] Commission, 'Guidance on the implementation/application of Directive 2005/29/EC on Unfair Commercial Practices' 126–128.

[227] Modernisation Directive, art 4(5).

[228] See UCPD, art 3(1).

[229] Modernisation Directive, art 7(1).

[230] See <https://ec.europa.eu/info/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/coordinated-actions_en#social-media> accessed 28 January 2021.

[231] In this regard it might be relevant to look at Recital 10 of the CPC Regulation, which allows consumer protection authorities to request any relevant information from intermediaries for the purpose of establishing whether violations of the Regulation have taken place. Of course, this is only a Recital that is not replicated in the operative part of the instrument.

[232] Commission, 'EU Crisis Protocol: Responding to Terrorist Content Online' 2.

[233] P2B Regulation, art 3(1)(a), 3(2).

[234] P2B Regulation, art 11.

[235] P2B Regulation, art 12.

3.3.7. Product safety

3.3.7.1. Market surveillance Regulation

The Market surveillance Regulation will enter into force in July 2021 and will replace the Accreditation and Market Surveillance Relating to the Marketing of Products Regulation as far as market surveillance is concerned. The goal of this Regulation is to better prevent the selling of (non-food) products that are illegal (in terms of health, safety or environmental aspects).[236]

This Regulation closes a gap as far as online trade and e-commerce are concerned. Until its adoption, only end users were considered importers of the imported products they buy online and thus formally responsible for the issue of whether the imported product is in compliance with EU law.[237] For this reason the market Surveillance Regulation reinforces the control on products entering the EU market.[238] As part of this reinforced control, this Regulation creates specific obligations for information society services. More in particular Article 7(2) requires them to cooperate with market surveillance authorities, including the facilitation of actions taken to eliminate or mitigate risks displayed by products available on the EU market and which were offered for sale through their services. Market surveillance authorities can also require them to provide access to their online interface as a last resort in order to avoid a serious risk and when no other alternative exists.[239]

Finally, the Rapid Information Exchange System (RAPEX) will be at play in case a potentially non-compliant product presenting serious risks travels through various member states. RAPEX will be used to exchange such information as is necessary for the identification of the product or the risks related to the product.[240]

3.3.7.2. Safety pledge for safety of products

The Product Safety Pledge is a voluntary initiative sponsored by the European Commission in order to improve the detection of unsafe products which are sold into the EU through these online marketplaces, especially given the possibility of non-EU manufacturers to sell their products on such marketplaces.[241] In June 2018, four online marketplaces signed Product Safety Pledge.[242] Since then three more have signed the Pledge.[243]

The Product Safety Pledge contains a list of 12 commitments. Among these, the most relevant ones are the creation of a clear notice and take down mechanism for customers to flag unsafe products (and response given within five working days) and including stay down measures; provide a single contact point for competent authorities to notify dangerous products (and possible removal within two working days); the commitment to consult existing databases containing information on unsafe products such as the RAPEX one; customers information; or special measures against repeated offenders.[244]

---

[236] See Market Surveillance Regulation, art 1(1).

[237] See <https://certification-experts.com/the-eu-market-surveillance-regulation-what-is-it-and-how-can-it-affect-your-business/> accessed 18 February 2021. As an aside, one can also mention the specific case of explosive precursors, which are specifically regulated, and which now also provide for specific duties for online marketplaces such as the reporting of suspicious transactions. See, Regulation on the marketing and use of explosives precursors, art 9.

[238] Market Surveillance Regulation, art 1(1) and 1(2).

[239] Market Surveillance Regulation, art 14(k)(ii).

[240] Market Surveillance Regulation, art 20.

[241] Product Safety Pledge 1.

[242] See, Product Safety Pledge. The original marketplaces are: AliExpress, Amazon, eBay and Rakuten France.

[243] Allegro, C-Discount, and Wish.

[244] Product Safety Pledge 2.

The Pledge also provides for bi-annual reporting on these commitments and on two Key Performance Indicators (KPIs).[245] Namely, the percentage of products removed on the basis of notifications by competent authorities, and the percentage of products removed based on the consultation of databases such as RAPEX.

3.3.8. Online disinformation

Following the European Commission's 2017 Communication, a number of important online platforms (Facebook, Google, Twitter, Mozilla and Microsoft) agreed upon a Code of Practice on Disinformation.[246] It contains a number of procedural provisions such as a type of trusted flagger system, which it refers to as "third party analysis of content", that is, a network of fact-checkers,[247] including "third party verification companies".[248] It also contains specific transparency measures such as requiring that political advertising is clearly distinguishable from editorial content. It also requires that hosting service providers publicly disclose the amount spent (and the sponsoring body) on content removal.[249]

The Code of practice also relies upon automated technology, not for the removal of content but for more "positive" purposes. It provides that algorithms should be used in order to redirect users towards "better content" and in so doing promote diversity of opinions.[250] This entails that hosting service providers should invest in technologies that are instrumental to these goals. Such technology could perform the following functions. It could allow people to make informed decisions when confronted with -possibly- fake online news (e.g., develop and implement effective indicators of trustworthiness). [251] Automated technology could also be used to classify information in search results, feeds, or other automatically ranked distribution channels in view of its relevance, authenticity and authoritative nature.[252] Technology should also be used in order to help people find more easily diverse sources about a given topic.[253]

Finally, it provides for cooperation between various stakeholders (hosting service providers, civil society, governments, editorial institutions) in order to support efforts aimed at improving digital media literacy and critical thinking.[254]

The scope of the Code of Practice on Disinformation is larger than the scope of this report. The Code of practice is not limited to the limitation of the dissemination of *illegal* online disinformation, it also applies to online disinformation that is *undesirable* without necessarily being illegal (see also Section 1.2.2). For this reason, it is not further discussed in this report.

---

[245] Product Safety Pledge 2.
[246] EU Code of Practice on Disinformation.
[247] EU Code of Practice on Disinformation, para 12.
[248] EU Code of Practice on Disinformation, para 18.
[249] EU Code of Practice on Disinformation, para 3.
[250] EU Code of Practice on Disinformation, para 9.
[251] EU Code of Practice on Disinformation, para 7.
[252] EU Code of Practice on Disinformation, para 8.
[253] EU Code of Practice on Disinformation, para 11.
[254] EU Code of Practice on Disinformation, para 10.

3.3.9. Data protection

The General Data Protection Regulation (GDPR) places restrictions on the processing of personal data. Various judgements by the European Court of Justice show that the GDPR also applies to personal data that is processed on online platforms. However, the relationship between the GDPR and the e-Commerce Directive is unclear. Article 1(5)(b) of the e-Commerce Directive states that the Directive does not apply to questions that are covered by (the predecessor of) the GDPR.[255] At the same time, Article 2(4) of the GDPR states that the Regulation is without prejudice to Articles 12 to 15 of the e-Commerce Directive. Moreover, it is not always clear whether and to what extent an hosting service provider should be considered the 'controller' of the personal data that is uploaded by content providers.[256]

A full analysis of these issues falls outside the scope of this report. However, it is important to note that the GDPR does impose additional obligations to limit the dissemination of illegal content. Insofar as the hosting service provider is a controller, it can be obligated to remove the personal data at the request of the data subject pursuant to Article 17 of the GDPR. Notably, data subjects can force search engines to remove websites that publish their personal data from the list of search results.[257] At the same time, the fact that the GDPR is without prejudice to Articles 12 to 15 of the e-Commerce Directive suggests that merely hosting illegal content containing personal data can only lead to liability if the hosting service provider fails to remove it after being notified.[258]

3.4. National legislation

Beyond the European legal framework, national legislation may also impose obligations within the limitations set by the e-Commerce Directive (Section 2.2.1). This report is limited to a small selection of these national rules.

3.4.1. The Netherlands: Notice-and-Take-Down Code of conduct

The Netherlands has adopted a code of conduct specifically dedicated to the notice and take down procedure.[259]

This code provides for the following procedure. Hosting service providers should have their own specific notification procedure in place, which are publicly accessible. These contain a number of elements such as the time limits to deal with notifications, or what is considered illegal content according to their own terms of use.[260] Notices to hosting service providers should contain a minimum amount of information such as the contact information of the notifier, reasons why the content is considered illegal and why approaching the hosting service provider was deemed the best solution, or where to find the content.[261] Notifiers can ask

---

[255] The Data Protection Directive. See also GDPR, art 94(2).

[256] About this issue see Case C-210/16, *Wirtschaftsakademie* [2018] ECLI:EU:C:2018:388; Case C-40/17, *Fashion ID* [2019]] ECLI:EU:C:2019:629.

[257] Case C-131/12 *Google Spain* [2014] ECLI:EU:C:2014:317.

[258] Cf Stalla-Bourdillon 284-286.

[259] Gedragscode Notice-and-Take-Down 2018. This code of conduct also touches upon the requests by law enforcement authorities.

[260] Gedragscode Notice-and-Take-Down 2018, art 3(a) and (b).

[261] Gedragscode Notice-and-Take-Down 2018, art 4(b).

for emergency considerations of their notice,[262] and hosting service providers can apparently claim some sort of compensation from the notifier as a result of investigating their claim.[263] Hosting service providers must determine whether the notified content is unequivocally unlawful (see also Section 2.3.2) or not. In case the content is unequivocally unlawful, the hosting service provider must immediately remove it. In case it is not unequivocally unlawful, the intermediary informs both the notifier and the content provider in the hope that the latter can reach an agreement on the disputed content. In case of a lack of agreement, the notifier always has the possibility to bring the dispute before courts (civil or criminal). It might also be the case that the content provider does not wish to share its contact information with the notifier, in which case the hosting service provider can decide to do so nonetheless of its own accord or to remove the content instead after all.[264]

3.4.2. France: Avia law

France recently adopted the Avia law to fight against online hate speech. Most of its far-reaching provisions have been struck down by the French Constitutional Council.[265] The provisions that were struck down were considered "not necessary, appropriate and proportionate to the aim pursued". On the basis, the Council quashed the requirement to remove content within 24 hours pursuant to a notice; the one hour deadline to remove terrorist and/or child sexual abuse material pursuant a removal order; the procedural obligations linked to the two previous provisions (e.g., transparency measures and redress mechanism); as well as the "*Conseil Superieur de l'Audiovisuel*"'s power to supervise the implementation of the latter mechanisms.[266] The remainder of the the notice mechanism has been preserved. It provides for more restrictive conditions than the other systems as far as the freedom and anonymity of the notifier are concerned. Contrary to the 2018 Recommendation which provides for the possibility to stay anonymous, the French system requires notifiers to indicate their name, electronic address (or for a legal person - private or public - its legal denomination) and electronic address.[267] The identification of the notifier can also be achieved if the latter is a registered user of the hosting service provider's service who is logged in at the moment of notifying (and the hosting service provider has gathered the sufficient elements to properly identify him/her).[268] The notification itself should contain a description of the contested content, its precise localisation, including the URLs where it is made available, and a legal motivation justifying the removal of content.[269]

The French Avia law also provides for cooperation through a multi-stakeholder forum that is meant to analyse content and follow the situation as far as online hateful content is concerned ("observatory of online hatred).[270] This observatory is composed of hosting service providers, civil society organisations, administrative bodies, and academics working in the field. It is under the tutelage of the "*Conseil Superieur de l'Audiovisuel*".

---

[262] Gedragscode Notice-and-Take-Down 2018, art 4(c).

[263] Gedragscode Notice-and-Take-Down 2018, art 4(d).

[264] See Gedragscode Notice-and-Take-Down 2018, art 6.

[265] See, Cons. const. n° 2020-801DC of 18 June 2020, Loi no 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet

[266] See also <https://edri.org/our-work/french-avia-law-declared-unconstitutional-what-does-this-teach-us-at-eu-level/> accessed 9 march 2021.

[267] Avia law art 2(I).

[268] Avia law art 2(I).

[269] Avia law, art 2(I).

[270] Avia law, art 16. Author's own translation.

Finally, it provides for a specific tribunal,[271] in cases of sexual or moral harassment in case they took place online,[272] when it is committed with the aggravating circumstance that it is based upon the victim's race or ethnic origin,[273] insofar as the plaintiff has complained via electronic means.[274]

3.4.3. Germany: NetzDG (Network Enforcement Act)

Informally referred to as "hate speech law",[275] the German NetzDG was adopted in 2017. Its goal is to improve the enforcement of existing criminal offences on large social media platforms.[276] This includes offences such as "distribution of child pornography", "incitement to hatred", "defamation of religions", "dissemination of depictions of violence", "forming terrorist organizations", or "use of symbols of unconstitutional organizations", but also violations of IPR to name a few.[277]

The NetzDG applies to large social media platforms with more than two million registered users in Germany,[278] with the exception of platforms that disseminate a specific type of content (e.g., a professional social network) and platforms publishing journalistic content.[279]

The NetzDG imposes a number of obligations on the concerned social media platforms. They must put in place a mechanism that enables users to notify illegal content.[280] Such procedures should be "effective and transparent", "easily recognisable, directly accessible and permanently available to users".[281] This includes the obligation to designate a representative in Germany in order to receive the notifications.[282]

Upon receipt of a notification, these platforms must investigate whether the content is indeed illegal.[283] The NetzDG makes a distinction between content that is "manifestly illegal" and other types of illegal content. The former must be removed within 24 hours, whereas the latter must be removed within seven days.[284] However, the seven days delay can be exceeded when further verification into the alleged illegal nature of the content is warranted, if the platform gives the content provider the possibility to discuss the case prior to taking a decision, or when the platform's own procedural mechanisms entail that a self-regulated body should decide on the illegal nature of the content.[285] Further, in case of removal the content should nonetheless be kept for ten weeks for evidence-related purposes.[286]

Finally, social media platforms are also subject to transparency requirements. On the one hand they are obliged to inform and motivate their decision both to the notifier and to the content provider.[287] On the

---

[271] Avia law, art 10. See also French Criminal Procedure Code, art 15-3-3.
[272] Avia law, art 10. See also, French Criminal Code, art 222-33 and art 222-33-2-2.
[273] Avia law, art 10. See also, French Criminal Code, art 132-76 and 132-77.
[274] Avia law, art 10. See also, French Criminal Procedure Code, art 15-3-1.
[275] Tworek and Leerssen 1.
[276] Tworek and Leerssen 2.
[277] NetzDG, § 1(3).
[278] NetzDG, § 1(1), (2).
[279] NetzDG, § 1(1).
[280] NetzDG, § 3(1).
[281] NetzDG, § 3(1).
[282] NetzDG, § 5. See also De Streel and others 89.
[283] NetzDG, § 3(2).
[284] NetzDG, § 3(2) points 2 and 3.
[285] NetzDG, § 3(2) point 3.
[286] NetzDG, § 3(2) point 4.
[287] NetzDG, § 3(2) point 5.

other hand, social media platforms who receive more than 100 notifications a year must publish bi-annual reports giving more insights into their content moderation practice (e.g., procedures, amount of complaints received, nature of actor who complained, amount of removal decisions and reason thereof, etc.).[288]

3.5. Conclusion

This chapter described the relevant legal framework for the limitation of the dissemination of illegal content online. Given the focus of Chapter 2 on the e-Commerce (see in particular Sections 2.2 and 2.3) this chapter focuses on the legal framework complementing this instrument. As a consequence, it focuses on the relevant instruments that create obligations for hosting service providers. It therefore provides the rest (see also Section 2.4) of the answer to question 2: *What role and responsibilities in relation to the limitation of the dissemination of illegal online content do hosting service providers have according to the various legislative and self-regulatory initiatives?*

Some rules have a horizontal scope, meaning that they apply to all types of content (or at least various types of content). Other rules are of a vertical nature. That is, they create obligations for a specific type of content and/or for a specific type of hosting service provider. On top of that, one has to make a distinction between binding instruments such as Directives and Regulations, and non-binding instruments such as soft-law (e.g., Recommendations), self-regulation (codes of conduct, codes of practice, Memoranda of Understanding, initiatives, etc.). Given the importance of binding law in the current European strategy to limit illegal content online (see Section 2.3), the chapter addresses both binding and non-binding instruments.

This chapter starts with a description of the horizontal instruments (Section 3.2). This section refers to three instruments. Namely, the e-Commerce Directive (very briefly) (Section 3.2.1), the Audiovisual Media Services Directive (Section 3.2.2), and the European Commission Recommendation on Measures to Effectively Tackle Illegal Content Online (Section 3.2.3).

Next, it discusses the vertical instruments (Section 3.3). This Section is divided by type of content. Section 3.3.1 addresses terrorist content online. It looks at the Directive on Combating terrorism, the Regulation on addressing the dissemination of terrorist content online, and the EU Internet Forum. Section 3.3.2 addresses Child sexual abuse material. It looks at the Children sexual abuse and sexual exploitation and child pornography Directive, the Alliance to better protect minors online, and the WePROTECT Global Alliance. Section 3.3.3 addresses hate speech. It looks at the Counter-Racism Framework Decision, and at the Code of Conduct on Countering Illegal Hate Speech online. Section 3.3.4 addresses intellectual property rights. It looks at the Copyright in the Digital Single Market Directive (Section 3.3.4.1); the Memorandum of Understanding on the sale of counterfeit goods via the internet (Section 3.3.4.2); the Enforcement Directive, the InfoSoc Directive (Section 3.3.4.3); and the Memorandum of understanding on online advertising and intellectual property rights on the online advertising market (Section 3.3.4.4). Section 3.3.5 addresses consumer protection issues. It looks at the European Commission's Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices (Section 3.3.5.1), at the Modernisation Directive (Section 3.3.5.2), and at the Joint Action of the consumer protection cooperation network authorities (Section 3.3.5.3). Section 3.3.7 addresses product safety. It looks at the Market surveillance Regulation (Section 3.3.7.1) and at the Product Safety Pledge (Section 3.3.7.2). Additional important instruments that are not directly relevant for the limitation of illegal content online are briefly mentioned. They include the Platform to business Regulation (Section 3.6), the EU Code of Practice on Disinformation (Section 3.8), and the GDPR (Section 3.9).

---

[288] NetzDG, § 2(1) and § 2(2).

Finally, Section 3.4 addresses various national rules. It looks at three relevant instruments. Namely, the Dutch Notice-and-Take-Down Code of conduct (Section 3.4.1), the French Avia law (Section 3.4.2), and the German Network Enforcement Act – NetzDG- (Section 3.4.2).

On the basis of this description one can already observe a number of important elements. First, there are only very few binding instruments with the aim of creating obligations for hosting service providers in order to limit the dissemination of illegal content online (basically the AVMSD and the CDSMD, while the TERREG has not been formally adopted yet). Other binding instruments do contain relevant obligations for hosting service providers but these obligations are just a part of the instrument (e.g., Modernisation Directive, Market surveillance Regulation). This also means that an important share of the EU legal framework for limiting the dissemination of illegal content online is left to non-binding instruments. On top of that, recently adopted national legislation creating obligations for hosting service providers concerning specific types of content (e.g., Avia law, NetzDG) further complicates the framework.

Second, these instruments often provide for overlapping obligations. Without providing an exhaustive description, it might be useful to signal that notice mechanisms are foreseen in a number of instruments (e.g., 2018 Recommendation, AVMSD, CDSMD, Code of Conduct on Hate Speech, Memorandum of Understanding on counterfeit goods, product safety pledge, etc.). Some instruments provide for redress mechanisms (e.g., AVMSD, CDSMD). Other instruments provide for proactive measures (e.g., 2018 Recommendation, TERREG, Memorandum of Understanding on counterfeit goods, or the product safety pledge and the CDSMD insofar as they concern stay down obligations). Yet, other instruments also provide for transparency measures (e.g., Code of Conduct on Hate Speech, TERREG), while others also foresee the possibility for trusted flagging (e.g., 2018 Recommendation, Code of Conduct on Hate Speech).

Chapter 4 discusses these differences in more detail. It will analyse the gaps of the current legal framework on the basis of this description combined with the findings of Chapters 1 and 2.

4. Gaps in the current legal framework

4.1. Introduction: meaning of a gap

In this chapter of the report we address question 3: *Can any gaps be discerned in the European framework for the liability and responsibilities of hosting service providers?* Section 1.4 has already defined what this report means by 'gap. For purpose of clarity, we reproduce it here.

A 'gap' is described as a situation in which the current framework is unjustifiably inconsistent or when the various involved interests are insufficiently safeguarded by the current legal rules. In both of these situations, the gaps are identified primarily by the previous analysis of the existing rules. This means that this chapter avoids to the extent possible to re-describe the rules at stake, and instead prefers to focus on the gaps as such.

Like cases should be treated alike. This maxim of justice holds especially true in the digital single market, where hosting service providers (and other businesses) should be able to offer their services throughout the European Union. As a starting point, the rules for intermediary liability should be the same in all member states, for all types of illegal content and for all types of hosting service providers. This is not to say that no relevant differences between the member states, types of illegal content and service providers can exist.[289] Relevant differences may form a justification for divergent rules. However, a gap exists when legal differences are not justified by relevant differences.

Gaps may also exist because the existing rules provide insufficient safeguards for the various involved interests discussed in Section 1.5. The legal framework for intermediary liability is designed to protect and balance various interests. However, an analysis of the existing legal framework can reveal that a particular interest is, generally or in relation to a specific type of online content or hosting service, insufficiently safeguarded by the current legal rules. This can refer to various situations. For instance, it can refer to the case where a rule does not exist where it ought to, but it can also refer to a case where a rule does exist but its interpretation is not clear thereby leading to a sub-optimal level of protection.

This chapter therefore identifies gaps that are considered as inconsistencies and gaps that are considered as missing safeguards.

As far as inconsistencies (Section 4.2) are concerned, this report identifies three main categories:

- Lack of consistent implementation of the legal framework (Section 4.2.1);
- Lack of comprehensive and harmonised definition of what counts as illegal content (Section 4.2.2);
- Diverging measures between the various instruments of the legal framework (Section 4.2.3).

As far as the missing safeguards (Section 4.3) are concerned, this report identifies five gaps:

- Lack of clarity concerning the criterion of actual knowledge (Section 4.3.1);

---

[289] As a matter of fact, the need to strive for unity of rules while catering to the specificities of certain type of content has been explicitly endorsed by the European Commission, see Commission, 'Tackling Illegal Content Online' 4.

- The nature of the procedural obligations to limit the dissemination of illegal content as well as the nature of the sanctions for their violation is not clear (Section 4.3.2);
- Lack of adequate safeguards for fundamental rights (Section 4.3.3);
- Lack of agreement as to what constitutes adequate procedural measures (Section 4.3.4);
- High compliance costs for SMEs (Section 4.3.5).

Some of these gaps are sub-divided into smaller gaps. For instance, the lack of consistent implementation of the legal framework concerns both the implementation of the instruments as such and the co-existence of binding and non-binding instruments. Similarly, the gap concerning the diverging measures touches upon various issues including a specific focus on notice mechanisms, the divergence of other procedural measures, or the need to possibly finer distinguish between types of illegal content. Equally, Section 4.3.4 regarding the lack of agreement on what constitutes adequate procedural measures makes a distinction between notice mechanisms and other procedural measures.

4.2. Inconsistencies

The first types of gaps that will be discussed fall under the umbrella of inconsistency. We identify various types of inconsistencies. There can be inconsistencies because the legal framework is not uniformly implemented, because it does not contain uniform definitions, or because it contains diverging measures (in particular procedural ones).

4.2.1. Lack of consistent implementation of the legal framework

We observe two main reasons as to why the legal framework is not always consistently implemented. The first reason pertains to the lack of uniform implementations of binding EU law (and in particular Directives) in the member states' legal order. The second pertains to the important role played by non-binding law. Because of its characteristics, non-binding law can also lead to the inconsistent implementation of rules.

4.2.1.1. Inconsistent implementation of the legal framework leading to a problematic fragmentation of the legal framework

Some Directives do not directly create obligations for hosting service providers and leave quite some discretion to member states in how they should be implemented. This leads to a fragmented, inconsistent, and disharmonised legal framework, which can be problematic.

This is particularly the case for the e-Commerce Directive, the Directive on combatting terrorism (CTD) and the Directive on combating the sexual abuse and sexual exploitation of children and child pornography (CSAED). The inconsistencies in the implementation of the e-Commerce Directive have been discussed in Section 2.4.

As far as the CTD and CSAED are concerned, Sections 3.3.1 and 3.3.2 have highlighted that the relevant provisions of both these Directives leave a large amount of discretion in terms of the measures to be adopted, including elements such as the offences covered, the time limits for removal and/or blocking, or the consequences of non-compliance.[290] Because of this lack of uniformity and because they do not directly target hosting service providers, these provisions lead to insufficient results.[291] This lack of uniformity has

[290] Commission, 'TERREG impact assessment' 116.

[291] Commission, 'TERREG impact assessment' 9–11.

for instance lead the European Commission to point to the need for a more consistent implementation of the CSAED Directive (Section 3.3.2).[292]

4.2.1.2. The co-existence of binding and non-binding instruments is inconsistent

As mentioned in Section 3.1, self-regulation and other forms of soft law (such as recommendations) can be said to result from the original e-Commerce Directive's support for self-regulation (Article 16), as well as from the European Commission's explicit strategy to rely thereupon.[293] However, relying upon non-binding instruments also has number of pitfalls.

First, one can point to the general lack of precision of soft-law provisions. It is indeed not possible to expect detailed provisions in soft-law instruments.[294] However, this lack of precision can be problematic insofar as it leads to an uneven implementation of the provisions. This can be the case with explicit transparency duties, which for the time being only exist in soft-law instruments complementing the e-Commerce Directive (see for instance Section 3.2.3 on the European Commission 2018 Recommendation, Section 3.3.3 on the Code of Conduct on Countering Illegal Hate Speech online – note that some transparency measures are foreseen in the TERREG but at the time of writing it is not formally adopted yet, see Section 3.3.1).

Second, because of their non-binding nature, soft-law instruments are not adhered to by everyone.[295] A recurrent lament about the Memorandum of Understanding on the sale of counterfeit goods on the Internet (MoU) concerns the number of signatories which remains too low.[296] The same holds true for the Code of Practice on Disinformation.[297] Even broadly supported instruments such as the Code of Conduct on Countering Illegal Speech Online might suffer from the same flaw. Beyond the initial signatories, Instagram, Google+, Dailymotion, Snap and Jeuxvideo.com have joined, meaning that "the Code now covers 96% of the EU market share of online platforms that may be affected by hateful content".[298] Still, new companies that have not signed (yet) may become larger. Further, other instruments have not achieved such widespread support. On top of that, even for those that have adhered to such code of conducts, their non-binding nature and vague obligations do not really allow effective or direct enforcement.[299] Similar criticisms have been voiced against the Dutch Notice-and-Take-Down Code of conduct.[300]

4.2.2. Lack of comprehensive and harmonised definition of what counts as illegal content

This second type of inconsistency refers to the lack of definitional agreement as to what exactly constitutes illegal content. The rules of the European Union only harmonize certain types of illegal content (ie some IPR, terrorist content, child pornography, racist and xenophobic hate speech) and only provides limited specific

---

[292] Commission, 'Assessing the implementation' 12.

[293] Commission, 'Tackling Illegal Content Online' 4.

[294] See, e.g., Senden.

[295] Commission, 'Impact Assessment Digital Services Act' 30.

[296] See, Commission, 'Report on the Memorandum'.

[297] See, ERGA.

[298] The Council of the European Union 2.

[299] Commission, 'Impact Assessment Digital Services Act' 30.

[300] See van Eijk and others 36. Of course, there are exceptions such as in the case of the UCPD, which under its article 6(2)(b) would make it an unfair commercial practice not to comply with codes of conduct to which they have committed in their commercial communications. However, this exception only applies within the scope of the UCPD (e.g., business to consumer relations).

rules on others (ie unfair commercial practices and product safety rules for online offers). Beyond these rules, the illegality of online content is left to the member states (Section 1.2.2). Furthermore, the current situation at member state level can be characterised as divergent on a number of topics such as freedom of expression for instance (e.g., some States prohibiting blasphemy, or different ways of implementing the prohibition of hate speech owing to local cultural factors) (Section 2.2.2.1).[301] Furthermore, the available EU-wide definitions are not always helpful. This is the case for hate speech, where the only instrument available is the Counter-Racism Framework Decision, which as seen in Section 3.3.1 only criminalises certain forms of hate speech against specific groups (see also Section 2.3.2 on the distinction between legal and factual uncertainty).

This lack of clarity as to what constitutes illegal content also has practical repercussions on the hosting service providers' limitation of illegal content online, since it hinders their ability to best allocate resources. In other words, the limitation of the dissemination of illegal content could be more efficient if there was more clarity as to what exactly should be prevented from being disseminated.[302]

This lack of clarity also leads to more restrictive content moderation policies. Given the uncertainty, hosting service providers often decide to go beyond the law, in order to avoid liability (Section 2.2.2.2) - or sometimes will not provide some content in some jurisdictions. The avoidance of over-removal of content is one of the rationales for Article 14 e-Commerce Directive (Section 2.2.2). Against this backdrop, Article 14 has not fully achieved this goal.[303]

4.2.3. Diverging measures

The third type of inconsistency refers to diverging procedural obligations for limiting the dissemination of illegal online content. This ranges from the lack of consistency between the procedural measures contained in the various instruments, to the diverging notice and action mechanisms at member states' level, the inconsistency of proactive monitoring obligations and to the lack of specific obligations for certain types of content (such as products violating intellectual property rights or product safety rules).

4.2.3.1. Inconsistency of the procedural obligations

The current EU legal framework for the limitation of the dissemination of illegal content online is a patchwork made of various types of instruments (i.e., binding, non-binding), providing for specific rules for different types of content. For instance, we have highlighted the diverging notice and action procedures in Sections 3.2.2, 3.2.3, 3.3.3, 3.3.3.4.1 and 3.3.4.2; the various transparency obligations in Sections 3.2.3, 3.3.1 and 3.3.3; the proactive measures in Sections 3.2.3 and 3.3.1; and the trusted flaggers systems in Sections 3.2.3 and 3.3.3. Representatives of industry and/or trade associations have argued that the need for differentiated rules should be based on clearer criteria, which at present is lacking.[304]

While fully harmonised rules are not necessarily a goal, given the need to cater for the specificities of certain types of content,[305] the current situation may hinder the limitation of the dissemination of illegal content online. The differences created by the various instruments in terms of timeframes, possibility of proactive measures including automated tools (see Sections 3.2.3, 3.3.1), upload filters (see Section 3.3.4.1) or

[301] See also Commission, 'Impact Assessment Digital Services Act' 13.

[302] Commission, 'Impact Assessment Digital Services Act' 24.

[303] See also Commission, 'Impact Assessment Digital Services Act' 19, 21.

[304] See De Streel and others 53.

[305] See also Commission, 'Tackling Illegal Content Online'; Section 1.4.

transparency requirements (see Sections 3.2.2, 3.3.1, 3.3.3) just to name a few create important legal uncertainty as well as increased compliance costs.[306]

Further, one can point out difficulties not only associated with the incoherence of the various procedural elements but also with the legal definition of hosting service providers which creates more confusion and legal uncertainty. For example, the notion of 'Video-Sharing Platforms' (VSP) in the AVMSD coexists with that of 'Online Content-Sharing Service Providers' in the CDSMD (see Sections 3.2.2 and 3.3.4.1). This creates an overlapping, complex, and inconsistent legal framework.[307]

4.2.3.2. Lack of harmonised procedure for notice mechanisms

In addition to the inconsistent procedures in specific instruments, the e-Commerce Directive does not prescribe any mechanisms for the removal of illegal content.

Article 14 e-Commerce Directive is a very broad and general provision, which as such does not impose any specific type of measure or mechanism.[308] Following the example of the US where the procedure is codified in the DMCA,[309] notice and take down procedures (NTD, or more generally Notice and Action – N&A) have become popular.[310] This procedure allows rights holders to directly contact the hosting service provider and ask them to remedy the situation (i.e., hosting of illegal content).[311] However, NTD is only implied in Article 14. The e-Commerce Directive only requires expeditious action in case of actual knowledge or awareness, but does not prescribe any type of mechanism or procedure (Section 2.3.1.3).

Because of this lack of detail, there is no uniformity in the NTD mechanisms implemented at member state level. One can distinguish between member states that have codified NTD procedures into their law and those that have not, and which therefore rely upon general rules of law or codes of conduct (see Section 2.3.1.3). To this day, an important number of member States have no codified NTD procedure. Among the countries that have codified such procedures (and which include Finland, France, Hungary, Lithuania, Sweden), there are also discrepancies in terms of scope (in terms of content or actors concerned) and in terms of procedure (e.g., timeframe, formal requirements).[312] Furthermore, some member states place formal requirements on the notifications, only obligating hosting service providers to remove content when the notification contains certain information and/or is made by a competent authority (Section 2.3.1.3).[313]

In terms of material scope, even though Article 14 e-Commerce Directive concerns any type of illegal content, the majority of codified NTD procedures concern copyright violation issues,[314] though member States seem to be broadening the scope of their mechanisms. For instance, Hungary has extended the original copyright-bound scope to include the rights of minors.[315] Similarly, the German NetzDG requires social media to remove any type of unlawful content following a complaint. However, this obligation only applies to social media and not to all hosting service providers (Section 3.4.3).

---

[306] De Streel and others 56–57. See also Commission, 'Impact Assessment Digital Services Act' 24, 25.

[307] Commission, 'Impact Assessment Digital Services Act' 29-30.

[308] See also Commission, 'Impact Assessment Digital Services Act' 28.

[309] See, Digital Millennium Copyright Act. On the origins of the notice and action mechanism see also van der Sloot.

[310] See Kuczerawy.

[311] Kuczerawy 526. See also Commission, 'Impact Assessment Digital Services Act' 28.

[312] Kuczerawy 528, 530. See also Verbiest and others 41-47.

[313] See also Commission, 'Impact Assessment Digital Services Act' 29.

[314] Kuczerawy 529 and the references contained therein.

[315] Kuczerawy 529. For other examples of discrepancies between national legislations see also Commission, 'Impact Assessment Digital Services Act' 28-29.

4.2.3.3. Inconsistency of proactive monitoring obligations

Article 15 of the e-Commerce Directive prohibits member states from imposing general monitoring obligations. Section 2.3.1.1 has highlighted the difficulties associated with monitoring obligations, and more in particular the issue of determining what constitutes a general monitoring obligation and what is sufficiently specified so as not to constitute such an obligation. For example, the European Court of Justice suggests but does not explicitly state that a notice and stay down obligation is possible.[316]

Beyond this open legal question, there are also inconsistencies between the existing provisions imposing proactive measures. This is the case for the European Commission's 2018 Recommendation (Section 3.2.3), the TERREG (Section 3.3.1), the CDSMD (Section 3.3.4.1) and the Memorandum of understanding on the sale of counterfeit goods via the Internet (Section 3.3.4.2). Whereas the Recommendation mentions the detection of illegal content,[317] the TERREG mentions the detection and expeditious removal of illegal content,[318] the Memorandum of Understanding refers to the active monitoring[319] and the CDSMD is the only binding instrument clearly pointing to a notice and stay down mechanism (while the Product Safety Pledge also foresees one but is not binding).[320] This inconsistency is problematic on the account of the general issue of the inconsistency between measures from separate specific instruments (Section 4.2.3.1), but also owing to the legal uncertainties surrounding proactive –monitoring– measures.

Such inconsistency can be linked to the controversial status of proactive measures.[321] Such controversy can be observed in the shifting position of the European Commission on the topic. In earlier stances it explicitly supported proactive measures based on automated tools for content detection and removal including re-upload filters,[322] which translated among others into the provisions of the 2018 Recommendation on proactive measures and automated tools (Section 3.2.3). Its -more recent- DSA proposal retains the prohibition of general monitoring obligations (Section 5.2.3). In any case, and in spite of this contested legal status, hosting service providers do resort to automated tools in practice (Section 2.3.1.2).

4.2.3.4. Lack of specific obligations for certain types of content

So far, we have identified several gaps due to *unjustifiably* inconsistent and diverging rules. This is not to say that no relevant differences between the member states, types of illegal content and service providers can exist (Section 1.4). Many different types of hosting service providers and types of online content exist (Sections 1.2.1 and 1.2.2), and they may require specific rules that are not always imposed by the current framework.[323]

In its Resolution "Digital Services Act: Improving the functioning of the Single Market", the European Parliament has emphasised that online marketplaces should be distinguished from other types of hosting service providers.[324] This points to the distinction between the mere hosting of content and the role of online marketplaces, which are deeply integrated in the process of online sale even though the sales contract is formed between two other parties.[325] As such they should be subject to additional obligations to

---

[316] Section 2.3.1.1. See also Kuczerawy 538, and Commission, 'Impact Assessment Digital Services Act' 31-32.

[317] Recommendation on illegal content, art 18.

[318] TERREG art X(2)(a).

[319] Memorandum of understanding on the sale of counterfeit goods via the Internet, para 21.

[320] See CDSMD art 17(4)(c).

[321] See for instance, Schmon.

[322] See, e.g., Commission, 'Tackling Illegal Content Online' 12–13, 19.

[323] Cf De Streel and others 58.

[324] European Parliament, 'Improving the single market' Annex VI.

[325] European Parliament, 'Improving the single market' Annex III.

limit the dissemination of illegal content online that match their level of involvement.[326] This point was also made by one of the interviewed stakeholders representing consumer interest organisations. These new obligations should come on top of the existing legal framework discussed in Chapter 3. Note that legislation in the field of counterfeit goods, product safety, and consumer protection specifically targeted at hosting service providers (Sections 3.3.4.2, 3.3.4.4, 3.3.5.1, 3.3.7.2) is mostly non-binding with the exception of the Market Surveillance Regulation (Section 3.3.7.1) and the Modernisation Directive (Section 3.3.5.2). Both the Market Surveillance Regulation and the Modernisation Directive contain a limited set of obligations for hosting service providers and it therefore remains to be seen whether these will be sufficient.

Furthermore, interviewed stakeholders representing organisations with an interest in removing certain types of illegal content (children abuse material including pornography and counterfeit goods infringing on IPR) argue that the limitation of the dissemination of the type of illegal content they deal with requires imposing obligations on actors that are not at the forefront of the current legal framework. This requires focusing on website hosting providers rather than platforms. Even though both fall under Article 14 of the e-Commerce Directive, there are differences between these two types of hosting providers that should be better taken into account.

4.3. Lack of adequate safeguards

The second type of gaps refers to the lack or absence of safeguards in order to adequately protect one of the interests identified in Section 1.5. The legal framework for intermediary liability is designed to protect and balance various interests. However, an analysis of the existing legal framework can reveal that a particular interest is, generally or in relation to a specific type of online content or hosting service, insufficiently safeguarded by the current legal rules. As indicated in section 4.1 a lack of sufficient protection can have a plurality of causes. it can refer to the case where a rule does not exist where it ought to, but it can also refer to a case where a rule does exist but its interpretation is not clear thereby leading to a sub-optimal level of protection (of possibly various interests).

Our analysis reveals various gaps. Namely, a lack of clarity concerning the criterion of actual knowledge that underpins Article 14 e-Commerce Directive; a lack of clarity concerning the nature of the procedural obligations to limit the dissemination of illegal content as well as the nature of the sanctions for their violation; a lack of safeguards for fundamental rights; a lack of agreement as to what constitutes an adequate procedural measure to limit the dissemination of illegal content online; and high compliance costs for SMEs.

4.3.1. Lack of clarity concerning the criterion of actual knowledge

Section 2.3 shows that various aspects about the meaning of actual knowledge or awareness are unclear and disharmonised. Section 2.3.4 formulates various aspects that remain unclear and should be clarified. We refer to that Section for a more detailed analysis of the various unclarities.

This report has concluded that the current legal framework does not provide a clear answer as to what exactly the meaning of actual knowledge is (Section 2.3). More specifically this report emphasised that it is not clear under which conditions hosting service providers acquire actual knowledge (both in the case of the monitoring of content and the notification by third parties, Sections 2.3.1.1, 2.3.1.3). It also showed that the criterion concerning the type of knowledge required, and in particular the knowledge concerning the

[326] See for instance, European Parliament, 'Improving the single market', para 60-67.

illegality of the content is far from a clear-cut notion especially because it is so intertwined with the obligation to act "expeditiously" –another less than clear term. Along the same lines, it is hard to find the right balance between the need for accurate and speedy removal (Section 2.3.2). Finally, the report also underlines the difficulties in determining when such knowledge is acquired. It highlighted the current uncertainties regarding whether knowledge by machines is sufficient, or regarding who precisely within a company should actually possess the knowledge (Section 2.3.3.1). Finally, uncertainty persists as to whether the hosting service provider needs to have the knowledge or if it suffices that it is in a position whereby a normally diligent actor would acquire such knowledge (Section 2.3.3.2).

4.3.2. The nature of the procedural obligations to limit the dissemination of illegal content as well as the nature of the sanctions for their violation is not clear

As Section 2.2.1 emphasises, one should distinguish between liability under Article 14 e-Commerce Directive, and liability in relation to the various procedural obligations created by the EU legal framework. However, the legal nature of the additional procedural obligations (e.g., NTD, transparency, etc.) is not clear, and as a result the sanctions in cases of violations thereof aren't either.

For instance, these procedural obligations have often been referred to as "duties of care",[327] which can be misleading not least because it may mean different things depending on the member state and the legal system.[328] The notion of duty of care is often associated with private law liability,[329] which is why authors like Koelman have stated that a violation of a duty of care "may constitute an unlawful act or a tort in itself, or may play a role in the requirement of fault and therefore result in liability".[330] Because of this link with private law liability, resorting to the concept of duty of care in the context of the fight against illegal content online has been an ongoing source of confusion as to what this means for the hosting service providers' liability.

Regardless as to whether these obligations are qualified as a duty of care or not, the confusion persist because of the lack of clarity and harmonisation of the sanctions for the violation of these duties in the relevant EU instruments. As far as procedural obligations are concerned, the most relevant instruments are the CDSMD, the AVMSD, and the TERREG since they are the only binding instruments providing for these types of procedural mechanisms (even though the TERREG is not formally adopted yet). The AVMSD and the CDSMD do not contain specific provisions on sanctions in case of violation of the procedural obligations they impose, thus leaving complete discretion to member states on that matter. The TERREG contains a provision specifically dedicated to sanctions in case of violation of these obligations.[331] The provision simply requires member states to adopt effective, proportionate and dissuasive penalties.[332] Such language does

[327] Van Hoboken and others 43.

[328] Note that the final compromise version of the TERREG has replaced the general duty of care with a concept of 'specific measures', while the DSA proposal refers to a due diligence duty, thus sustaining the confusion. TERREG, art X(1); DSA proposal, art 1(1)(b).

[329] See for instance, Van Dam.

[330] Koelman 11.

[331] TERREG, art 18.

[332] TERREG, art 18(2).

not clarify or provide rules on private law liability for a violation of procedural obligations. This is left to the member states.[333]

This legal uncertainty and the (potential) fragmentation can adversely impact the various involved interests. First, it leads to uncertainty for hosting service providers (Section 1.5.4). In this regard, a number of scholars have emphasised that these sanctions should be limited to criminal law and/or public law types of sanctions.[334] Private law liability for these types of violations (e.g., private law duty to help prevent copyright infringement) might blur the lines with the secondary liability under Article 14 e-Commerce Directive (a similar point was made by an interviewed representative of a digital rights organisation).[335] More specifically, the fear of a very strict liability for a violation of procedural obligations could lead to collateral censorship (Section 2.2.2) and thus adversely impact fundamental rights and freedoms (Section 1.5.2). This would be even more so if the hosting service provider would think that such liability would be the same as that under Article 14 e-Commerce Directive.

On the other hand, the absence of harmonised private law liability also adversely impacts the protection of the victims of illegal content. A violation of the procedural obligations may cause illegal content to be disseminated for a longer time before the hosting service provider acquires actual knowledge and removes it. Without private law liability, a victim cannot get compensation for the additional harms that are caused by this delay. In the absence of liability, hosting service providers are also insufficiently incentivized to fulfil their obligations.

4.3.3. Lack of adequate safeguards for fundamental rights

As discussed in Sections 1.5.2 and 1.5.3, online content moderation poses risks to the protection of fundamental rights and the rule of law. These risks can be mitigated by imposing safeguards such as procedural mechanisms. However, it seems that the current legal framework does not always adequately safeguard the various rights at play.[336]

A first gap pertains to the delays for the deletion of content which in some cases can be too short. This is the case under the TERREG, in which hosting service providers will have to respond to removal orders within one hour (Section 3.3.1). The stringency of such a short delay could lead to over-removal.[337] In France, a similar provision in the AVIA law was struck down by the French Constitutional Court on grounds that it was disproportionate (Section 3.4.2).

Further, key issues concern safeguards pertaining to rights such as the right to a fair hearing, adversarial proceedings, and equality of arms (Section 1.5.3).[338] A useful safeguard in this regard consists in the possibility to inform content providers of the (planned) decision to remove content and to give them the possibility to submit counter notices. However, such a mechanism is not always imposed at the level of member states' law, see for instance the situation in Finland, Hungary (note that such a possibility exists in the Dutch Notice and Take Down Code of Conduct but only in case the content is not unequivocally

---

[333] Note that art 18(4) of TERREG provides specific penalties in case of 'systematic or persistent failure to comply', but this doesn't clarify the issue at stake any further.

[334] See for instance, Edwards 10.

[335] Van Hoboken and others 44. For further examples on this confusion, see, Angelopoulos, *European intermediary liability in copyright* 94–95. See also Yordanova Trapova and Montagnani.

[336] Commission, 'Impact Assessment Digital Services Act' 18.

[337] Van Hoboken 8.

[338] Kuczerawy 535.

unlawful, see Section 3.4.1).[339] At EU level, no binding instrument provides for this possibility (Section 3.2.3). This absence is particularly problematic since many view counter notices as having a key role to play in order to render the content moderation process more transparent and fairer.[340] This report has noted that in practice, many platforms provide for counter notice procedures, but not all hosting service providers inform content providers of their decision to remove content (regardless of the possibility to submit a counter notice), nor do they provide a statement of reasons (Section 2.3.1.4).[341]

Other important safeguards are those allowing for adequate remedies, and in particular complaint and redress mechanisms.[342] At present, only two EU binding instruments provide for complaint and redress mechanisms, the AVMSD and the CDSMD (Sections 3.2.2 and 3.3.4.1). The CDSMD requires the setting up of an effective and expeditious complaint and redress mechanism",[343] but it remains unclear how exactly member States will implement such mechanism.[344] Similarly, the AVMSD requires the "establishing and operating transparent, easy-to-use and effective procedures for the handling and resolution of users' complaints",[345] and what this means in practice remains unclear here too.[346] Beyond the lack of clear criteria that would give a better idea of the adequacy of the implementation at member states level, one should keep in mind the narrow scope of these instruments. Meaning that even if adequate mechanisms were put in place pursuant to these two instruments their scope would nonetheless remain limited. As far as hosting service providers are concerned, an interviewed representative of an online intermediary confirmed that they are still working on an internal complaint mechanism, but this is ongoing work. The TERREG, though not yet in force, on the other hand provides for an internal complaint-handling mechanism (Section 3.3.1), thereby creating more discrepancy between the various existing possibilities.

Specific attention must be dedicated to safeguards concerning the use of automated tools for the detection and deletion of content (Sections 1.5.2 and 1.5.3). The inconsistency with which automated tools are addressed in the legal framework has been addressed in Section 4.2.3.3. This section focuses on the issue of safeguards.

First, and as Section 4.2.3.3 has shown, automated tools are little regulated but are nonetheless used in practice. In this regard, Section 2.3.1.2 mentioned the possible risks for fundamental rights in case hosting service providers resorting to these tools do not implement adequate safeguards, and also mentioned one possible safeguard whilst acknowledging that there is no clear-cut answer on the matter. This concern is particularly salient as far as the CDSMD is concerned since it provides for notice and stay down obligations (see Section 3.3.4.1), which in practice will very likely involve the use of upload filters i.e., automated tools.[347] Thus, even though the provision does not explicitly require the use of automated tools, there are strong chances that it will lead to the *de facto* use thereof. And critically, it does not contain any provisions on what the adequate safeguards would be in relation to the use of such automated tools.

---

[339] Kuczerawy 531, 535.

[340] De Streel and others 49.

[341] Commission, 'Impact Assessment Digital Services Act' 19, 26.

[342] Commission, 'Impact Assessment Digital Services Act' 26.

[343] CDSMD, art 17(9).

[344] Kuczerawy 542. Concerning the divergences in the implementation of Art 17 CDSMD, see Larroyed. Note that CDSM art 17(9) also obliges member states to put out-of-court mechanisms in place.

[345] AVMSD Article 28b(3)(i).

[346] According to the Council of Europe the transposition of the Directive at member states level is still an ongoing process, see <https://www.obs.coe.int/en/web/observatoire/home/-/asset_publisher/9iKCxBYgiO6S/content/which-eu-countries-have-transposed-the-avmsd-into-national-legislation-?_101_INSTANCE_9iKCxBYgiO6S_viewMode=view/> accessed 7 February 2021.

[347] Husovec and Quintais 3.

Second, the provisions in the EU instruments that do regulate automated tools and contain safeguards are insufficient.[348] The 2018 Recommendation on tackling illegal content states that automated tools should be subject to effective and appropriate safeguards, but it remains rather vague on what these safeguards are (Section 3.2.3). Beyond a general duty to use them in a proportionate and diligent way,[349] the Recommendation recommends the use of effective and appropriate safeguards in order to achieve accurate and well-founded decision (vague language), which should include the use of human oversight and verifications "where appropriate".[350] As far as terrorist content is concerned, the level of safeguards is even lower since it only refers to "proportionate and specific measures".[351] The European Commission's proposal for the TERREG contained a similar list of safeguards as that of the Recommendation, which has been criticised by van Hoboken on similar accounts of vagueness.[352] Van Hoboken's criticism is equally applicable to the final compromise text.[353]

4.3.4. Lack of agreement as to what constitutes adequate procedural measures

Providing for procedural obligations to limit the dissemination of illegal content online is one thing. Another thing is to make sure that the law provides for mechanisms that are efficient and adequate in achieving their goals. This section looks at this type of shortcoming concerning a variety of mechanisms. It starts with notice and action procedures before also addressing other mechanisms.

4.3.4.1. Lack of agreement on notice mechanisms

There are very few instruments at EU level that explicitly require the use of a formalised instrument for flagging content (Section 4.2.3.2), and even fewer so that explain what such instruments should look like, thereby leading the way to similar discrepancies as those observed at member state level. In other words, this section builds upon the discrepancy previously observed (Section 4.2.3.2) not with respect to the inconsistencies between notice mechanisms, but rather, the lack of agreement as to what precisely constitutes an adequate notice mechanism.

The AVMSD (Section 3.2.2) probably contains the most formalised and detailed provisions concerning the flagging of content. It doesn't establish an NTD as such but rather requires that VSPs establish a "transparent and user-friendly mechanism" for reporting/flagging content.[354] Further, they should also inform the flagger of the effect given to the flagged content.[355] Yet, in spite of such formalisation and detail, this mechanisms still leave a lot of leeway for hosting service providers, which can result in not user-friendly mechanisms, and hence in a low uptake of the mechanism.[356] The CDSMD (Section 3.3.4.1) simply refers to "sufficiently substantiated notice[s] from the rights holders", without further defining what this means.[357]

---

[348] See also Commission, 'Impact Assessment Digital Services Act' 26.

[349] Commission, 'Tackling Illegal Content Online', para 19.

[350] Commission, 'Tackling Illegal Content Online', para 20.

[351] Commission, 'Tackling Illegal Content Online', para 36-37; Van Hoboken 9.

[352] van Hoboken 9.

[353] See TERREG, art X(3)(d).

[354] AVMSD, art 28b(3)(d).

[355] AVMSD, art 28b(3)(e).

[356] Kukliš 21.

[357] CDSMD, art 17(4)(c).

The lack of a description of what constitutes an appropriate NTD mechanism can be problematic given the diverging practices. For instance, the European Commission argues that the Memorandum of Understanding for counterfeit goods (Section 3.3.4.2) allows for the possibility of bulk notifying (which the Commission argues would also be in line with the NTD procedure as defined in the 2018 Recommendation).[358] However, an interviewed stakeholder representing European hosting service providers has argued that notifications should be sufficiently precise. In practice, bulk notifications are frequently not of sufficient quality. In other words, the lack of commonly accepted criteria as to what qualifies as an adequate notification mechanism not only leads to a disharmonised situation, but also to a situation whereby notifications of insufficient quality are tolerated if not explicitly endorsed. In a similar sense, the general lack of precision of the notice requirements of the Code of Conduct on Countering Illegal Hate Speech (see Section 3.3.3) has also been the target of criticism.[359]

The lack of commonly agreed criteria for adequate notification procedures has important practical implications. In practice, the notification procedure varies from platform to platform, and is not considered user-friendly in various cases, with some going as far as suggesting that some hosting service providers deliberately implement design making it more difficult for users to submit a notice (Section 2.3.1.4). This obviously prevents the efficient submission of notices. This was echoed by the interviewed representative of a digital rights organisation. The representative argued that currently many notice systems are of too poor quality, providing users with too little information. Given the current lack of European binding rules on the matter, a lot of the variation in the quality of the procedure will also depend on the hosting service providers' resources (Section 2.3.1.4). On the other hand, more unsubstantiated claims could arise if the process becomes too "user-friendly" (Section 2.3.1.4). This last fear was also echoed by interviewed representatives of online intermediaries that pointed to possible abuses of the system. Other interviewed stakeholders representing European hosting service providers underlined the diverging challenges depending on the size of the hosting service provider. For big companies the challenge lies in adequately dealing with high volumes of notifications, while for smaller players one of the key challenges is to be able to verify the validity of the notices they receive.

4.3.4.2. Lack of agreement on adequate procedures: beyond NTDs

Beyond NTDs, other procedural measures can be characterised by a lack of agreement concerning their adequacy. This is the case for counter notice mechanisms (see, Sections 3.2.3, 3.4.1). In the field of copyright for instance, they have resulted in court actions from the rights holders against the content provider on the basis of the counter notice. This has had the effect that the possibility of a counter notice has in effect become largely symbolic measures that contribute little to safeguarding the users' rights.[360] On the other hand, interviewed stakeholders having an interest in removing illegal content that violates IPR raised attention on the possible abuse of counter notices, for example by using it as a delaying tactic. This points to the need to determine what an appropriate counter notice procedure would be, and in particular whether anonymous counter notices would be appropriate. Some interviewed stakeholders such as those representing European hosting service providers were clearly against it (see also Sections 5.3.1.2, 5.3.1.3, 5.3.2.1).

One can mention similar debates concerning the functioning and accreditation of trusted flaggers, or the adequate cooperation with competent authorities. Various interviewed stakeholders representing hosting service providers mentioned that they have their own procedure for collaborating with trusted flaggers and/or competent authorities. Beyond the probable discrepancy between these procedures, the question

---

[358] See, European Commission, 'Report on the Functioning of the Memorandum of Understanding on the Sale of Counterfeit Goods on the Internet' 24.

[359] De Streel and others 49.

[360] Kuczerawy 532. Cf Section 2.3.1.4.

remains as to which one is the most adequate one. An interviewed representative of a digital rights organisation pointed to the abuse of the trusted flagging system in the US by extreme right groups, and also to the possibly problematic situation whereby competent authorities would make use of trusted flagging schemes, thereby circumventing official channels and the safeguards that go with them. Symmetrically, one can also point to the situation whereby hosting service providers force competent authorities to create a personal account in order to request the take down of a specific content.[361]

A salient issue is what constitutes adequate transparency. This is well epitomised by the EU Code of Conduct on Countering Illegal Hate Speech Online (Section 3.3.3), which is regularly assessed by the European Commission.[362] Such assessment contains useful information in terms of the efficiency hosting service providers' moderation practices, for instance how much content has been taken down.[363] However, such transparency is only partial. It leaves aside a number of important issues such as what type of content exactly has been removed and on which legal basis, or the amount of false-positives/negatives detected.[364]

4.3.5. High compliance costs for SMEs

Along with the remarks made in Section 1.5.4 on the economic burdens that can be too heavy for smaller enterprises, various interviewees pointed to the heavy compliance burdens for SMEs, which can limit their economic viability (Section 1.5.4). Accordingly, such burden has two main sources. On the one hand, interviewed representatives of a regulator pointed to the discrepancy of the national legal frameworks. Adapting to the specificities of each national system can be too burdensome for some SMEs (and particularly for small and micro enterprises).[365] On the other hand, an interviewed representative of a digital rights organisation pointed to the compliance costs created by the new binding specific instruments (e.g., CDSMD, TERREG). These are not always sustainable for SMEs. Van Hoboken has voiced similar criticism in the context of the TERREG's obligation to remove terrorist content within one hour (Section 3.3.1). According to him it is an illusion to think that smaller players would have sufficient resources to dedicate to what would amount in practice to a 24h staffing obligation.[366]

These high compliance costs can be problematic for two reasons. On the one hand they are problematic for the interests of smaller hosting service providers who will face significant difficulties to enter the market because of these high costs.[367] On the other hand the interests of the victims are also at jeopardy since hosting service providers who do not have enough resources to comply cannot adequately protect their rights.

4.4. Conclusion

This chapter identified gaps on the basis on the methodology developed in Section 1.4. The latter makes a distinction between a situation in which the current framework is unjustifiably inconsistent and a situation in which the various involved interests are insufficiently safeguarded by the current legal rules. In other words, like cases should be treated alike unless such difference is justified (for instance by the nature of the

---

[361] European Parliament, 'Fundamental rights', point 32.

[362] See for instance, Commission, '5th Evaluation'.

[363] See for instance, Commission, '5th Evaluation'.

[364] De Streel and others 46. See also Ellen-Koren and Perel 674-675, and Commission, 'Impact Assessment Digital Services Act' 26.

[365] See also, Commission, 'Impact Assessment Digital Services Act' 23.

[366] Van Hoboken 8.

[367] Commission, 'Impact Assessment Digital Services Act' 24-25.

content). Each time the difference between provisions is not justified, this report concludes to the existence of an inconsistency. Further, gaps may also exist because the existing rules provide insufficient safeguards for the various involved interests discussed in Section 1.5. The legal framework for intermediary liability is designed to protect and balance various interests. However, in some cases these interests are insufficiently protected by the current legal framework (e.g., a needed rule does not exist, or the relevant rules are unclear leading to sub-optimal protection).

As far as inconsistencies are concerned (Section 4.2), the report identifies three broad categories of gaps. Namely a lack of consistent application of the legal framework (Section 4.2.1), a lack of comprehensive and harmonised definition of what counts as illegal content (Section 4.2.2), and the existence of diverging measures between the various instruments of the legal framework (Section 4.2.3).

The lack of consistent application of the legal framework (Section 4.2.1) refers to mainly two types of situations. On the one hand it refers to the discretion that member states are awarded when implementing Directives, which can lead to too much discrepancy and a fragmentation of the legal framework (Section 4.2.1.1). On the other hand, it refers to the co-existence of binding and non-binding instruments (Section 4.2.1.2). The latter's shortcomings are well known (i.e., lack of precise provisions, lack of sufficient compliance and adherence).

The lack of comprehensive and harmonised definition of what counts as illegal content (Section 4.2.2) refers to the absence of EU-wide consensus on what counts as illegal content -thus concerning all types of content. Beyond the uneven legal framework, this also has side effects such as over-removal for fear of liability.

The existence of diverging measures between the various instruments of the legal framework (Section 4.2.3). puts the focus on the lack of harmonised provisions concerning the various procedural elements of the legal framework. This points to divergences concerning notice mechanisms (Section 4.2.3.2), but also concerning the other procedural elements such as transparency obligations or trusted flagging schemes (Section 4.2.3.1). It also refers to the specific situation concerning proactive measures (Section 4.2.3.3). Finally, this section also points to a situation where more divergence should exist concerning certain type of online content such as product safety or child pornography where more granularity and discrepancy might be warranted for certain hosting service providers (Section 4.2.3.4).

As far as lacks are concerned (Section 4.3), the report identifies five main gaps. The first gap refers to the absence of clarity concerning the criterion of actual knowledge (Section 4.3.1). More particularly the meaning of what constitutes actual knowledge or awareness is unclear and disharmonised. The problematic implications of this situation have been explored more in detail in Section 2.3.

The second gap refers to the lack of clarity concerning the hosting service providers' procedural obligations as well as the sanctions for their violation (Section 4.3.2). Such lack of clarity can have two types of nefarious consequences. On the one hand the confusion about the existence and scope of such liability can lead to over-removal practices. On the other hand, the lack of clear-cut liability for these obligations might also be in the detriment of the victims of illegal content online who cannot rely upon clear liability rules.

The third gap refers to the lack of adequate safeguards for fundamental rights (Section 4.3.3). This lack puts particular focus on the absence of minimum safeguards such as information rights, the possibility to submit counter notices, or the absence of complaint mechanisms. It also puts emphasis on the fact that even though automated tools are used in practice, there are not enough safeguards in relation to them in existing legislation.

The fourth gap refers to the lack of agreement as to what constitutes adequate procedural measures (Section 4.3.4). This refers to the absence of agreement as to what constitutes an adequate notice mechanism (Section 4.3.4.1) and goes on to address the same issue as far as the other procedural measures are concerned –e.g., transparency, trusted flagging, etc.- (Section 4.3.4.2).

The fifth and final gap refers to the high compliance costs for SMEs (Section 4.3.5). These high compliance costs can prevent smaller hosting service providers from entering the market, but they also put the users' rights at jeopardy since these smaller hosting service providers do not have sufficient resources to comply with their obligations.

These various gaps constitute the bedrock on which the recommendations of Chapter 5 are elaborated.

5. Recommendations for the revision of the European framework for the liability and responsibilities of hosting service providers in the DSA

5.1. Introduction

The previous chapters have given an overview of the current legal framework and its various gaps. This chapter provides recommendations to address these gaps. It evaluates possible legal solutions to stimulate hosting service providers to limit the dissemination of illegal online content through their services without unduly affecting fundamental rights and other concerned interests. It answers question 4: *How can new rules best encourage hosting service providers to limit the dissemination of illegal online content?*

This chapter also indicates how the recommendations compare to the legal rules of the DSA proposal. However, it is not meant as a detailed analysis of this proposal and does not discuss every provision.

This chapter starts with various recommendations of the core principles of the European framework for intermediary liability (Section 5.2). It subsequently presents several recommendations in relation to notice and action mechanisms (Section 5.3), transparency (Section 5.4) and differences between various kinds of hosting service providers (Section 5.5). It ends with a conclusion (Section 5.6).

5.2. The core principles

The first set of recommendations concerns the core principles of the framework for intermediary liability as introduced by the e-Commerce Directive:

1. The exemptions from liability should be maintained (Section 5.2.1).
2. A 'Good Samaritan provision' is not necessary, but can still be a useful clarification (Section 5.2.2).
3. Hosting service providers should have a (modest) duty of care to proactively monitor publicly available online content (Section 5.2.3).
4. The delineation between general and specific monitoring obligations should be clarified. Specifically, notice and *stay* down obligations should be allowed (Section 5.2.4).
5. The meaning of 'actual knowledge or awareness' and 'expeditiously' should be harmonised and clarified (Section 5.2.5).
6. Self-regulation can be a useful addition, but should not be relied upon excessively (Section 5.2.6).

The European framework should harmonise the private law liability in relation to the various obligations in relation to the limitation of the dissemination of illegal content (Section 5.2.7):

7. A hosting service provider should be liable if it hosts content that is illegal under European law and the exemption from liability does not apply (Section 5.2.7.1).
8. A hosting service provider should be liable whenever it violates its monitoring obligations (Section 5.2.7.2).
9. A hosting service provider should be liable whenever it violates other duties designed to limit the dissemination of illegal content (Section 5.2.7.3).
10. Users should be liable for uploading illegal content to platforms (Section 5.2.7.4).
11. Harmonise and clarify the illegality of online content where feasible (Section 5.2.7.5).

5.2.1. Maintaining the exemption of liability

Various policy makers, academics and stakeholders have criticised the current framework for intermediary liability. This criticism is generally targeted at the resulting balance between the various interests and the lack of legal responsibility for hosting service providers. At the same time, there is a relatively strong consensus that the core principles of the e-Commerce Directive are sound (Section 1.1). This consensus was also reflected in the interviews. Although the various stakeholders may disagree about certain safeguards and duties of care, it is generally considered fair that hosting service providers are not liable for any and all illegal content that is shared through its services and its content providers. The DSA proposal retains the principles of the e-Commerce Directive. Article 14 of the e-Commerce Directive is largely replaced with the almost[368] identical Article 5 of the DSA Proposal.

5.2.2. Good Samaritan provision

The fact that a hosting service provider (voluntarily) monitors the hosted information does not mean that it acquired knowledge or awareness about any existing illegal content or that it can no longer benefit from the exemption from liability (Section 2.3.1.1). Although this follows from recital 40 of the e-Commerce Directive and has been confirmed by the Commission,[369] various authors claim that monitoring could lead to this result, or at least that this issue is unclear. In short, they claim that a hosting service provider that monitors the information may no longer be 'neutral', 'merely technical', 'automatic' and 'passive'.[370]

At the same time, it is clear that voluntary monitoring should not lead to this result. Voluntary monitoring can be an effective tool to limit the dissemination of illegal content. Since it is not primarily motivated by a fear of liability (Section 2.3.1.1), the risk of collateral censorship can be relatively small (see also Section 2.2.2). However, hosting service providers are still obligated to remove illegal content (or face liability) that is discovered through voluntary monitoring (Section 2.3.1). Since voluntary monitoring will lead to the analysis of the permissibility of more online content, it can also cause collateral censorship because more permissible content is flagged as illegal by mistake.[371]

---

[368] Except for DSA proposal, art 5(3), which states that the exemption does not apply with respect to liability under consumer protection law of online platforms allowing consumers to conclude distance contracts with traders, but only if the online platform presents information in a way that would lead an average and reasonably well-informed consumer to believe that the information, product or service is provided by the online platform. In this situation, the liability of the platform is not strictly secondary. It is not held liable for information provided by others, but because the online platform itself confused the consumer.

[369] E-Commerce Directive, recital 40; Commission, 'Tackling Illegal Content Online' 12-13.

[370] Eg Sartor 18, 24-25; Stalla-Bourdillon 281-282; Van Hoboken and others, *Hosting intermediary services and illegal content online* 39; Montagnani 300; De Streel and others 20. Cf Section 1.2.1; Batura.

[371] See also Van Hoboken and others, *Hosting intermediary services and illegal content online* 41-42.

In order to stimulate voluntary monitoring, the DSA proposal various authors and interviewed representatives of both online intermediaries and other stakeholders propose to add a 'Good Samaritan' provision that explicitly clarifies that voluntary monitoring does not mean that a hosting service provider can no longer benefit from the exemption from liability.[372] Such a provision is also included in Section 230(c)(2) of the (American) Communication Decency Act.[373] Although such a provision may not be strictly necessary in the European framework for intermediary liability,[374] there is also no compelling reason *not* to include it.[375] It serves a useful purpose as a clarification and codification of existing law.

5.2.3. General proactive monitoring obligations

Proactive monitoring obligations can limit the dissemination of illegal content (Section 1.5.1). Sections 2.3.1.2, 3.2.3, 3.3.1, 3.3.2, 3.3.4.1, 3.3.4.2, 3.3.7.2, 4.2.3.3 and 4.3.3 show that proactive measures are already used and imposed in (existing and proposed) legislation and non-binding law. Furthermore, technological advances continually improve the effectiveness and efficiency of automated technological monitoring mechanisms (Section 2.3.1.1) and intermediaries already apply these techniques (Section 2.3.1.2). Under these circumstances, it makes sense to harmonise these practices by requiring *all* hosting service providers to proactively monitor and restrict the access to *all* types of illegal content. Indeed, the European Commission and various authors have proposed to impose such a monitoring obligation.[376]

However, various factors warn against imposing a stringent monitoring obligation. As discussed in Section 2.3.1.1, far reaching monitoring obligations can lead to collateral censorship and affect freedom of expression and freedom of information (see also Section 1.5.2). Since monitoring may cause content to be removed before it is accessible online, it can be particularly hard to oversee this kind of moderation (Section 1.5.3). Next, the general proactive monitoring obligation should respect confidentiality, privacy and cybersecurity. It should only apply to publicly available online content (see also Section 2.3.1.1). Furthermore, proactive monitoring may not be feasible for smaller hosting service providers that lack the capacity to efficiently implement them (Sections 1.5.4 and 5.5.3). Finally, it may not be suitable or sufficiently effective for certain kinds of illegal content such as hate speech or cyberbullying. Although the interviewed representatives of online intermediaries have mentioned the use of certain techniques that may detect these forms of illegal content such as spam detection and profanity filters in the interviews, an accurate evaluation of whether the content is actually illegal still requires a manual assessment. On the other hand, there is no clear reason why there should not be a binding (Section 3.3.4.2) obligation to proactively identify and remove offers for counterfeit goods.

For these reasons, monitoring obligations should not be too strict. They should be limited to a duty of care, obligating the hosting service providers of publicly available online content to take reasonable measures

---

[372] DSA proposal, art 6, recitals 25, 47; Sartor 24-25; Adviesraad Internationale Vraagstukken 8; De Streel and others 80.

[373] 47 U.S.C. § 230.

[374] Various authors emphasize that the European and American framework are different. Sartor 17-18; De Streel and others 58. For this reason, DSA proposal, art 6 should not be considered a direct legal transplant of Section 230(c)(2). It should be interpreted in the context of its purpose in the European framework.

[375] Of course, such a clarification does not mean that a hosting service provider does not have any responsibilities in relation to its proactive monitoring. See eg Sections 5.2.3 and 5.5.4. An interviewed organisation representing the interests of rights holders mentioned that it was not necessarily against the content of this provision, but worried that it might be abused to advocate for an interpretation that would expand the liability exemptions.

[376] Section 4.2.3.3; Yannopoulos 51-52; Montagnani 299; De Streel and others 80; n 379. Cf Senftleben.

without holding them liable if illegal content is disseminated despite these efforts.[377] Generally, such obligations should not require an independent assessment of potentially illegal content. Instead, they should only require monitoring that can be done efficiently through automated search tools and technologies.[378] The exact scope of the monitoring obligation should depend on various factors such as the potential negative impact of illegal content, the size of the hosting service provider, the available automated measures and their costs and effectiveness and the risks of collateral censorship.[379] Such a rule is flexible enough to adapt itself to changing circumstances. At the same time, safeguards should exist to protect the fundamental rights of users (Section 1.5.2). These safeguards are further discussed Sections 5.3.1.3 and 5.5.4.

In practice, most hosting service providers are already proactively monitoring publicly available online content (Section 2.3.1.2). In this light, the recommendation for a general proactive monitoring obligation should not be understood as necessarily and immediately leading to a much higher degree of content moderation throughout. Instead, it should be understood as a way to force certain hosting service providers to catch up. It is primarily targeted at *mala fide* hosting service providers and providers that are lagging behind significantly. Under a proactive monitoring obligation, all providers are obligated to do their part for the protection of victims of illegal content. Furthermore, it prevents content providers from migrating to another hosting service provider in order to more easily disseminate illegal content. As long as the European rules apply, the other providers are also required to limit the dissemination of this content.

Despite these arguments for a (modest) general proactive monitoring obligation, Article 7 of the DSA proposal retains the prohibition of general monitoring obligations of Article 15(1) of the e-Commerce Directive while also being without prejudice to the monitoring obligations that are imposed in other instruments.[380] The current proposal therefore fails to harmonise the legal framework on proactive monitoring obligations. This is unfortunate. There is no fundamental reason to impose monitoring obligations for certain kinds of illegal content, while prohibiting them in other situations (Section 4.2.3.3. Furthermore, the fact member states may still impose *specific* monitoring obligations can lead to further legal fragmentations (see also Section 5.2.4).

At the same time, the DSA proposal could implicitly[381] impose monitoring obligations. Very large online platforms are required to put in place mitigation measures, including adapting content moderation systems (see Section 5.5.4). Although not imposed explicitly, best practices (see also Article 27(2)(b) of the DSA proposal) may turn out to include proactive monitoring obligations. Furthermore, Article 20(1) of the DSA proposal imposes an obligation to act against *users* that frequently provide manifestly illegal content. They are required to suspend them.

The recommendation for a (modest) general proactive monitoring obligation comes with an important caveat. It will only lead to a better balance of the various interests if it is faithfully interpreted and applied by courts and hosting service providers. In reality, the necessary uncertainty that such a general duty of care would entail could be abused to prohibit legally permissible and even socially beneficial content such as critical journalism. Furthermore, fear of liability, especially due to the risk of strict interpretations by courts, may lead to collateral censorship (Section 2.2.2). Although the same risks apply in relation to responses to notices, the large scale of proactive monitoring may enlarge this effect. The automated nature can make this

---

[377] An interviewed representative from an organisation fighting against online abuse insisted that the intermediaries should take more responsibility, but that the law should not impose specific obligations.

[378] Cf Case C-18/18 *Glawischnig-Piesczek v Facebook* [2019] ECLI:EU:C:2019:821; Section 2.3.1.1.

[379] Sartor 30; Adviesraad International Vraagstukken 13. Cf De Streel and others 12, 76.

[380] See also DSA proposal, art 1(5), recital 28.

[381] Cf Yannopoulos 51-52; Frosio and Husovec 629.

process become less transparent. For these reasons, Section 5.2.4 provides a more modest recommendation.

5.2.4. The delineation between general and specific monitoring obligations should be clarified

The delineation between prohibited general monitoring obligations and permissible specific obligations is not always clear (Section 2.3.1.1). A clarification of this delineation facilitates the creation of specific monitoring obligations that more effectively limit the dissemination of illegal content (Section 1.5.1) while preventing general monitoring obligations that adversely affect fundamental rights (Section 1.5.2) and impose excessive costs on hosting service providers (Section 1.5.4). In this light, the exact delineation is of secondary importance, as long as it is sufficiently clear.

At the same time, we do have several more specific recommendations. First, the clarification should clearly settle that a member state can, at least under certain situations, impose an obligation to monitor that can be performed efficiently through automated search tools and technologies (see also Section 5.2.3). Furthermore, such a clarification should unambiguously formulate that and under what conditions notice and *stay* down rules are allowed. Various instruments already impose such a mechanism (Sections 3.3.4.1 and 3.3.7.2). Furthermore, *Glawischnig-Piesczek v Facebook* suggests that these orders are allowed (Section 2.3.1.1). At the same time, a more explicit and thorough delineation can clarify remaining uncertainty. The DSA proposal does not provide this clarity. Although the explanatory memorandum suggests that notice and stay down orders can be allowed, it explicitly states that it leaves case law unaffected.[382]

5.2.5. Harmonisation and clarification of 'actual knowledge or awareness' and 'expeditiously'

In Section 2.3, we have identified several unclarities in relation to the concept of 'actual knowledge or awareness'. In Section 2.3.4, we formulated the following questions:

a) Does actual knowledge only exist if the illegal nature is clear or 'manifest'?
b) Can ignorance of the law prevent the existence of actual knowledge if the law is unclear?
c) Does actual knowledge always require *human* knowledge? Or can actual knowledge also exist before the information is processed?
d) Under what circumstances should the knowledge of employees be imputed to the hosting service provider? Is this imputation harmonised? Is it affected by the existence of a notice and take down procedure?
e) What kinds of monitoring obligations may be imposed on hosting service providers (addressed in Sections 5.2.3 and 5.2.4)?
f) Under what circumstances does a hosting provider have an obligation to analyse the permissibility of (specific) online content? Specifically, when does a notification trigger such an obligation?
g) How much time after receiving information or acquiring actual knowledge or awareness can a hosting service provider take before it no longer acts 'expeditiously'?

[382] DSA proposal 3-4.

The answers to these questions should be clarified and harmonised. The secondary liability of hosting service providers depends on three interconnected factors (Section 2.3.4): the obligations to analyse the permissibility of online content, the threshold for actual knowledge and the timeframe for 'expeditious' removal. For these reasons, the questions should not be answered in isolation. A higher threshold for actual knowledge should be coupled with an obligation to analyse the permissibility of the content under certain circumstances. Under a lower threshold, the timeframe for 'expeditious' removal should be longer (Section 2.3.4). As long as these principles are followed, the exact answers to the individual questions are of limited importance.[383]

This does not mean that these recommendations cannot affect the balance between the various involved interests. Under the current framework, many member states only accept actual knowledge when the illegality is clear without clearly imposing obligations to analyse the permissibility of the potentially illegal content. A clear rule that actual knowledge can also exist if the illegality is not 'manifest' *or* that a hosting service provider has an obligation to analyse the permissibility of potentially illegal content would lead to a better limitation of the dissemination of illegal content. Under such a rule, the timeframe for 'expeditiously' should be longer in order to prevent collateral censorship (questions a), f) and g), Section 2.3.2). At the same time, the mere fact that the hosted content is illegal should not lead to liability as long as the hosting service provider has insufficient information about the potential illegality. Finally, a shorter timeframe for expeditious removal protects the victims at the expense of freedom of speech and freedom of information.

The DSA proposal only provides a limited clarification of the concepts of 'actual knowledge or awareness' and 'expeditiously'. Recital 22 mostly repeats the clarifications of *eBay*.[384] Article 14(3) of the DSA proposal does provide an important clarification. It answers the question under c) by stating that sufficiently precise and adequately substantiated notices give rise to actual knowledge or awareness. In contrast, *eBay* merely considers that *in*sufficiently precise or *in*adequately substantiated may *not* lead to actual knowledge or awareness (see also Section 2.3.1.3). Article 14(3) clarifies that actual knowledge can also exist before the notice is processed and human knowledge is obtained (see also Section 2.3.3.1). As discussed, this should mean that the timeframe for expeditious removal is longer.

Furthermore, the formulation of Article 14(2) suggests that actual knowledge is not limited to situations in which the illegality is clear or 'manifest'. The notice only requires that the hosting service provider *can* identify the illegality of the content in question. In contrast, *eBay* states that there is awareness when the hosting service provider *should* have identified the illegality. Although 'can' suggests a lower threshold than 'should', this interpretation is far from clear or explicit. Article 14 of the DSA proposal is further discussed in Section 5.3.1.4. Similarly, the fact Article 20(1) and the corresponding recital 47 of the DSA proposal (see also Section 5.3.1.3) expressly compels online platforms to act against users that frequently provide *manifestly* illegal content, suggests that other obligations are *a contrario* not limited to manifestly illegal content.

5.2.6. The role of self-regulation and terms and conditions

For many aspects, the current legal framework relies on self-regulation and other forms of soft law. Although such self-regulation can fulfil a useful purpose, it also has several disadvantages (Section 4.2.1.2). For this reason, self-regulation should not be relied upon excessively. Important legal obligations in relation to the limitation of the dissemination of illegal content should be codified in binding, enforceable and

[383] Note that the difference between actual knowledge and an obligation to analyse the permissibility can be of importance for the resulting liability of the hosting service provider. Cf Sections 5.2.7.1 and 5.2.7.3.

[384] Case C-324/09, *eBay* [2011] ECLI:EU:C:2011:474.

harmonised legal norms. For example, transparency obligations and a notice and action mechanism should be imposed by law and not by a code of conduct.[385]

This does not mean that self-regulation cannot be a useful *addition* to these binding rules. Even under a harmonised legal framework, intermediaries will (and should) still have freedom to make certain choices about content moderation (see Sections 1.5.2, 1.5.4 and 2.2.2.2). Self-regulation can provide a useful role by stimulating a responsible use of this freedom and by providing insight about its use. Furthermore, this can also be done by terms and conditions of individual intermediaries. At the same time, it should be clear that this role is ancillary. Self-regulation and terms and conditions should only be relied upon for things that cannot or should not be included in the 'baseline' of binding legal norms.

Hosting service providers may want to practice stricter content moderation practices than mandated by law. Self-regulation, including terms and conditions, can provide a useful role by clarifying what types of content are not allowed,[386] especially when it is sufficiently clear and applied in a transparent and consistent manner.[387] Such application has a positive effect on the various involved interests.

First, it strengthens the protection of victims of illegal content (Section 1.5.1). It provides them with clear expectations about what they can expect in relation to the removal of content. If the actual practice of the hosting service providers does not match these expectations, the victims can appeal to the self-regulation to force the intermediaries to do more.

Next, sufficiently clear and consistently applied self-regulation protects freedom of speech and freedom of information and prevents discrimination due to unequal content moderation (Section 1.5.2). Under a consistent application of clear terms and conditions, content providers are better able to know what is and what isn't allowed on a particular platform. The consistent application should prevent uneven content moderation that causes, for example, LGBTQ-content to be removed more often. Conversely, if the terms and conditions themselves are discriminatory or too strict, content providers may pressure the intermediary to change the terms and conditions, move to another service or even take legal action if the terms lead to illegal discrimination.

Finally, a consistent application of clear terms and conditions helps maintaining the rule of law and judicial oversight by providing insight about content moderation by hosting service providers that goes beyond the particularities of individual decisions (Section 1.5.3). Because hosting service providers may host large amounts of online content, they are bound to make mistakes or questionable decisions in relation to content moderation. Clear and consistently applied terms and services allow courts to look beyond these individual cases. In this light, it is important that intermediaries also demonstrate this consistent application. They should be transparent about their content moderation practices, including their practices *in accordance with their terms and services* (Section 5.4.1).

For these reasons, intermediaries should be obligated to formulate clear information about their content moderation practices, including the possibility to submit notices and information about the way in which these notices are processed. Next, they should apply these practices consistently. In particular, it is important to also provide information about the use of automated decision-making (Section 4.3.3). Inspiration can be taken from the GDPR, which requires meaningful information about the involved logic.[388]

---

[385] Cf Gedragscode Notice-and-Take-Down 2018; Sections 5.3 and 5.4. See also Yannopoulos 56.

[386] Yannopoulos 55.

[387] See also DSA proposal, recitals 38 and 47; De Streel and others 9-10, 44, 46, 50; n 45.

[388] GDPR, arts 13(2)(f), 14(2)(g), 15(1)(h).

In this regard, the Modernisation Directive contains concrete and workable algorithmic transparency provisions.[389]

The recommended obligation can mitigate the disadvantages of self-regulation, namely its vague and non-binding nature (Section 4.2.1.2). Although it imposes additional burdens on intermediaries (Section 1.5.4), the advantages to the protection of the other interests outweigh these burdens. Furthermore, this system is in line with other European obligations[390] and does not place any additional[391] restrictions on the content of the moderation practices, but only on their application. As long as the intermediaries apply their terms and conditions consistently, they are free to shape their content moderation as they see fit. Finally, the obligation to apply the content moderation practices in a consistent manner should be interpreted as a duty of care, acknowledging that it may not always succeed and that it may be necessary to continuously revise and further clarify the terms and services.

Article 12 of the DSA proposal requires providers of intermediary services to include clear and unambiguous information in their terms and conditions about the restrictions in relation to the use of their service and their (automated) content moderation practices. Furthermore, they are obligated to apply and enforce these terms and conditions in a diligent, objective and proportionate manner with due regard to the rights and legitimate interests of all parties involved. Article 13, in particular (b), obligates the intermediaries to be transparent about their content moderation and the role of their terms and conditions for this moderation (Section 5.4.1).

Self-regulation can also be a useful and flexible tool to further specify and clarify technology-neutral[392] and relatively vague obligations. By creating effective standardised procedures, it is possible to facilitate the compliance with these rules. For example, they could provide a useful guide for smaller hosting service providers.[393] Furthermore, the interoperability of certain measures can broaden their effect[394] and decrease the costs of compliance. For example, a shared code of conduct on online advertising can support industry-wide compliance and limitation of the dissemination of illegal advertisements.[395] Articles 34, 35 and 36 of the DSA proposal facilitate the drawing up of such standards and codes of conduct.

5.2.7. Harmonising private law liability

The current European framework for intermediary liability imposes prohibitions or *limits*. It prohibits member states from holding intermediaries liable and from imposing general monitoring obligations (Sections 2.2.1 and 2.3.1.1). It does not guarantee private law liability and obligations below these limits: this is left to the member states. For this reason, the harmonisation by the European framework is incomplete (see also Section 4.2.1.1). In order to better limit the dissemination of illegal content, the European framework should not limit itself to prohibitions of liability and monitoring obligations. It should also impose private law liability and monitoring obligations when these prohibitions do not apply. The potential scope of

---

[389] For more on the Modernisation Directive and algorithmic transparency, see Gellert 17-18.

[390] For example, see GDPR, arts 12-14. A controller must provide clear and transparent information about the processing of personal data to the data subjects.

[391] Some requirements of course remain. For example, hosting service providers must remove illegal content after obtaining actual knowledge or face liability. See also Section 2.2.2.2.

[392] See also DSA proposal, recital 4; De Streel and others 77.

[393] DSA proposal, recital 66.

[394] See eg n 94.

[395] DSA proposal, art 36, recital 70.

the harmonised monitoring obligations has been discussed in Sections 5.2.3 and 5.2.4. This Section provides recommendations on the harmonisation of liability.

Except for the CDSMD (Section 3.3.4.1), the European framework does not impose private law liability for failing to limit the dissemination of illegal content by platforms. Instead, it mostly prescribes 'penalties' (Section 4.3.2). However, private law liability can be a useful addition to other forms of enforcement. It provides the victims with additional redress tools, allowing them to play a bigger role in the enforcement.[396] Although this liability increases the obligations of intermediaries, the additional costs are partly offset by the harmonisation of the rules.[397]

Figure 3. The harmonisation of liability and monitoring obligations

From a Dutch perspective, it should be emphasized that liability is consistent with general principles of Dutch tort law. Although exceptions may exist,[398] obligations to limit the dissemination of illegal content should generally be understood as (at least partly) intended to protect the victims of such illegal content. Generally, the violation of a legal norm designed to protect individuals leads to private law liability towards

[396] Cf Walree and Wolters 351 in the context of data protection law.

[397] See also DSA proposal 13.

[398] For example, one could argue that the obligations against terrorist content (Section 3.3.1) are only designed to protect society as a whole, and not potential individual victims.

these individuals.[399] However, this may be different in other legal systems. Similarly, 'primary' liability for uploading illegal content is consistent with Dutch tort law, but not harmonised by the European framework (Section 5.2.7.4).

The effects on the fundamental rights of individuals and society are, at least in theory, limited. The harmonisation of liability does not in itself affect the balance that is created by the European framework between the limitation of the dissemination of illegal content and the various involved fundamental rights. It only means that this balance is actually applied in each member state. Figure 3 gives a schematic overview of this change. The recommended harmonisation of liability should lead to the changes recommended in the following Subsections.

5.2.7.1. Liability for hosting illegal online content

For the reasons described in Section 5.2.7, hosting service providers should under certain conditions be subject to a harmonised liability for hosting illegal content. First, since we recommend to keep the exemption from liability (Section 5.2.1), the providers should only be liable if this exemption does not apply. In other words, they should only be liable if they had actual knowledge or awareness and failed to act expeditiously.

Next, the liability should only apply for hosting content that is illegal under binding European law (see also Section 4.2.2). This can either refer to types of content that are illegal under all circumstances (for example: child pornography) and to content that violates a specific rule (for example: an unfair commercial practice). In these situations, the illegality of the content is already harmonised throughout the entire European Union. In order to limit the dissemination of illegal content and provide a level playing field throughout, it makes sense to also harmonise the secondary liability for hosting this content. In contrast, such harmonisation is not necessary for types of illegality that are not governed by binding European law.[400]

Finally, the liability should be in accordance with generally accepted principles of liability. For example, it should only apply to legally relevant harms that have actually been caused by the hosting of the illegal content by the hosting service provider. The exact interpretations of these principles of liability by European law are still in development. Ultimately, the Court of Justice has the power to interpret them. Until then, the exact requirements remain unclear. This is an ongoing issue that goes beyond the scope of the topic of intermediary liability.[401] In any case, it has not stopped the European Union from imposing private law liability in other situations (see also Section 5.2.7.4).

Ideally, harmonised liability is imposed through a provision in a regulation.[402] In contrast, the DSA proposal does not harmonise the liability for hosting illegal content.[403] Instead, it maintains the current system of exemptions with liability depending on national law.

5.2.7.2. Liability for violating monitoring obligations

For the reasons described in Section 5.2.7, hosting service providers should under certain conditions be liable for a violation of their monitoring obligations. First, it should be emphasised that a violation of the

---

[399] Cf the *exception* of Dutch Civil Code, art 6:163.

[400] For example, certain types of defamatory or hate speech that are not covered by the AVMSD or the Counter-Racism Framework Decision. See Sections 3.2 and 3.3.3.

[401] For example, see Walree 168-169 about the interpretation of damages in European data protection law.

[402] Cf GDPR, art 82 (imposing liability for a violation of data protection law).

[403] DSA proposal, recital 17. See also recital 47: the DSA proposal does not affect the liability *of the users* for the misuse of the hosting service.

monitoring obligation should not be accepted lightly. The mere fact that illegal content is disseminated does not in itself support the conclusion that the monitoring obligations have been violated (Section 5.2.3).

Next, it is again (Section 5.2.7.1) important to emphasise the general principles of liability. Notably, a hosting service provider can only be held liable if the dissemination of the illegal content *was caused by* the violation of a monitoring obligation. In other words, it is not liable if the content would not be discovered[404] or blocked by the existing specific obligations or the modest general monitoring obligation recommended in Sections 5.2.3 and 5.2.4.

Since the DSA proposal does not impose any monitoring obligations, it also does not hold hosting service providers liable for a violation of such duties.

5.2.7.3. Liability for other obligations designed to limit the dissemination of illegal content

Besides liability and monitoring obligations, the legal framework for intermediary liability also imposes other obligations that are (at least in part) designed to limit the dissemination of illegal content. This includes notice and actions mechanisms, but also transparency obligations (Section 4.3.4).

For the reasons described in Section 5.2.7, hosting service providers should under certain conditions be liable for a violation of these obligations. For example, the failure to implement a proper procedure to facilitate notifications could lengthen the online availability of illegal content on a platform and thus increase the dissemination of this content.

Private law liability for a violation of monitoring (Section 5.2.7.2) and other obligations is important because it complements the liability for hosting illegal content (Section 5.2.7.1) and the rules and recommendations on actual knowledge (Section 5.2.5). It makes sure that a hosting service provider cannot escape its responsibilities by avoiding actual knowledge. For example, even if a certain notification does not trigger actual knowledge because the notification is insufficiently substantiated (Section 2.3.1.3), the illegality is not 'manifest' (Section 2.3.2) or the knowledge cannot be imputed to the hosting service provider (Section 2.3.3.1), the service provider may still be held liable for failing to respond to the notification by clarifying that additional information is needed, analyse the permissibility of the content or transmit the information to the responsible employees. Again (Sections 5.2.7.1, 5.2.7.2 and 5.3.1.4), this liability should be in accordance with general principles of liability. A violation of an obligation should only lead to private law liability if this violation actually caused the harm to the victim.[405]

Despite these arguments, the existing instruments of the European framework do not explicitly hold a hosting service provider liable for a violation of these obligations. Instead, they only state that a member state should impose effective, proportionate and dissuasive penalties (Section 4.3.2). Similarly, Article 42(1) and (2) of the DSA proposal only states that member states shall lay down rules on effective, proportionate and dissuasive penalties. This provision seems to be primarily concerned about administrative fines. This is evidenced by Article 42(3) and (4), which provides maximum penalties for infringements.

5.2.7.4. Primary liability for uploading illegal content

The focus on this report is on the obligations and 'secondary' liability of hosting service providers. However, it remains important to emphasize that the content providers commits the 'primary' unlawful act by uploading the illegal content (Section 2.1). The dissemination of illegal content can be disincentivised by also holding the content providers liable.

---

[404] And thus lead to actual knowledge or awareness. See also Section 5.2.5.

[405] Cf De Streel and others 81 (proposing that intermediaries lose the benefits of the exemption if they violate other obligations).

Again (Section 5.2.7.1), this liability should only apply for content that is illegal under binding European law and should be in accordance with generally accepted principles of liability. Importantly, the primary liability of the content providers should *supplement but not replace* the secondary liability of intermediaries. The fact that the content providers are *also* liable does not mean that the victim cannot directly claim damages from the hosting service provider. There should not be a requirement of subsidiarity. However, the intermediary should be able to have recourse against the content providers after paying damages to the victim. Furthermore, the recommendation to harmonise the liability of the content providers should not in itself affect the possibilities to use a platform anonymously. It should not be construed as a general know-your-customer obligation, let alone a requirement to disclose information about customers to the victims of illegal online content (see also Sections 4.3.4.2, 5.3.1.2, 5.3.2.1, 5.5.1 and 5.5.2).

Under these conditions, the liability of content providers can be a useful supplement to European framework for intermediary liability without affecting fundamental rights. Since the content was already illegal, it does not place additional restrictions on content providers. Although private law liability could cause them to be more careful, we do not generally consider such prudence a problem.[406]

The current European framework generally does not always harmonise or even provide rules on the primary liability for disseminating illegal content. At the same time, some newer rules do impose private law liability. Articles 11a UCPD (as revised by the Modernisation Directive) and 82 GDPR grant a right to receive compensation for suffered damage. This indicates that primary liability is already starting to take shape in the European framework. For this reason, it makes sense to harmonise it for all kinds of illegal content under European law.

5.2.7.5. Harmonising and clarifying the illegality of online content

Besides the harmonisation of sanctions, the limitation of the dissemination of illegal content could also be improved by harmonising the illegality itself. The European framework only harmonises certain types of illegal content and only provides limited specific rules for others (Section 4.2.2). This legal fragmentation adversely impacts the various involved interests. It makes it more difficult for platforms to identify and remove illegal content (Section 1.5.4) and therefore encourages them to adopt moderation practices that are stricter than the law, thus limiting the freedom of expression and freedom of information (Section 1.5.2).

The solution seems straightforward: harmonise the illegality of online content. Although this would be an effective solution from the perspective of the limitation of the dissemination of illegal content, it would lead to a significant increase of the European Union's competencies. Although a shared basis can often be identified, member states have different perspectives on topics such as hate speech (Sections 2.2.2.1 and 4.2.2). Harmonisation would either lead to an infringement of fundamental freedoms (when the rules of the more restrictive countries are followed) or to an unchecked dissemination of previously illegal content (when the rules of the more liberal countries are followed). For this reason, a complete harmonisation of the illegality of online content is not desirable.

Instead, further harmonisation and clarification of the illegality of online content should be limited to areas where the divergence between the member states is relatively limited and not of a fundamental nature. For example, a representative from an organisation fighting against online abuse mentioned small differences in relation to child pornography (non-nude erotica, series of pictures). Such differences could be harmonised in order to make the limitation of the dissemination of such content more efficient.

More generally, further harmonisation and clarification is a feasible option for types of content and rules that are already harmonised by the European framework. For example, this can be done by opting for

---

[406] It is not a bad thing if a user thinks twice before uploading a copyright protected movie or nude photos that might depict a minor.

maximum harmonisation, formulating clear rules and stimulating explanatory opinions that provide more details when necessary. Although this falls outside of the scope of the DSA,[407] it is a useful approach to gradually improve the efficient limitation of the dissemination of illegal content.

5.3. The harmonisation of notice and action mechanisms as well as other procedural mechanisms

In practice, notice and action mechanisms constitute one of the most important tools for detecting and removing illegal content. However, the e-Commerce Directive does not impose such a mechanism for all kinds of illegal content. For this reason, the mechanisms vary by member state and by type of illegal content (Sections 2.3.1.3 and 4.2.3.2). Similarly, not all of these mechanisms offer the same kind of protection, not least because there is no consensus as to what constitutes the most adequate mechanism (Section 4.3.4.1). The same remarks apply to other procedural mechanisms such as redress possibilities (Sections 4.2.3.1 and 4.3.4.2). These issues also trigger related problems, namely the insufficient protection of users' fundamental rights (Section 4.3.3).

The second set of recommendations concerns the harmonisation and standardisation of these notice and action mechanisms:

12. Harmonise and standardise the notice and action procedure throughout the European Union and for all kinds of illegal content (Section 5.3.1).

This general recommendation can be subdivided into a number of more specific recommendations.

13. Hosting service providers should facilitate sufficiently precise and adequately substantiated notifications (Section 5.3.1.1).
14. Anonymous notices should be possible (Section 5.3.1.2).
15. Safeguards should be provided against abuses of the notice mechanism (Section 5.3.1.3).
16. Hosting service providers should act diligently on all the notices they receive (both founded and unfounded) (Section 5.3.1.4).
17. Hosting service providers should provide clear information about the decision to (not) remove online content to both the notifier and the content provider (Section 5.3.1.5).
18. There should be a trusted flagging system, with particular emphasis on the harmonisation of the attribution of the trusted flagger status and of the prevention against abuses (Section 5.3.1.6).
19. Competent authorities should communicate with hosting service providers through specific and harmonised channels (Section 5.3.1.7).

In addition to these notice-related recommendations, we also make a number of recommendations concerning redress mechanisms:

20. There should be a quick internal complaint-handling mechanism (Section 5.3.2.1).
21. There should be an out-of-court redress mechanism (Section 5.3.2.2).
22. The possibility of judicial redress should be re-emphasised (Section 5.3.2.3).

[407] DSA proposal 4.

5.3.1 Harmonise and standardise the notice and action procedure throughout the European Union and for all kinds of illegal content

The fragmentation of notice and action mechanisms has important disadvantages for victims, users, society and hosting service providers. For victims, the fragmentation can mean that an effective, fast and user-friendly notice and action procedures may not always be available (Section 1.5.1). It can mean that there is a lack of safeguards to protect fundamental rights against over-removal (Sections 1.5.2, 4.3.3) and to maintain the rule of law and judicial oversight (Section 1.5.3). Finally, it imposes costs on hosting service providers by forcing them to comply with many different mechanisms (Sections 1.5.4 and 4.2.1.1).[408]

For these reasons, it is desirable to impose a notice and action mechanism in a regulation that directly applies throughout the European Union and for all kinds of illegal content.[409] This mechanism should balance the various interests. It should be user-friendly and facilitate the effective limitation of the dissemination of all kinds of illegal content, but also contain standardised safeguards to facilitate fundamental rights and other involved interests.[410] At the same time, certain situations may require specific rules. For example, the particularly damaging character of terrorist content may justify a requirement to remove the illegal content within one hour after receiving an order from a competent authority (see Section 3.3.1). However, such deviations should be kept to a minimum in order to preserve the benefits of harmonisation and standardisation.

The DSA proposal creates a harmonised notice and action mechanism. This mechanism functions as a baseline. It applies to all kinds of illegal content, but specific rules may be imposed by other, vertical instruments.[411] More specifically, the DSA proposal does not affect existing rules. Given the overlap between specific vertical instruments and the horizontal DSA, we recommend to use the DSA as a baseline in terms of what constitutes a valid notice and action mechanism. Further, and in order to avoid too much discrepancy between the various instruments, the notice and action mechanisms taken pursuant to other instruments should be streamlined with the DSA as much as possible. Specific differences should also be clearly indicated and justified where possible. A more detailed analysis of this issue falls outside of the scope of this report.

In the interviews, representatives of online intermediaries reacted differently to the proposed notice and action mechanism. On the one hand, several interviewees reacted positively to the fact that the DSA proposal creates a harmonised mechanism for the European Union. However, others indicated that the proposal may be too restrictive, forcing them to abandon or change current moderation practices without necessarily improving the protection of the various interests. These diverging responses illustrate the difficulty and importance of finding the right balance between standardisation and a technology-neutral formulation of the rules (Section 1.5.4).

Building on the problems just described, the following subsections provide various recommendations concerning specific aspects of the notice system. Namely, the content of the notice, the anonymity of the notice, the safeguards against abuses of the notice mechanism, the processing of notices, information rights pursuant to a decision, trusted flagging systems, and communication channels for competent authorities. These various recommendations are all related to the gaps and interests mentioned at the beginning of this

---

[408] See also DSA proposal 13.

[409] See also DSA proposal, recitals 16, 41.

[410] See also DSA proposal 2-5, 9, recitals 34, 41; De Streel and others 78.

[411] DSA proposal 4-5, 9, recitals 10-11, art 1(5).

section. Where needed, they are further specified and discussed for each subsection. The DSA proposal harmonises the notice system for hosting service providers.[412] We agree with this standpoint. A direct consequence is that all the specific aspects of the notice system that we discuss herein below also apply to hosting service providers in general. This is not necessarily the case in the DSA proposal, which limits certain provisions (e.g., trusted flaggers) to online platforms.[413] We address these differences when discussing the relevant provisions.

5.3.1.1 Content of notice

If notices are insufficiently precise or substantiated it will be more difficult for hosting service providers to make the right decision, to the detriment of users' fundamental rights (Sections 1.5.1, 1.5.2, and 4.3.3). Furthermore, this entails that hosting service providers need to invest more time into the processing of notices which costs resources and might lead to wrong removal decisions (Section 4.3.4.1). In this sense inadequately substantiated notices can create legal and factual uncertainty which leads to over-removal (Section 2.2.2.1). Currently, there is no agreement on what a notice should contain (Section 4.3.4.1).

Along with the European Commissions' 2018 Recommendation (Section 3.2.3), we recommend that notices should be sufficiently precise and adequately substantiated. Hosting service providers should facilitate this. The precision refers to the ability to locate the content. In most cases a URL will suffice, but sometimes more information might be needed for instance when a URL refers to a plurality of content,[414] or in the case of videos which might require the use of timestamps.[415] The substantiation should allow the hosting service provider to conduct a limited but sufficient legal and factual assessment of the notice within a short timeframe.[416] It should entail for instance the reason for the notice and some evidence justifying the claim.[417]

The DSA proposal is in line with this recommendation.[418] Providers of hosting services are obligated to facilitate adequate notices pursuant to Article 14(2), for example by setting up an online pre-formatted submission form. As far as the precision is concerned, some interviewed stakeholders representing organisations having an interest in removing certain types of illegal content (children abuse material including pornography, IPR) emphasised the limits of URL-based identification of content given that once the content has been deleted it is extremely easy to re-upload it elsewhere. Although true, this objection does not change the fact that there is broad agreement on URLs as being the most adequate method to identify illegal content. Instead, this issue can be addressed through other obligations, such as a general monitoring obligation and, more specifically, an obligation to facilitate notice and *stay* down (Sections 5.2.3 and 5.2.4). As far as substantiation is concerned, the DSA proposal requires an "explanation of the reasons why the individual or entity considers the information in question to be illegal content".[419] Such a requirement seems compatible with our recommendation to include the reason for the notice and to provide some evidence justifying the claim, especially because the DSA proposal also specifies that an adequate notice should enable the hosting service provider to identify the illegality of the content in question.[420] However, the requirement itself could be made more explicit.

---

[412] DSA proposal, art 14.

[413] DSA proposal, art 19.

[414] See Wilman 301.

[415] European Parliament, 'Adopting commercial and civil law rules', Annex B, art 9(1)(a).

[416] See Wilman 302.

[417] See, European Parliament, 'Adopting commercial and civil law rules', Annex B, art 9(1)(b),(c); DSA proposal, art 14(2)(a).

[418] DSA proposal, art 14(2)(b).

[419] DSA proposal, art 14(2)(a).

[420] DSA proposal, art 14(2).

5.3.1.2 Anonymous notices as a rule

Requiring notices not to be anonymous can be seen as an incentive for better substantiated notices and in general better-quality notices, as well as an efficient safeguard against abuses by individuals. However, it also puts a jeopardy users' anonymity on the internet, which is itself key to the rights of privacy, freedom of expression and freedom of information (Section 1.5.2). Next, fear of retaliation may create a barrier, preventing victims and other notifiers from flagging the illegal content. Furthermore, there are other ways to address notice abuses (See Section 5.3.1.3). In view of an adequate balancing of rights (Sections 1.5 and 4.3.3), we therefore recommend that anonymous notices should be possible unless there is a justified exception.

The DSA proposal requires the hosting service providers to facilitate non-anonymous notices, except in cases of child sexual abuse material.[421] Although notifiers could, at least in theory, decline to give their (real) name and e-mail, such a notification would not give rise to actual knowledge under Article 14(3) of the DSA proposal. We do not agree with this rule. Keeping an adequate balance of rights in mind, we believe that anonymity should be the rule rather than the exception. For this reason, anonymous notices should be possible and have the same effect as non-anonymous notices unless the identity of the notifier is important for the evaluation of the permissibility of the content, for example because the notice alleges an infringement of copyright without permission.[422]

5.3.1.3 Safeguards against abuses of the notice mechanism

As seen in the previous section (5.3.1.2) anonymous notices are key to ensuring an adequate balance of rights online. However, they also create a risk of abuse, which itself would be detrimental to the protection of the various interests at stake (Section 1.5.2). Yet, the fear of abuse through anonymous notices can be mitigated by providing safeguards against such abuses.[423]

Article 20(2) of the DSA proposal states that online platforms shall suspend the processing of notices by notifiers that frequently submit manifestly unfounded notices. However, it is possible to go further by extending this obligation beyond online platforms to hosting service providers (see also Section 5.5.1) and by imposing liability for such repeated false notices, especially in case they are submitted by a person in the context of their business or profession.[424]

5.3.1.4 Decision on notice and actual knowledge

As mentioned in Section 5.3.1.1, notices should be adequately substantiated. However, this does not mean that hosting service providers should not process notices that are not duly substantiated. Hosting service providers should act diligently and expeditiously on the notices they receive,[425] irrespective of whether the notice leads to actual knowledge. This includes cases where the notice is adequately substantiated (and is right or wrong on the illegality of the content), but also cases where the notice is inadequately substantiated. In order to determine whether the notice is inadequately substantiated it should indeed be first processed.

The DSA seems adequate in this regard. Article 14 of the DSA proposal seems indeed to create a two-pronged duty for hosting service providers. On the one hand they must put in place a mechanism that will help (i.e., "facilitate") notifiers to submit duly substantiated notices.[426] Such notices are presumed to give

---

[421] DSA proposal, art 14(2)(c).

[422] See also European Parliament, 'Adopting commercial and civil law rules', Annex B, art 9(1)(e).

[423] See Wilman 303–304.

[424] On this see European Parliament, 'Adopting commercial and civil law rules', Annex B, art 7(2). See also Section 5.2.7.

[425] See, e.g., Wilman 304.

[426] DSA proposal, art 14(1), 14(2).

rise to actual knowledge or awareness,[427] thereby triggering the obligation to act expeditiously thereupon (see Section 2.2). On the other hand, the DSA proposal also requires the hosting service providers to process "any notices that they receive",[428] thus irrespective of whether the notice leads to actual knowledge. Furthermore, the DSA proposal also requires that the processing of all notices shall be "timely, diligent and objective".[429] The DSA proposal itself therefore states that hosting service providers should act expeditiously on any notice. The fact that a notice is sufficiently substantiated entails actual knowledge, but this also means that the meaning of "expeditious" will be longer (Section 5.2.5).

5.3.1.5 Information rights

As indicated in Section 4.3.3, individual information rights are key procedural safeguards that should be part of any adequate notice and action mechanism. For this reason, various forms of information should be provided to users at various stages of the notice mechanism. First of all, the hosting service providers should provide information on how to use the notice mechanism. This is addressed in Section 5.2.6. This section focuses on the information rights once a decision has been taken concerning a content item pursuant to a notice.

When a "positive" decision has been taken (i.e., removal or disabling of access to the content), hosting service providers should inform both parties (i.e., notifier where relevant and content provider) of the decision,[430] and should include a general motivation of the decision. Furthermore, this obligation should not be limited to content that is removed after a notification, but also if it is removed after proactive monitoring. When a negative decision has been taken (i.e., not to remove or disable access to content -informally referred to as a "must-carry" decision), only the notifier should be informed.

Article 15 of the DSA proposal requires hosting service providers to provide a clear and specific statement of reasons leading to their decision to remove online content.[431] This provision has been criticised by various interviewed stakeholders representing online intermediaries on the account that it would be too burdensome to provide a specific statement of reason for each and every decision taken. When looking at the provision more in detail one can see that the reasons statements' core is embodied in the following two requirements. Hosting service providers must make a reference to the legal ground relied upon,[432] and must include a reference to the "facts and circumstances" that lead to the decision.[433] We do not consider such requirements overly burdensome, both on a principled basis and on a practical basis.

From a principled-based viewpoint, receiving a motivated decision is one of the key elements and safeguards of fair trial and due process rights (See Section 4.3.3). From a practical viewpoint, the requirement to provide a statement of reason should not be seen as too burdensome. First, including the legal ground does not entail much effort. In addition, there is no need to go into too many specifics of the "facts and circumstances" leading to the decision. A general, but sufficiently informative statement should suffice. This should be even easier when a notice has been submitted given the requirement that valid notices must be adequately substantiated (Section 5.3.1.1).[434]

Furthermore, the information should also mention whether the decision was taken with the help of automated tools, and what the possibilities for redress are, with specific reference to internal complaint-

---

[427] DSA proposal, art 14(3).

[428] DSA proposal, art 14(6).

[429] DSA proposal, art 14(6).

[430] See European Parliament, 'Adopting commercial and civil law rules', Annex B, art 12.

[431] DSA proposal, art 15(1).

[432] DSA proposal, art 15(2)(d).

[433] DSA proposal, art 15(2)(b).

[434] On this point, see DSA proposal, art 15(2)(b).

handling and out-of-court mechanisms. As far as these last elements are concerned, the DSA proposal seems adequate.[435]

5.3.1.6 Trusted flaggers

As indicated in Section 2.3.1.4, trusted flaggers can lead to a more efficient removal of illegal content (Section 1.5.1). However, the current legal framework is characterised both by discrepancy and uncertainty (Section 4.2.3.1). Beyond issues of discrepancy between the various trusted flagging schemes used by hosting service providers on the basis of their own initiative or as part of a self-regulatory scheme (Section 4.2.1, see also Section 3.3.3), uncertainty remains as to what constitutes an adequate trusted flagging scheme. In particular, issues of abuse of trusted flagging mechanism (both by private and public bodies) and the related risks to fundamental rights (Section 1.5.2) have been highlighted. Furthermore, because the trusted flagging schemes are non-binding, hosting service providers are not obligated to use them. We therefore recommend imposing and harmonising the trusted flagger mechanism. The harmonisation should concern the procedure for receiving the trusted flagger status and the safeguards against abuse.

First, hosting service providers should be obligated to work with trusted flaggers that fulfill certain requirements. They should process their notices with priority. Article 19(1) of the DSA proposal imposes this obligation, but only on online platforms. We recommend to extend this obligation to all hosting service providers. Specifically, it should also apply to intermediaries that facilitate the hosting of websites (Section 4.2.3.4).

As far as the trusted flagger status is concerned, the DSA proposal harmonises the procedure for being granted the trusted flagger status but only to a very limited extent. It only contains very general criteria pertaining to e.g., the expertise or diligence of the trusted flagger,[436] but leaves the concrete procedure and implementation of these criteria to the newly created Digital Services Coordinators, which operate at member state level. This solution may lead to differences in relation to trusted flaggers between the member states. We therefore recommend that the procedure for being granted the trusted flagger status is fleshed out in more detail.[437] Alternatively, there should at the very least be a harmonised certification procedure, if needed through delegated acts.

Of particular importance, the DSA proposal does not clarify whether online platforms (or in our case hosting service providers) can continue to employ their existing trusted flaggers schemes, which has been a concern for some interviewed representatives of online intermediaries.[438] However, as long as these existing schemes do not violate any other provisions of the law,[439] they should be free to continue them *in addition to* the processing of the new trusted flaggers with an officially awarded status.[440] This is our interpretation of Article 19 of the DSA proposal, but it is not stated explicitly in the DSA proposal. It would be helpful to provide additional legal certainty on this matter. Given the probable co-existence of multiple trusted flagging schemes it seems useful to also insert a non-discrimination provision.[441] Such a provision prevents

---

[435] DSA proposal, art 15(2)(c), (e).

[436] DSA proposal, art 19(2).

[437] Compare in particular with DSA proposal art 19(7), which indicates some level of harmonisation as far as the revocation of the trusted flagger status is concerned.

[438] Cf the solution put forth in the 2018 Recommendation on Measures to Effectively Tackle Illegal Content Online, which also provided for similar general and broad criteria but left it to the intermediaries to devise the procedure for being eligible as a trusted flagger. Recommendation, points 26-27.

[439] For example, the fact that a notice has been submitted by a trusted flagger does not mean that the content providers should not receive a statement of reasons. Section 5.3.1.5.

[440] See DSA proposal, art 19(1).

[441] Wilman 306.

hosting service providers from privileging the notices of certain trusted flaggers over others, but also prevents them from granting the trusted flagging to some but not to others when there is no justifiable reason. It is therefore crucial in a system that seemingly allows both certified trusted flaggers and trusted flaggers selected by the hosting service providers.

As far as abuses are concerned, the DSA proposal provides for the possibility of sanctions in case of abuse of the trusted flagging mechanism.[442] However, these provisions only concern abuses from the side of the trusted flaggers (e.g., submission of inadequate notices) but do not address other issues that might arise. These could include the lack of sufficient examination of trusted notices by the hosting service provider (akin to an automated acceptance of such notices), or the neglect of "non-trusted" notices. For these reasons, it is still important to include a provision emphasising that notices from trusted flaggers should be processed diligently and not automatically be accepted, that is, taken at face value without any further checks.[443] In other words, some minimal level of verification of these notices should always take place. This could be addressed by adding a provision requiring hosting service providers to also diligently process notices from trusted flaggers,[444] which is currently absent from the DSA proposal (Article 14(1) only requires them to process trusted noticed "with priority and without delay").

5.3.1.7 Competent authorities

Another gap that was discussed is the absence of a harmonised procedure concerning the notices and orders by law enforcement agencies and other public authorities (Section 4.3.4.2). The lack of agreement on what constitutes an adequate exchange procedure between hosting service providers and competent authorities is obviously problematic for the safeguards of the content providers' interests (Section 1.5.2) since there is no guarantee against abuses (for instance requiring the removal of legal content but which is against the terms and conditions). Finally, the interests of the hosting service providers (Section 1.5.4) can also be subject to abuse in case competent authorities would require too much of them without there being legal checks as to what can actually be required. Furthermore, harmonisation would make it easier for hosting service providers to identify competent authorities. For this reason, this report makes the following two recommendations.

First, there should be a provision clearly stating that member states' competent authorities shall communicate with hosting service providers (including concerning removal orders) via specifically established communication channels.[445] The DSA proposal's Articles 8 and 9 already mention removal orders and information orders. The provisions do not harmonise completely the procedure but do provide a number of mandatory requirements (e.g., statement of reason, territorial scope).

Second, it should be clarified and made explicit that competent authorities can only request content to be taken down on the basis of law and not on the basis of the hosting service providers' terms and conditions.[446] Competent authorities can indeed only act within the bounds of their legal mandates, which is limited to what is illegal before the law.

---

[442] DSA proposal, art 19(5), (6).

[443] Wilman 305.

[444] See, Wilman 305.

[445] See, The Greens/EFA, art 6.

[446] European Parliament, 'Fundamental rights', point 32. See also, European Parliament, 'Improving the single market', Annex II(V)(1).

5.3.2 Create harmonised redress mechanisms

The need for efficient judicial oversight was highlighted in Sections 1.5.2 and 1.5.3. As indicated in these sections, a well-functioning judicial system will enable the legal challenge of wrongful removal decisions (and also decisions not to remove). Furthermore, it contributes to upholding the rule of law in the online world which is critical to democratic societies. However, the use of judicial oversight suffers from a number of shortcomings. As far as users are concerned, the costs and efforts of suing a hosting service provider often outweighs the benefits. Further, the lengthy procedural time that characterise judicial institutions is not adequate for the speed that characterises the online world. Sections 4.3.4 and 4.2.3.2 have shown there are some emerging and diverging redress mechanisms. However, there remains disagreement as to what would constitute an adequate redress mechanism adapted to the specificities of online content. For this reason, we recommend two types of specific redress mechanisms: internal complaint-handling mechanisms (Section 5.3.2.1), and out-of-court redress mechanisms (Section 5.3.2.2).

Finally, one should not overlook the pivotal role of the judiciary system and of courts, which remain instrumental in ensuring the rule of law and ensuring that there is some public oversight on an otherwise private system of adjudication (Section 5.3.2.3).

5.3.2.1 Internal complaint-handling mechanism

One of the key safeguards identified in Section 4.3.3 concerns the need for content providers to have an opportunity to express their views when a decision has been made concerning their content.[447] This is a key safeguard in relation to the fundamental right of a fair trial (Section 4.3.3). Yet, there is no agreement as to what such a system should look like (Section 4.3.4).

Such a possibility to express one's views has often been encapsulated under the concept of counter notices (see Section 2.3.1.4). One of the key issues concerning counter notices is whether they should be *ex ante* or *ex post*, that is, whether the content provider can contest the decision before it is taken or afterwards. There are arguments on both sides.

On the one hand, there is no doubt that allowing content providers to only contest a decision after it is taken down is a deviation from standard procedural rules and works to the their detriment.[448] Furthermore, *ex ante* counter notices can also help hosting service providers to make a better informed judgement.[449] Finally, they are a useful way to ensure that the overall architecture of the DSA is not overtly skewed towards a "delete first rectify after" approach, which is detrimental not only for the overall balance of fundamental rights generally, but also for specific types of content (such as perishable content) for which it makes no sense to be reinstated after they have been down for some time (e.g., news items).[450]

On the other hand, there is no doubt that some content should be taken down immediately. This is particularly the case for child sexual abuse material or terrorist content.[451] Furthermore, Section 2.3.1.4 has shown that counter notices are seldom successful in practice and it is also easy to abuse them (e.g., use a counter-notice to keep the content online for another 2 weeks for instance). For this reason, an *ex ante* counter-notice system would lead to the further dissemination of illegal content (Section 1.5.1).

---

[447] See also, Wilman 370.

[448] Wilman 372-373. See also Angelopoulos, 'Online Platforms and the Commission's New Proposal', 40.

[449] Wilman 373.

[450] Wilman 374. See also, Sunday Times v. UK (2) App no 13166/87 (ECtHR, 24 October 1991), para 51.

[451] Wilman 374. On the increased live-streaming of copyright-infringing content, see Rickard.

There are pros and cons for both solutions, which makes it a case of "hard" or difficult balancing. We make a conscious choice in favour of an *ex post* mechanism given the flaws and impractical nature of an *ex ante* approach.[452] For this reason, and in order to avoid confusions, we distinguish between the counter notice mechanism, which is purely *ex ante*, and an internal complaint-handling mechanism, which is *ex post*.

Given the existence of other safeguards and mechanisms dedicated to redress possibilities (see Section 5.3.2.2), the goal of this internal complaint mechanism is to make it as close as possible to a counter notice mechanism (except that it is *ex post*). This has a number of consequences. First, the procedure should be as fast as possible in order to quickly address cases where content has been unduly removed (and should therefore be reinstated as quickly as possible).[453] Although the exact time will depend on the complexity of the case, a practice in which permissible content is deleted very fast but only reinstated after weeks should be avoided.

Next, the diminished level of protection for content providers should be compensated by particularly strong safeguards.[454] For this reason, content providers and notifiers should be allowed to submit complaints without revealing their real identity. In order to avoid the risks of abuses, complaints submitted to the internal complaint-handling mechanism should therefore satisfy a number of criteria in terms of precision and substantiation that are similar as those discussed in the context of notices (see section 5.3.1.1). The DSA proposal now simply refers to the submission of "sufficiently precise and adequately substantiated complaints", without offering any further detail.[455]

The submission of such complaints should also be user-friendly, meaning that the hosting service providers should facilitate the submission of complaints in a manner that is similar to notices (see section 5.3.1.2). The DSA proposal mentions an internal complaint-handling mechanism that should be "easy to access, user-friendly" and that should "enable and facilitate the submission of sufficiently precise and adequately substantiated complaints".[456] This seems adequate. Further, the DSA proposal also provides that such complaint-handling mechanism should be free.[457]

As a mechanism purely internal to the hosting service provider, it should not be expected to display all the guarantees of independence and impartiality that a court should possess.[458] Rather, we recommend that the mechanism should be subject to some minimum requirements in relation to quality, speed and impartiality. This is in line with the DSA proposal, which requires that the internal complaint-handling mechanism is "timely, diligent and objective".[459] Finally, and in line with the DSA proposal, we argue that this complaint mechanism can resort to automated tools as long as its decisions are not taken solely on the basis of automated means.[460] On the one hand, partially resorting to automated tools can help speed up the process which is key as seen herein above. On the other hand, the guarantee that there will be a human input in the decision-making process is also key for at least two reasons. First, it provides stronger fair trial

---

[452] See for instance, Quintais and others 280.

[453] Interestingly, the DSA proposal, art 17(1) now allows complaints to be submitted for "at least" 6 months after the decision has been taken. This is too long. Content providers should have a maximum of two weeks (14 days) to submit a complaint once they have been informed of the decision. Giving them more time would run counter the "*ex post* counter notice" logic of the mechanism.

[454] See also, Wilman 373-374.

[455] DSA proposal, art 17(2).

[456] DSA proposal, art 17(2).

[457] DSA proposal, art 17(1).

[458] Wilman 371.

[459] DSA proposal, art 17(3).

[460] DSA proposal, art 17(5).

safeguards. Second, it will be crucial if the original decision was taken pursuant solely automated means.[461] In line with the GDPR requirements, we argue that in case a decision on a notice is taken solely by an automated tool, there should always be the possibility to contest such decision before a human person.[462] The fact that a human will also be a part of the decision-making process of the internal complaint-handling mechanism can be used to implement this safeguard.

The DSA proposal only imposes a mandatory internal-complaint-handling system on online platforms. We recommend to extend this obligation to all hosting service providers. This is justified for two reasons. From a fundamental rights perspective, it is an important safeguard given the absence of *ex ante* contestation mechanisms. From a practical perspective, it requires very little additional resources. As explained above, we do not see it as an "internal court" but rather more like an *ex post* notice mechanism. In other words, if a hosting service provider has enough resources to examine a notice, it should also have the resources for this internal complaint-handling mechanism.

5.3.2.2 Out-of-court mechanism

Whereas the internal complaint-handling mechanism can be said to partake of the broader dimension of the decision-making procedure under a notice and action mechanism (namely ensuring that the decision-making process is fairer by allowing the content provider to challenge it very rapidly), this does not alleviate the need for a proper redress venue, which remains a key fundamental rights safeguard (Section 1.5.3), and which remains largely absent at present (Sections 2.3.1.2, 2.3.1.4 and 4.3.3). Further, such a venue should be adapted to the specificities of online content (Sections 1.5.3). As the European Parliament put it, "the immediate nature of content hosting and the often ephemeral purpose of content uploading" make it necessary to provide independent redress mechanisms that can provide quick and efficient decisions.[463] Further, such mechanisms would also relieve the burden on courts.[464] For this reason, specific and harmonised out-of-court mechanisms are needed,[465] which can function as a first venue of complaint or as a way to contest a decision taken pursuant to the internal complaint mechanism discussed in Section 5.3.2.1.[466] Out-of-court mechanisms should be easily accessible, impartial, transparent, efficient, and affordable.[467] Furthermore, they should provide a fast resolution of disputes.[468]

Article 18(1) of the DSA proposal grants users and content providers the possibility to resort to a certified out-of-court dispute settlement body. Pursuant to Article 18(2)(a), (b) and (e), the certified dispute settlement bodies must fulfil requirements of impartiality, independence, expertise, and procedural fairness. However, it contains little language on the rapidity of the process, apart from references to the body's "swift, efficient, and cost-effective" actions.[469] Yet, one of the key rationales for increasingly resorting to out-of-court mechanisms instead of courts are the speed and efficiency gains.[470] For this reason, it is

---

[461] See, DSA proposal, art 14(6).

[462] See, GDPR, art 22(3).

[463] European Parliament, resolution internal market, point 43. See also European Parliament, 'Adopting commercial and civil law rules', Annex B, Recital 16.

[464] European Parliament, resolution internal market, point 43. See also European Parliament, 'Adopting commercial and civil law rules', Annex B, Recital 17.

[465] See, e.g., EDRi 32.

[466] See the language of DSA proposal, art 18(1): "in order to resolve disputes relating to those decisions, **including complaints** that could not be resolved by means of the internal complaint-handling system referred", emphasis by authors.

[467] See, European Parliament, resolution internal market, point 43. See also European Parliament, 'Adopting commercial and civil law rules', Annex B, Recital 18.

[468] European Parliament, 'Adopting commercial and civil law rules', Annex B, Recital 17.

[469] DSA proposal, art 18(2)(d).

[470] See for instance, EDRi (n 53) 32.

useful to have stronger language on delays. Such language could be the following: 'effective and timely',[471] or 'without undue delay'.[472] A key fair trial safeguard is the ability to understand the proceedings.[473] The DSA proposal requires the out-of-court mechanism to speak "at least one official language of the Union".[474] This might not always prove sufficient. It might be better to require the out-of-court mechanism to speak the language of the hosting service provider's terms and conditions (which will be in English in most cases), and 'ideally also the language of the complainant'. Finally, in order to ensure an efficient and effective process it might also be useful to require another certification condition pertaining to human, technical, and financial resources.[475]

This leads to the issue of the financing of such mechanisms, which is key in ensuring that the right to redress is a reality and thus that the various interests are adequately balanced. The DSA proposal requires complainants to pay the fees and be refunded if they win.[476] Given the DSA proposal explicit requirement that these fees should be reasonable, such a proposal seems reasonable and can also be construed as a useful safeguard against abusive complaints (i.e., if it's free users might abuse it).[477] However, the DSA proposal also mentions that such fees should not exceed the procedure costs. Such language might contain a loophole since the DSA proposal says nothing about the maximum of these costs. Beyond the need to clarify this issue, one can argue that the requirement of reasonableness is too vague and might in practice exclude a number of potential complainants.[478] For this reason, it could be further clarified. One could also think about a role for the Digital Services Coordinators to supervise that the fees and costs remain reasonable in practice. Alternatively, a financial assistance mechanism could be put in place, for instance a fund. Such fund would be funded among others by the fines paid by hosting service providers under Article 42 of the DSA proposal.[479]

A final issue concerns the scope of out-of-court mechanisms. Under the DSA proposal they are limited to online platforms.[480] Extending the mechanism to all hosting service providers has pros and cons. Given that the internal complaint-handling mechanism is extended to all hosting service providers, content providers already have a way to contest decisions. However, as discussed in Section 5.3.2.1, this mechanism is more of an *ex post* notice mechanism than a fully-fledged complaint-handling mechanism. This means that victims and content providers of hosting services that are not platforms could only fully exert their rights to an effective remedy and fair trial before ordinary courts. As explained above, this is far from optimal.

On the other hand, one should keep in mind that the victims of illegal content on hosting services that are not online platforms are often representatives of rights holders who have sufficient resources to go to court. Furthermore, the content providers against whom they are acting (for example: websites selling counterfeits) may also be more professional than a typical user of an online platform. For this reason, an out-of-court mechanism is less important in relation to hosting service providers that are not platforms. The benefits may not always outweigh the costs that are imposed on the hosting service providers.

---

[471] The Greens/EFA, art 22(2).

[472] See, The Greens/EFA, art 22(4)(f), (g).

[473] See, European Convention on Human Rights, art 6(3)(a).

[474] DSA proposal, art 18(2)(d).

[475] See, The Greens/EFA, art 22(2).

[476] DSA proposal, art 18(3).

[477] DSA proposal, art 18(3).

[478] This points was also mentioned by the interviewed representative of a digital rights organization.

[479] See for instance, The Greens/EFA, art 22(3).

[480] DSA proposal, art 18.

At the same time, the importance of the various interests may be different in other situations. For example, an individual victim of child sexual abuse material may not have the resources to go to court. Similarly, going to a court may also represent a significant burden on a website that is hosting permissible information (for example, provided by whistleblowers) without a commercial purpose. We believe that the benefits of adequate access to justice ultimately outweigh the additional financial burdens on hosting services. For this reason, the obligation to facilitate an out-of-court mechanism should ideally apply to all hosting service providers. If this recommendation is not followed, it is even more crucial to extend the internal complaint-handling mechanism to all hosting service providers (Section 5.3.2.1).

5.3.2.3 Judicial redress

Beyond out-of-court mechanisms, it is also important to restate that individuals can exercise their right to effective remedy and to a fair trial (enshrined in Article 47 of the EU Charter for Fundamental Rights) before a court,[481] which is the only instance able to fully provide all these guarantees. Judicial oversight is therefore a crucial guarantee for the safeguards of the various involved interests (Section 1.5), and especially for the rule of law (Section 1.5.3). We therefore recommend to re-state this right and to re-emphasise that the final decision on the legality of online content rests with the judiciary system and not with privatised adjudication bodies.[482]

Currently, the DSA proposal only mentions the right to judicial redress in its recitals,[483] and incidentally as a residual recourse to other mechanisms. For instance, the right to an out-of-court mechanism is "without prejudice" to the right of redress before a court.[484] Similarly, Article 15(2)(f) mentions this possibility as part of the information provided after a decision has been taken on content. However, re-stating this right explicitly in a separate provision would have a much stronger impact. In this regard it could be proposed to require out-of-court mechanisms to regularly publish their decisions so as to inform the relevant judicial authorities.

5.4. Transparency

Transparency is of crucial importance to maintain the rule of law and judicial oversight (Section 1.5.3). However, Chapter 4 reveals several gaps in the existing transparency obligations. The obligations are often non-binding (Section 4.2.1.2), inconsistent (Section 4.2.3.1) and not targeted at all relevant aspects (Section 4.3.4.2). For this reason, the third set of recommendations concerns transparency obligations.

We have already recommended several obligations in relation to transparency. First, see recommendation 17 and Section 5.3.1.5. Furthermore, Section 5.2.6 also supports the following recommendation:

23. Self-regulation, including terms and conditions, should be clear and transparently applied (Section 5.2.6).

These recommendations are primarily important in individual cases. They allow content providers and judges to understand and correct the decision-making process for individual pieces of online content. However, much content moderation is done automatically and relatively 'invisibly', without the general public noticing that a piece of online content was scrutinized and/or removed (Section 1.5.3). Furthermore, the moderation obligations of hosting service providers should be interpreted as a duty of care. The fact that specific illegal online content was not discovered or removed faster does not necessarily mean that the

---

[481] See for instance The Greens/EFA, art 22(5).

[482] European Parliament, 'Adopting commercial and civil law rules', point 5.

[483] DSA proposal, recitals 42, 44.

[484] DSA proposal, art 18(1).

hosting service provider violated its obligations (see also Sections 5.2.3 and 5.2.6). However, this can only be analysed by going beyond the particularities of individual decisions and by looking at the entirety of the moderation practices. For this reason, we are making the following recommendations:

24. Hosting service providers, and especially platforms, should have effective and proportional reporting obligations (Section 5.4.1).
25. Reporting obligations should be harmonised and standardised as much as possible (Section 5.4.2).

5.4.1. Effective and proportional reporting obligations

The reporting obligations should be tailored to their goals. In relation to the limitation of the dissemination of illegal content, it is important that they provide insight into the moderation practices to victims, supervisory authorities and judges (see also Section 5.2.6). However, current transparency obligations often fall short of this goal. They often do not require information about important aspects (Section 4.3.4.2). For example, they may not provide insight into the number of moderation decisions that are overturned. Furthermore, they may not always provide adequate information about the safeguards in relation to automated decision making (Section 4.3.3). For this reason, it may be unclear whether the moderation provides a balance between the limitation of the dissemination of illegal content and freedom of expression and freedom of information.

The DSA proposal contains various reporting obligations.[485] Notably, these obligations correct many of the gaps identified in Section 4.3.4.2. Article 13(b) and (c) requires distinctions between various types of illegal content and between illegal content and content that violates the terms and conditions. Articles 13(d) and 23(1) require information about the functioning of the internal complaint-handling system, out-of-court dispute settlement bodies and automated moderation.[486]

At the same time, these monitoring obligations do impose substantial burdens on the hosting service providers. These burdens can put pressure on their economic viability. This is only justified if the advantages of the provided transparency outweigh its costs. In the interviews, various interviewed representatives of online intermediaries questioned whether this was the case in relation to some of these obligations. They doubted whether some parts of the required information would be useful to anyone or whether they would even be read. In contrast, an interviewed representative of a digital rights organisation insisted that the benefits may not always be easy to determine and advocated for even more transparency obligations. Furthermore, several interviewed intermediaries emphasized that these obligations may be especially burdensome for mid-sized hosting service providers that are not covered by the exceptions (Sections 5.5.3).

A detailed analysis of the various reporting obligations of the DSA proposal falls outside of the scope of this report, especially because their purposes and added value are not limited to the limitation of the dissemination of illegal content.[487] However, it is necessary to critically analyse the added-value of the various obligations.

---

[485] DSA proposal, arts 13, 23, 24, 28, 30, 31, 33. See also recitals 39, 51-52, 60-61.

[486] See also DSA proposal, arts 28(1)(a) and 33(2)(c). Very large online platforms have to audit their compliance with these and other obligations and publish the audit report.

[487] Cf the obligations in relation to advertisements of DSA proposal, art 24, 30.

5.4.2. Harmonisation and standardization of reporting obligations

The existing transparency obligations are inconsistent and not always binding (Sections 4.2.1.2 and 4.2.3.1). The costs that are imposed by the reporting obligations of the European framework may also be reduced by harmonising and standardising them as much as possible. This can make it easier to comply with the obligations (Section 1.5.4). For other involved parties, harmonisation and standardisation can make it easier to compare the moderation of various kinds of illegal content.

For this reason, the reporting obligations should be harmonised and standardised as much as possible. Unless there is a justification for a difference, aspects such as frequency, form, content and applicability should be the same for all kinds of hosting service providers and all kinds of illegal content. In contrast, the DSA proposal adds new reporting obligations without harmonising and standardising the existing obligations. The 'horizontal' reporting obligations of the DSA proposal are without prejudice to existing 'vertical' obligations, including the reporting obligations of the TERREG.[488] At the same time, it remains possible to critically assess and standardise the various reporting obligations in the non-binding instruments.

5.5. Differences between hosting service providers

Most of the recommendations in this report are aimed at the harmonisation of unjustifiable inconsistent and diverging rules. However, this is not to say that no relevant differences can exist. Generally, the European legal framework should make distinctions between hosting service providers based on the risks in relation that are caused by them. This means that exclusions from obligations should *primarily* be justified by the absence of certain risks to the interests discussed in Section 1.5. Similarly, providers that cause additional risks may be subject to additional obligations. This leads to the final set of recommendations, related to the characteristics of the hosting service providers and the content that is disseminated through them.

First, several recommendations are related to the various 'types' of hosting service providers:

26. Online platforms should have additional obligations, including an obligation to take measures against users that repeatedly disseminate illegal content (Section 5.5.1).
27. Online marketplaces should be subject to more stringent obligations, in particular in relation to the users that offer products and services on through their platform (Section 5.5.2).

Next, the size of a hosting service provider can be an adequate (although imperfect, see also Section 5.5.4) proxy for the magnitude of the risks. For this reason, the size justifies certain differences:

28. Small hosting service providers should be exempt from certain obligations in relation to risks that are not or less prevalent in the context of their services (Section 5.5.3).
29. Very large online platforms should be subject to additional obligations in relation to risks that are caused by their size and influence (Section 5.5.4).

Interestingly, the DSA proposal exempts small hosting service providers based on the number of employees and the annual turnover or balance sheet (Section 5.5.3), but creates additional obligations on very large online platforms based on the number of users (Section 5.5.4). At least in theory, a small hosting service

---

[488] DSA proposal 4-5, art 1(5); Section 3.3.1. See also DSA proposal, art 23(4). The Commission may use implementing acts to lay down standardised templates.

provider may also qualify as a very large online platform. According to recital 43 of the DSA proposal, the exemptions for small hosting service providers do not apply in this situation.

5.5.1. Additional obligations for platforms

As mentioned in Sections 1.1 and 1.2.1, most of the current issues specifically involve platforms. The fact that any user can quickly and anonymously disseminate illegal content poses specific risks for the limitation of the dissemination of illegal content (Section 1.5.1). At the same time, the fact that these platforms have become so important for the dissemination of *legal* information also means that it has become more important to safeguard fundamental rights and judicial oversight (Sections 1.5.2 and 1.5.3). For these reasons, several of the recommended obligations such as proactive monitoring, requirements in relation to self-regulation and terms and conditions, a notice and action mechanism and reporting obligations are especially relevant in relation to platforms (Sections 5.2.3, 5.2.6, 5.3.1 and 5.4.1). At the same time, we do not recommend limiting these obligations to online platforms. For example, obligations in relation to trusted flaggers and internal complaint-handling should also apply to other hosting service providers (Sections 5.3.1.6 and 5.3.2.1).

Most of the other discussed recommendations primarily concern the way platforms deal with illegal content. However, platforms should also have an obligation to take action against *users* that disseminate illegal content. Article 20(1) of the DSA proposal obligates platforms to suspend users that repeatedly provide content that is clearly illegal. In the interviews, several interviewed representatives of intermediaries indicated that they were already taking such measures.

The effectiveness of this obligation depends on the platform. The effectiveness is larger for paid services or when the value of the service is increased by using it, for example by accumulating connections or reviews. In contrast, the effectiveness will be limited if content providers can simply re-join the platform through a new account without suffering any disadvantage.

This recommendation should not be understood as to mean that a platform has a know-your-customer obligation in relation to its users. Although anonymity on the internet can come at the expense of the effective limitation of the dissemination of illegal content, it is also important for the freedom of expression and freedom of information. However, depending on the available automated measures and circumstances, a platform may be obligated to takes additional measures to limit the immediate dissemination of illegal content by new users (see also Sections 5.2.3 and 5.5.4). An interviewed representative of an online intermediary indicated that it already utilised techniques to analyse such 'pattern behaviour'.

Several interviewed representatives of victims of illegal content advocated for more obligations for intermediaries that facilitate the hosting of websites (Section 4.2.3.4). They stressed that these intermediaries were often uncooperative and that websites containing illegal content were frequently rehosted straight away with a new address. More specifically, the interviewees advocated for a know-your-customer obligation for intermediaries that facilitate the hosting of websites and a clear obligation to share this information with the victims of the illegal content.[489]

---

[489] Or at least a 'know-your-*business*-customer' obligation. See also <www.kybc.eu> accessed 3 March 2021. Cf Section 5.5.2, it may not always be possible to distinguish professional and non-professional customers. See also Nordemann. The obligation to share information about content providers of illegal content to victims already exists in The Netherlands. HR 25 November 2005, ECLI:NL:HR:2005:AU4019 (*Lycos/Pessers*). However, this obligation to share information does not entail an obligation to collect information.

For the reasons discussed above, we do not share the recommendation for a know-your-customer obligation. Especially for types of online content whose format or subject matter is not suitable for platforms, an anonymous website provides a unique way to independently use the right to freedom of expression. As long as the online content is not illegal, this should be possible. In any case, a know-your-customer obligation should contain an exception if the user can demonstrate that the content is not illegal.

At the same time, it is important to repeat that other recommendations, including general proactive monitoring obligations, notice and stay down obligations, private law liability and an obligation to set up a notice and action mechanism should also apply to these intermediaries (Sections 5.2.3, 5.2.4, 5.2.7.1 and 5.3.1). These obligations may also limit the dissemination of illegal content through constantly rehosted websites without disabling the possibility to create a website anonymously. Furthermore, a know-your-customer strategy may even be used to comply with these obligations.

5.5.2. A know-your-customer obligation for online marketplaces

Although any kind of illegal content can pose significant risks, the financial risks are particularly immediate in the case of online marketplaces that facilitate the conclusion of distance contracts. *Mala fide* traders can use these platforms to sell junk products or commit fraud outright. Furthermore, online marketplaces typically play a much more involved role than other types of hosting service providers (Section 4.2.3.4).

The combination of the increased risk and increased involvement justify the creation of additional measures. In addition to obligations in relation to taking down content[490] and an obligation to *reactively* remove content providers (see Section 5.5.1), online marketplaces should also have an obligation to *proactively* ensure that users that offer their products and services (the 'sellers') can be held accountable for illegal offers. They should have a know-your-customer obligation in relation to these sellers. This allows the victims of illegal offers to take action against these sellers. This includes the users that purchase the products and services (the 'buyers'), but also the holders of intellectual property rights and even competing traders.[491]

Article 22(1) of the DSA proposal obligates 'online marketplaces'[492] to collect certain information about the identity of the 'traders'. They must take reasonable efforts to verify this information. However, this obligation should not be interpreted too strictly and should not lead to burdensome and costly verifications.[493] Furthermore, Article 22(7) imposes an obligation to design the interface in a way that enables the 'traders' to comply with their European information duties.

Although these provisions of the DSA proposal are in line with our recommendations, they may not go far enough. Notably, the obligations only apply to professional traders.[494] However, the anonymous character of the internet allows a *mala fide* trader to act as a non-professional seller. We therefore recommend to

---

[490] As recommended in (among others) Sections 5.2.3, 5.2.4 and 5.3.1 and discussed in Sections 3.3.5 and 3.3.7.

[491] See also DSA proposal, recital 49.

[492] The DSA proposal refers to "an online platform [that] allows consumers to conclude distance contracts with traders". Cf the definition of 'online marketplace' introduced in the Modernisation Directive, arts 3(1)(b), 4(1)(e): "'online marketplace' means a service using software, including a website, part of a website or an application, operated by or on behalf of a trader which allows consumers to conclude distance contracts with other traders or consumers". Although there are some differences between the Modernisation Directive and the DSA, notably the fact that C2C relations are excluded in the DSA as discussed below, both apply when the marketplace allows the conclusion of distance contracts.

[493] DSA proposal, art 22(2), recital 50.

[494] Cf the definition in DSA proposal, art 2(e).

impose a know-your-customer obligation in relation to all sellers, including non-professional sellers. Even non-professional sellers can identify themselves relatively easily through 'electronic identification means' as defined in Article 3(2) of the eIDAS Regulation. Although these means may not be readily available in all European member states, this should change in the future as the European Commission is preparing a revision of the eIDAS Regulation, including the introduction of a European digital identity.[495] As a final note, it is important to protect these non-professional sellers from scams and harassment. For this reason, not all information collected by the online marketplace should be publicly available to anyone.[496]

5.5.3. Exemptions for small hosting service providers

Even small hosting service providers can cause risks in relation to illegal content. For individual victims, the size of the platform may not be important. For example, disseminating nude pictures of a minor through a small forum may cause just as much harm as disseminating them through a large social media service. The fact that the hosting service provider is small does not justify the dissemination of illegal content (Section 1.5.4). For this reason, even small hosting service providers should have legal obligations to limit the dissemination of illegal content, especially in relation to individual cases. For example, they should also be obligated to set up a notice and action mechanism (Section 5.3) and face liability when they refuse to take down illegal content of which they have actual knowledge (Section 5.2.7.1).

In contrast, smaller hosting service providers pose smaller threats to the society as a whole. If legal content is removed without justification, content providers can simply move to another service.[497] The risks to the fundamental rights of expression and information are therefore limited. Close judicial oversight is less important. For this reason, certain obligations that go beyond the protection of individual victims may no longer be proportional in relation to smaller hosting service providers. In order to protect their economic viability and stimulate innovation, it is justified to exempt them from these obligations.

This approach can be recognized in the DSA proposal. Article 13(2) excludes micro and small enterprises from the reporting obligations discussed in Section 5.4.1. Similarly, Article 16 excludes micro and small enterprises from the additional provisions applicable to online platforms. Although they are obligated to set up a notice and action mechanism and inform individuals of their decision (Sections 5.3.1 and 5.3.1.5), they do not have to set up internal complaint-handling and out-of-court dispute settlement systems (Sections 5.3.2.1 and 5.3.2.2). Although these systems can also be important for individual content providers and victims, they also fulfil an important role in facilitating the protection of fundamental rights and judicial oversight.

At the same time, other exemptions are not justified by an absence of risks. For example, there is no reason not to ban a user that repeatedly provides manifestly illegal content such as the nude pictures of a minor (Section 5.5.1), inform law enforcement about serious criminal offences (Article 21), inform users about the fact that they are looking at an advertisement (Article 24) or make sure that the traders are traceable (Section 5.5.2). Although the economic interests of small hosting service providers can justify a less strict interpretation of these obligations,[498] the complete exemption from these obligations is not justified by the

---

[495] Commission, 'EUid'. See also European Parliament, 'Improving the single market', point 36. In the Netherlands, electronic identification means are readily available through the banks. See <www.idin.nl> accessed 27 February 2021.

[496] Cf DSA proposal, art 22(6).

[497] This may be different for small hosting service providers that serve an impactful niche. See also Section 5.5.4.

[498] Similarly, the monitoring obligation should not be as strict for small hosting service providers. For example, it may be sufficient to only use standardised publicly available tools. The exact scope of this monitoring obligation should depend on various factors, including the availability, effectiveness and cost of such tools. Cf Section 5.2.3.

absence of risks. Instead, the exemptions in the DSA are primarily motivated by a desire to avoid disproportionate burdens.[499]

The DSA proposal only provides exemptions for 'micro' and 'small' enterprises as defined in Recommendation 2003/361/EC. This means that the exemptions only apply to enterprises that employ fewer than 50 persons *and* have an annual turnover or balance sheet total that does not exceed 10 million euro. In the interviews, various representatives of online intermediaries and an organisation representing start-ups and scale-ups in the tech sector emphasized that the various obligations are also quite burdensome for intermediaries that are (much) larger than this threshold, even though these intermediaries may not pose any substantial risks to the involved fundamental rights. For this reason, it is important to carefully consider whether slightly larger hosting service providers could also be exempted from certain obligations. For example, it might be possible to exempt medium-sized enterprise from certain reporting obligations or to further limit the obligations to very large online platforms.[500] A full evaluation of the possible exemptions falls outside the scope of this report.

5.5.4. Additional obligations for very large online platforms

Very large online platforms cause additional risks. Of course, the potential impact on the dissemination of illegal content is bigger due to the size of their user base. More fundamentally, the size of platforms can also lead to different kinds of risks. Content moderation by very large online platforms has a much bigger impact on the fundamental rights discussed in Section 1.5.2. Whereas a content provider that is censored on a small platform can simply move to the next, it is not always feasible to ignore the larger platforms without losing a significant part of the intended audience. For this reason, judicial oversight is also more important (Section 1.5.3). Finally, the size of the platforms can make them efficient channels to spread disinformation and affect the public opinion. When such actions are taken through illegal means, they become 'illegal' instead of merely harmful (see also Section 1.2.2).

For these reasons, it is justified to impose additional obligations on very large online platforms.[501] These *additional* measures should be tailored to mitigate the *additional* risks that are caused by the size of the platform. This can be different from platform to platform. At the same time, it is possible to recommend several more general responsibilities.

First, very large online platforms can only take measures to mitigate the additional risks if they are aware of them. For this reason, they should assess them. Article 26(1) of the DSA proposal therefore obligates very large online platforms to identify, analyse and assess the significant 'systemic' risks that are caused by their service. Systemic risks include the dissemination of illegal content through their services (a), negative effects for the exercise of fundamental rights (b) and intentional manipulation of the service (c). Article 33 obligates the very large online platforms to report these risk assessments.

Next, many of the additional risks can be mitigated by diligently following the other recommendations in this chapter and by going beyond their minimum requirements when feasible. For example, the dissemination of illegal content can be limited by investing in proactive monitoring obligations, an efficient

---

[499] DSA proposal, recitals 39, 43.

[500] See also Section 5.4.1. A medium-sized enterprise employs fever than 250 persons, has an annual turnover that does not exceed 50 million euros and has an annual balance sheet that does not exceed 43 million euros. On the other hand, an interviewed representative from a consumer interest organisation insisted that the reporting obligations should also apply to small enterprises.

[501] DSA proposal, recitals 53-54, 56-57; De Streel and others 12, 76, 80-81.

notice and action mechanism and cooperation with trusted flaggers (Sections 5.2.3, 5.3.1 and 5.3.1.6). The risks in relation to fundamental rights can be mitigated by coupling this content moderation with efficient safeguards. The possibility of judicial oversight can be increased by being abundantly clear in the terms and conditions and (additional)[502] transparency reports, by providing a clear and detailed statement of reasons when content is (not) removed and by facilitating effective internal-complaint handling and independent out-of-court dispute settlement (Sections 5.2.6, 5.3.1.5, 5.3.2.1, 5.3.2.2 and 5.4.1). This approach is also visible in the DSA proposal. Article 27(1) states that very large online platforms shall put in place mitigation measures, tailored to the systemic risks identified pursuant to Article 26. These measures include better content moderation, terms and conditions and cooperation with trusted flaggers.[503]

Finally, very large online platforms should take additional measures that are specifically targeted at the additional systemic risks. Article 27(1) and recital 58 of the DSA proposal give several examples. In our view, these measures should in any case include safeguards against the risks of automated tools, including the risks of unintended discrimination. The current framework does not provide sufficient safeguards against these tools (Section 4.3.3). Besides Article 27, the DSA proposal does not introduce many new safeguards against the risks of automated tools. It seems to simply acknowledge the possibility that they are used in practice, without prohibiting them (except in the context of internal complaint-handling mechanisms),[504] nor regulating them (except for isolated provisions on information duties in the context of notices).[505]

Furthermore, very large online platforms should take measures to prevent illegal content from being widely disseminated before it is identified as illegal. For example, an interviewed representative of an intermediary indicated that it automatically deprioritised content that is notified (multiple times) but not yet evaluated. Furthermore, it may be possible to proactively monitor certain high-risk content that is spreading very fast.[506]

The DSA sets the threshold of 'very large platform' at 45 million monthly active users, or approximately 10% of the population.[507] One can wonder whether this criterion is always suitable. As several interviewed representatives of intermediaries rightly remarked, the criterion should be impact, not merely size. For example, depending on the exact methodology specified in the delegated acts pursuant to Article 25(3) of the DSA proposal, this criterion would not cover platforms that serve almost 95% of a market for a service that individuals only use infrequently but has a potentially high impact (for example, the sale or lease of homes) or platforms that are only dominant in one or two member states. Within these limited markets, the systemic risks may be just as big. In any case, the increased risks that are associated with such 'important but not very large online platforms' can still influence the interpretations of the other recommended obligations.

5.6. Conclusion

This chapter provides an answer to question 4: *How can new rules best encourage hosting service providers to limit the dissemination of illegal online content?* It formulates various recommendations that lead to a better

---

[502] See DSA proposal, arts 29, 30, 31, 33.

[503] DSA proposal, art 27(1)(a), (d). See also recital 58.

[504] DSA proposal, art 17(5); Section 5.3.2.1.

[505] DSA proposal, art 14(6), 15(2)(c); Section 5.3.1.5.

[506] For example, a tweet by Trump in the last months of his presidency could qualify as such. Of course, these systems should not be subject to abusive notifications and should contain adequate safeguards. In addition to such measures in relation to *illegal content*, it is also desirable to delist or deprioritise *harmful* content. See also DSA proposal, art 29, Section 1.2.2.

[507] DSA proposal, art 25(1), (2).

limitation of the dissemination of illegal content without unduly affecting other involved interests. This conclusion will not repeat the various recommendations. Instead, it identifies the most important common themes.

The first theme is about **clarification**. Despite the fact that the e-Commerce Directive is twenty years old, many aspects are still unclear. Most notably, many issues remain unclear or otherwise a source of contention. This is why we recommend to clarify the framework by providing a Good Samaritan provision, by more clearly delineating general and specific monitoring and by providing insight about the meaning of actual knowledge (Sections 5.2.2, 5.2.4, 5.2.5 and 5.3.1.4).

The second theme pertains to **harmonisation**. The current framework prohibits member states from imposing certain obligations, but does not always harmonise the rules that should exist. Furthermore, the obligations imposed by the vertical European instruments only apply to certain types of illegal content and certain types of hosting service providers. This leads to a fragmented legal framework. We therefore recommend to harmonise several aspects of the European framework, including monitoring obligations, actual knowledge, private law liability, notice and action mechanisms and transparency obligations (Sections 5.2.3, 5.2.5, 5.2.7, 5.3.1 and 5.4.2).

The third theme concerns **codification**. Many recommendations concern measures that are already taken, even without a (harmonised) legal obligation. For example, intermediaries are already taking proactive measures and already facilitate a notice and action mechanism (Sections 5.2.3 and 5.3.1). Furthermore, many issues are already imposed by self-regulation (Section 5.2.6). Codifying these practices and self-regulation into binding law ensures that all hosting service providers are obligated to adhere to them and that infringements can be enforced.

The final theme is about **increasing the protection** of the various involved interests. We recommend various obligations that force hosting service providers to do more against illegal content or face liability if they don't (for example, see Sections 5.2.3, 5.2.7 and 5.5.2). Perhaps even more importantly, the various recommended responsibilities impose additional safeguards for fundamental rights and judicial oversight (for example, see Sections 5.2.6, 5.3.1.5, 5.3.2.1 and 5.3.2.2).

Taken together, these recommendations should lead to a clearer legal framework that balances the effective limitation of the dissemination of illegal online content with the other concerned interests.

Many, but not all, of the recommendations are in line with the DSA proposal. The DSA proposal is of a more limited scope. It only provides limited clarifications of important concepts (Sections 5.2.4 and 5.2.5) and does not harmonise liability or obligations that are imposed by other vertical instruments (for example, see Sections 5.2.3, 5.2.7 and 5.4.1). Although it codifies and regulates obligations such as the duty to facilitate a notice and action mechanism and to work with trusted flaggers (Sections 5.3.1 and 5.3.1.6), it does not codify practices such as proactive monitoring (Section 5.2.3). For this reason, it may not do enough to limit the dissemination of illegal online content. In contrast, it does substantially increase the protection of fundamental rights and judicial oversight through the harmonised and detailed notice and action mechanism (Section 5.3.1, 5.3.1.5, 5.3.2.1 and 5.3.2.2). For these reasons, the DSA proposal is in many ways a significant step forward. However, it falls short of its goal of providing a better protection of the various involved interests through a clear and harmonised framework.[508]

[508] Eg DSA proposal 2-4, 5-6, 9, 11, recitals 2-3, 35, 39, 41, 106.

6. Conclusion

Twenty years after its creation, the European framework for the liability and responsibilities of hosting service providers is in need of revision. The Dutch Ministry of Economic Affairs and Climate Policy has requested this report in order to prepare itself for the substantive aspects of this revision. In order to this, this report provides an answer to the following research questions:

1. When does a hosting service provider have 'actual knowledge' or 'awareness' as referred to in Article 14 of the e-Commerce Directive?

Chapter 2 shows that actual knowledge is a key concept of the e-Commerce Directive and the European framework for intermediary liability. Hosting service providers can only be held liable for hosting illegal content if they have actual knowledge of this content and fail to remove it expeditiously. Despite this importance, the concept is unclear. It is important to clarify the obligations to analyse the permissibility of online content, the existence of actual knowledge and the timeframe for 'expeditious' removal.

2. What role and responsibilities in relation to the limitation of the dissemination of illegal online content do hosting service providers have according to the various legislative and self-regulatory initiatives?

Chapter 3 gives an overview of the relevant legislative and self-regulatory initiatives. The European framework is fragmented. It consists of horizontal instruments that apply to all types of content, but also of many different vertical instruments that apply to specific types of content. It is formed by Directives and Regulations, but also by non-binding instruments such as soft-law (e.g., Recommendations), self-regulation (codes of conduct, codes of practice, Memoranda of Understanding, initiatives, *et cetera*).

3. Can any gaps be discerned in the European framework for the liability and responsibilities of hosting service providers?

Chapter 4 shows that the lack of harmonisation and clarification and the fragmentation of the legal framework lead to various gaps. The rules are frequently unjustifiably disharmonised, inconsistently implemented and different for each type of illegal content. The safeguards for the various involved interests are not always adequate and frequently do not apply to all kinds of content.

4. How can new rules best encourage hosting service providers to limit the dissemination of illegal online content?

Finally, Chapter 5 provides recommendations to address the identified gaps. The recommendations concern the clarification, harmonisation and codification of the European legal framework and increasing the protection of the various involved interests.

The first set of recommendations concerns the core principles of the framework for intermediary liability as introduced by the e-Commerce Directive:

1. The exemptions from liability should be maintained.
2. A 'Good Samaritan provision' is not necessary, but can still be a useful clarification.
3. Hosting service providers should have a (modest) duty of care to proactively monitor publicly available online content.
4. The delineation between general and specific monitoring obligations should be clarified. Specifically, notice and *stay* down obligations should be allowed.

5. The meaning of ‘actual knowledge or awareness’ and ‘expeditiously’ should be harmonised and clarified.
6. Self-regulation can be a useful addition, but should not be relied upon excessively.

The European framework should harmonise the private law liability in relation to the various obligations in relation to the limitation of the dissemination of illegal content:

7. A hosting service provider should be liable if it hosts content that is illegal under European law and the exemption from liability does not apply.
8. A hosting service provider should be liable whenever it violates its monitoring obligations.
9. A hosting service provider should be liable whenever it violates other duties designed to limit the dissemination of illegal content.
10. Users should be liable for uploading illegal content to platforms.
11. Harmonise and clarify the illegality of online content where feasible.

The second set of recommendations concerns the harmonisation and standardisation of these notice and action mechanisms:

12. Harmonise and standardise the notice and action procedure throughout the European Union and for all kinds of illegal content.

This general recommendation can be subdivided into a number of more specific recommendations.

13. Hosting service providers should facilitate sufficiently precise and adequately substantiated notifications.
14. Anonymous notices should be possible.
15. Safeguards should be provided against abuses of the notice mechanism.
16. Hosting service providers should act diligently on all the notices they receive (both founded and unfounded).
17. Hosting service providers should provide clear information about the decision to (not) remove online content to both the notifier and the content provider.
18. There should be a trusted flagging system, with particular emphasis on the harmonisation of the attribution of the trusted flagger status and of the prevention against abuses.
19. Competent authorities should communicate with hosting service providers through specific and harmonised channels.

In addition to these notice-related recommendations, we also make a number of recommendations concerning redress mechanisms:

20. There should be a quick internal complaint-handling mechanism.
21. There should be an out-of-court redress mechanism.
22. The possibility of judicial redress should be re-emphasised.

The third set of recommendations concerns transparency:

23. Self-regulation, including terms and conditions, should be clear and transparently applied.
24. Hosting service providers, and especially platforms, should have effective and proportional reporting obligations.
25. Reporting obligations should be harmonised and standardised as much as possible.

This final set of recommendations is related to the characteristics of the hosting service providers and the content that is disseminated through them.

First, several recommendations are related to the various ‘types’ of hosting service providers:

26. Online platforms should have additional obligations, including an obligation to take measures against users that repeatedly disseminate illegal content.
27. Online marketplaces should be subject to more stringent obligations, in particular in relation to the users that offer products and services on through their platform.

Next, the size of a hosting service provider can be an adequate (although imperfect) proxy for the magnitude of the risks. For this reason, the size justifies certain differences:

28. Small hosting service providers should be exempt from certain obligations in relation to risks that are not or less prevalent in the context of their services.
29. Very large online platforms should be subject to additional obligations in relation to risks that are caused by their size and influence.

Many of the recommendations are in line with the DSA proposal. For this reason, the DSA proposal is in many ways a significant step forward. However, the proposal is of a more limited scope and therefore falls short of its goal of providing a better protection of the various involved interests through a clear and harmonised framework.

7. List of references

Primary sources

Proposals

DSA proposal
Commission, 'Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC' COM (2020) 828 final.

DMA proposal
Commission, 'Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)' COM (2020) 842 final.

TERREG
Council of the European Union, 'Proposal for a Regulation on addressing the dissemination of terrorist content online – Confirmation of the final compromise text with a view to agreement' [2021] 5634/21.

Regulations

Accreditation and Market Surveillance Relating to the Marketing of Products Regulation
Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 [2008] OJ L218/30

CPC Regulation
Regulation (EU) 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation (EC) No 2006/2004 [2017] OJ L345/1

eIDAS Regulation
Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L257/13.

GDPR
Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L119/1.

Market Surveillance Regulation
Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 [2019] OJ L169/1.

P2B Regulation
Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services [2019] OJ L186/57.

Regulation on the marketing and use of explosives precursors
Regulation (EU) 2019/1148 of the European Parliament and of the Council of 20 June 2019 on the marketing and use of explosives precursors, amending Regulation (EC) No 1907/2006 and repealing Regulation (EU) No 98/2013 [2019] OJ L186/1.

Directives

AVMSD, Audiovisual media services Directive
Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) (codified version) [2010] OJ L95/1.

CDSMD, Copyright in the Digital Single Market Directive
Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC [2019] OJ L130/92.

CTD, Directive on combatting terrorism
Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA [2017] OJ L88/6.

CSAED, Children Sexual Abuse and Exploitation Directive
Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA [2011] OJ L335/1.

Data Protection Directive
Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

Digital Content and Digital Services Directive
Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L136/1.

Directive 2015/1535
Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification)

Enforcement Directive
Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights [2004] OJ L195/16.

European Electronic Communications Code (Recast) Directive
Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast) [2018] OJ L321/36.

e-Commerce Directive, ECD
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 [2000] OJ L178/1.

InfoSoc Directive
Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society [2001] OJ L167/10.

Modernisation Directive, Omnibus Directive
Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and modernisation of Union consumer protection rules [2019] OJ L328/7.

NIS Directive
Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L194/1.

UCPD, Unfair Commercial Practices Directive
European Parliament and Council Directive 2005/29/EC 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 [2005] OJ L149/22.

Council Framework Decisions

Counter-Racism Framework Decision
Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law [2008] OJ L328/55.

Case law

European Court of Human Rights
Sunday Times v. UK (2) App no 13166/87 (ECtHR, 24 October 1991).

EU
Joined Cases C-236/08 to C-238/08 *Google France/Louis Vuitton Malletier* [2010] ECLI:EU:C:2010:159.

Case C-324/09, *eBay* [2011] ECLI:EU:C:2011:474.

Case C-131/12 *Google Spain* [2014] ECLI:EU:C:2014:317.

Case C-210/16, *Wirtschaftsakademie* [2018] ECLI:EU:C:2018:388.

Case C-40/17, *Fashion ID* [2019]] ECLI:EU:C:2019:629.

Case C-18/18 *Glawischnig-Piesczek v Facebook* [2019] ECLI:EU:C:2019:821.

Joined Cases C-682/18 and C-683/18 *Youtube* [2020] ECLI:EU:C:2020:586, Opinion of AG Saugmandsgaard Øe.

Netherlands
HR 25 November 2005, ECLI:NL:HR:2005:AU4019 (*Lycos/Pessers*).

France
Cons. const. n° 2020-801DC of 18 June 2020, Loi no 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet.

Germany
BGH Internetversteigerung I [2004] I ZR 304/01.

National law

Avia law
Avia Law Loi no 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet (FR).

Communication Decency Act
Communication Decency Act of 1996, 47 U.S.C. § 230 (US),

Digital Millennium Copyright Act, DMCA
Digital Millennium Copyright Act of 1998, 17 U.S.C. § 512 (US).

Dutch Civil Code (*Burgerlijk Wetboek*) (NL).

French Criminal Code (*Code pénal*) (FR).

French Criminal Procedure Code (*Code de procédure pénale*) (FR)

NetzDG
Netzwerkdurchsetzungsgesetz vom 1. September 2017 (BGBl. I S. 3352), das durch Artikel 274 der Verordnung vom 19. Juni 2020 (BGBl. I S. 1328) geändert worden ist <https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html> accessed 19 November 2020 (GER).

International instruments

European Convention on human rights
Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols Nos. 11 and 14 supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13 and 16 [1950] ETS No.005.

Self-regulation; soft law; recommendations.

Code of Conduct on Countering Illegal Hate Speech Online, The Code
Code of Conduct on Countering Illegal Hate Speech Online (2016).

EU Code of Practice on Disinformation
EU Code of Practice on Disinformation (2018).

Gedragscode Notice-and-Take-Down 2018
Gedragscode Notice-and-Take-Down 2018 inclusief addendum 1 <https://noticeandtakedowncode.nl/ntd-code/> accessed 19 November 2020.

Memorandum Of Understanding on Online Advertising and Intellectual Property Rights Memorandum Of Understanding on Online Advertising and Intellectual Property Rights (2018).

Memorandum of understanding on the sale of counterfeit goods via the Internet
Memorandum of understanding on the sale of counterfeit goods via the Internet (2016)

Product Safety Pledge
Product Safety Pledge: Voluntary Commitment of Online Marketplaces with Respect to the Safety of Non-Food Consumer Products Sold Online by Third Party Sellers (2018).

Recommendation on measures to effectively tackle illegal content online, Recommendation
Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online [2018] OJ L 63/50.

Recommendation 2003/361/EC
Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises [2003] OJ L 124/36.

Secondary sources

Adviesraad Internationale Vraagstukken
Adviesraad Internationale Vraagstukken, *Regulering van online content. Naar een herijking van het Nederlandse internetbeleid* (AIV-advies 113, 24 June 2020).

Alliance to Better Protect Minors Online
Alliance to Better Protect Minors Online, 'Statement of Purpose: Alliance to Better Protect Minors Online' (2017).

Angelopoulos, *European intermediary liability in copyright*
Christina J. Angelopoulos, *European intermediary liability in copyright: A tort-based analysis* (Wolters Kluwer 2016).

Angelopoulos, 'Online Platforms and the Commission's New Proposal'
Christina J. Angelopoulos, 'On Online Platforms and the Commission's New Proposal for a Directive on Copyright in the Digital Single Market' (2017).

Barlow
John P. Barlow, 'A Declaration of the Independence of Cyberspace' (*Electronic Frontier Foundation*, 8 February 1996) <https://www.eff.org/cyberspace-independence> accessed 19 August 2019.

Charikar
Moses S. Charikar, 'Similarity estimation techniques from rounding algorithms' in *STOC '02: Proceedings of the thiry-fourth annual ACM symposium on Theory of computing* (2002).

Commission, '5th evaluation of the Code of Conduct'
Commission, '5th evaluation of the Code of Conduct' (factsheet, 2020) available at <https://ec.europa.eu/info/sites/info/files/codeofconduct_2020_factsheet_12.pdf> accessed 12 February 2021.

Commission, ‘Assessing the implementation’
Commission, ‘Report from the Commission to the European Parliament and the Council assessing the implementation of the measures referred to in Article 25 of Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography’ (report) COM (2016) 872 final.

Commission, ‘Consumer Protection Cooperation Action on Facebook’s Terms of Service’
Commission, ‘Consumer Protection Cooperation Action on Facebook’s Terms of Service’ (Factsheet, 2019) availabe at <https://ec.europa.eu/info/sites/info/files/live_work_travel_in_the_eu/consumers/documents/factsheets_on_the_changes_implemented_by_facebook.pdf> accessed 12 february 2021.

Commission, ‘Digital Single Market Strategy’
Commission, ‘A Digital Single Market Strategy for Europe’ (Communication) COM (2015) 192 final.

Commission, ‘EU Crisis Protocol: Responding to Terrorist Content Online’
Commission, ‘A Europe that protects. EU Crisis Protocol: Responding to Terrorist Content Online’ (Factsheet, 2019).

Commission, ‘EUid’
Commission, ‘Revision of the eIDAS Regulation – European Digital Identity (EUid)’ (Inception Impact Assessment) [2020] Ares(2020)3899583.

Commission, ‘First report’
Commission, ‘First Report on the application of 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 (Directive on electronic commerce)’ (report) COM (2003) 702 final.

Commission, ‘Guidance on the implementation/application of Directive 2005/29/EC on Unfair Commercial Practices’
Commission, ‘Guidance on the implementation/application of Directive 2005/29/EC on Unfair Commercial Practices’ (Staff Working Document) SWD (2016) 163 final.

Commission, ‘Impact Assessment Digital Services Act’
European Commission, ‘Impact assessment Accompanying the Proposal for a Regulation of the European Parliament and off the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC PART 1/2’ SWD (2020) 348 final.

Commission, ‘Online Platforms and the Digital Single Market’
Commission, ‘Online Platforms and the Digital Single Market. Opportunities and Challenges for Europe’ (Communication) COM (2016) 288 final.

Commission, ‘Report on the functioning of the Memorandum of Understanding’
Commission, ‘Report on the functioning of the Memorandum of Understanding on the sale of counterfeit goods on the internet’ (Staff Working Document) SWD (2020) 166 final/2

Commission, ‘Tackling Illegal Content Online’
Commission, ‘Tackling Illegal Content Online. Towards an enhanced responsibility of online platforms’ (Communication) COM (2017) 555 final.

Commission, ‘TERREG impact assessment’
Commission, ‘Impact assessment. Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on rreventing the Dissemination of Terrorist Content Online’ (Staff Working Docutment) SWD (2018) 408 final.

Council of the European Union
Council of the European Union, 'Assessment of the Code of Conduct on Hate Speech on Line: State of Play' (27 September 2019) 12522/19.

Csiszér
Gábor Csiszér, 'Presentation of Hungary concerning national legislative approach to notice and action' (EC Expert group on electronic commerce, 27 April 2017) E01636.

Van Dam
Cees van Dam C, *European Tort Law* (Second edition, Oxford University Press 2013).

Dinwoodie
Graeme Dinwoodie, 'Who are Internet Intermediaries?' in Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (OUP 2020).

Batura
Olga Batura (with support from Roel Peeters and others), *Study on redefining 'hosting' under article 14 of the e-Commerce Directive. Final report* (report for the Ministry of Economic Affairs and Climate Policy, 2020).

EDRi
EDRi, *Platform Regulation Done Right: EDRi Position Paper on the EU Digital Services Act* (2020).

Edwards
Lilian Edwards, *Role and Responsibility of Internet Intermediaries in the Field of Copyright and Related Rights* (WIPO 2011).

Van Eecke and Truyens
Patrick Van Eecke and Maarten Truyens, *EU Study on the Legal Analysis of A Single Market for the Information Society—New Rules for a New Age?* (Publications Office of the European Union 2009).

Van Eijk and others
Nico van Eijk and others, *Moving Towards Balance: A Study into Duties of Care on the Internet* (2010).

Elkin-Koren and Perel
Niva Elkin-Koren and Maayan Perel, 'Guarding the Guardians: Content Moderation by Online Intermediaries and the Rule of Law' in Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (OUP 2020).

ERGA
ERGA, 'ERGA Report on Disinformation: Assessment of the Implementation of the Code of Practice' (2020).

European Parliament, 'Adopting commercial and civil law rules'
European Parliament, 'Digital Services Act: adapting commercial and civil law rules for commercial entities operating online' (Resolution) P9_TA(2020)0273.

European Parliament, 'Fundamental rights'
European Parliament, 'Digital Services Act and fundamental rights issues posed' (Resolution) P9_TA(2020)0274.

European Parliament, 'Improving the single market'
European Parliament, 'Digital Services Act: Improving the functioning of the Single Market' (Resolution) P9_TA(2020)0272.

Frosio
Giancarlo Frosio, 'Mapping Online Intermediary Liability' in Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (OUP 2020).

Frosio and Husovec
Giancarlo Frosio and Martin Husovec, 'Accountability and Responsibility of Online Intermediaries' in Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (OUP 2020).

Frosio and Mendis
Giancarlo Frosio and Sunimal Mendis, 'Monitoring and Filtering: European Reform or Global Trend' in Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (OUP 2020).

Geiger, Frosio and Izyumenko
Christophe Geiger, Giancarlo Frosio and Elena Izyumenko, 'Intermediary Liability and Fundamental Rights' in Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (OUP 2020).

Geiger and Izyumenko
Christophe Geiger and Elena Izyumenko, 'Blocking Orders: Assessing Tensions with Human Rights' in Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (OUP 2020).

Gellert
Gellert, 'Regulation of online manipulation in the Modernisation Directive: light and shadow from a data protection viewpoint' (forthcoming/on file with the author).

Hern
Alex Hern, 'TikTok's local moderation guidelines ban pro-LGBT content' (*The Guardian* 26 September 2019) <www.theguardian.com/technology/2019/sep/26/tiktoks-local-moderation-guidelines-ban-pro-lgbt-content> accessed 8 January 2021.

High Level Expert Group on Fake News and Online Disinformation
High Level Expert Group on Fake News and Online Disinformation, *A multi-dimensional approachto disinformation* (Report to the European Commission, 2018).

Hilty and Moscon
Reto M. Hilty and Valentina Moscon, 'Digital Markets, Rules of Conduct, and Liability of Online Intermediaries—Analysis of Two Case Studies: Unfair Commercial Practices and Trade Secrets Infringement' in Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (OUP 2020).

Van Hoboken
Joris van Hoboken, 'The Proposed EU Terrorism Content Regulation: Analysis and Recommendations with Respect to Freedom of Expression Implications' (Working paper of the Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression, 2019).

Van Hoboken and others, *Hosting intermediary services and illegal content online*
Joris van Hoboken and others, *Hosting intermediary services and illegal content online. An analysis of the scope of article 14 ECD in light of developments in the online service landscape* (Study for the European Commission, 2018).

Van Hoboken and others, *WODC-onderzoek*
Joris van Hoboken and others, *WODC-onderzoek: Voorziening voor verzoeken tot snelle verwijdering van onrechtmatige online content* (IViR 2020).

Husak
Douglas Husak, *Ignorance of Law: A Philosophical Inquiry* (Oxford University Press 2016).

Husovec, *Injuctions Against Intermediaries in the European Union*
Martin Husovec, *Injuctions Against Intermediaries in the European Union. Accountable but not liable?* (Cambridge University Press 2017).

Husovec, 'The Promises of Algorithmic Copyright Enforcement'
Martin Husovec, 'The Promises of Algorithmic Copyright Enforcement : Takedown or Staydown? Which Is Superior? And Why?' (2018) 42 Columbia Journal of Law & the Arts 53.

Husovec, 'Remedies First, Liability Second'
Martin Husovec, 'Remedies First, Liability Second: Or Why We Fail to Agree on Optimal Design of Intermediary Liability' in Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (OUP 2020).

Husovec and Quintais
Martin Husovec and João Quintais, 'How to License Article 17? Exploring the Implementation Options for the New EU Rules on Content-Sharing Platforms' (2021).

INHOPE
INHOPE, 'Annual Report 2019.' (2019).

Katan
Branda M. Katan, *Toerekening van kennis aan rechtspersonen* (Wolters Kluwer 2017).

Keller
Paul Keller, 'CJEU hearing in the Polish challenge to Article 17: Not even the supporters of the provision agree on how it should work' (*Kluwer Copyright Blog* 11 November 2020) <http://copyrightblog.kluweriplaw.com/2020/11/11/cjeu-hearing-in-the-polish-challenge-to-article-17-not-even-the-supporters-of-the-provision-agree-on-how-it-should-work/> accessed 11 November 2020

Klos
Michael Klos, 'Wrongful moderation' [2020] NJB 3314.

Koelman
Kamiel Koelman, 'Online Intermediary Liability' in P Bernt Hugenholtz (ed), *Copyright and Electronic Commerce: Legal Aspects of Electronic Copyright Management* (Kluwer Law International 2000).

Kuczerawy
Aleksandra Kuczerawy, 'From 'Notice and Takedown' to 'Notice and Stay Down': Risks and Safeguards for Freedom of Expression' in Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (OUP 2020).

Kukliš
Ľuboš Kukliš, 'Video-Sharing Platforms In AVMSD – A New Kind Of Content Regulation' (2020).

Kulk, *Internet intermediaries and copyright law*
Stefan Kulk, *Internet intermediaries and copyright law. Towards a Future-proof EU Legal Framework* (2018)

Kulk, 'Platformaansprakelijkheid'
Stefan Kulk, 'Platformaansprakelijkheid – van 'notice and takedown' naar algoritmisch toezicht' [2020] NtEr 132.

Kulk and Snijders
Stefan Kulk and Thom Snijders, 'Hoofdstuk 4. Casestudy Contentmoderatie door online platformen' in Stafan Kulk and Stijn van Deursen (ed), *Juridische aspecten van algoritmen die besluiten nemen* (Montaigne Centrum voor Rechtsstaat en Rechtspleging 2020)

Larroyed
Aline Larroyed, 'Assessing the Translations of Article 17 DCDSM: Finding the Delicate Balance and Specific Context Defining the "Best Efforts" Concept' (*Kluwer Copyright Blog* 21 December 2020) <http://copyrightblog.kluweriplaw.com/2020/12/21/assessing-the-translations-of-article-17-dcdsm-finding-the-delicate-balance-and-specific-context-defining-the-best-efforts-concept/> accessed 21 December 2020

Leskovec, Rajaraman and Ullman
Jure Leskovec, Anand Rajaraman and Jeffrey D. Ullman, *Mining of Massive Datasets* (2019)

Matthews
Paul Matthews, 'Ignorance of the law is no excuse?' (1983) 3 Legal Studies 174.

McGonagle
Tarlach McGonagle, 'Free Expression and Internet Intermediaries: The Changing Geometry of European Regulation' in Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (OUP 2020).

Montagnani
Maria Lillà Montagnani, 'A New Liability Regime for Illegal Content in the Digital Single Market Strategy' in Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (OUP 2020).

Montagnani and Trapova
Maria Lillà Montagnani and Alina Yordanova Trapova, 'Safe Harbours in Deep Waters: A New Emerging Liability Regime for Internet Intermediaries in the Digital Single Market' [2018] 26 International Journal of Law and Information Technology 294.

Nguyen and others
Thanh Thi Nguyen and others, *Deep Learning for Deepfakes Creation and Detection: A Survey* (2020) arXiv:1909.11573.

Nordemann
Jan Bernd Nordemann, 'Rogue Websites: Domain registrars have a duty to disconnect, says German BGH', (*Kluwer Copyright Blog* 15 February 2021) <http://copyrightblog.kluweriplaw.com/2021/02/15/rogue-websites-domain-registrars-have-a-duty-to-disconnect-says-german-bgh/> accessed 28 February 2021.

OECD
OECD, *The economic and social role of internet intermediaries* (2010).

OECD/EUIPO
OECD/EUIPO, *Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact* (OECD publishing 2019)

Plasilova
Iva Plasilova and others, *STUDY FOR THE "Assessment of the Implementation of the Code of Practice on Disinformation" Final Report* (2019).

Quintais and others
João Pedro Quintais and others, 'Safeguarding User Freedoms in Implementing Article 17 of the Copyright in the Digital Single Market Directive: Recommendations from European Academics' (2019) 10 Journal of Intellectual Property, Information Technology and Electronic Commerce Law 277.

Revolidis
Ioannis Revolidis, 'Internet Intermediaries and Copyright Enforcement in the EU: In Search of a Balanced Approach' in Marcelo Corrales, Mark Fenwick and Nikolaus Forgo (eds), *New Technologies, Big Data and the Law* (Springer 2017).

Rickard
James Rickard, 'Going Live: The Role of Automation in the Expeditious Removal of Online Content' (2016) 96 Boston University Law Review 2171.

Rosati
Eleonora Rosati, 'The Direct Liability of Intermediaries' in Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (OUP 2020).

Sartor
Giovanni Sartor, *Providers Liability: From the Commerce Directive to the future* (in-depth analysis for the European Parliament, PE 614.179, 2017).

Senftleben
Martin Senftleben, 'Intermediary Liability and Trade Mark Infringement: Proliferation of Filter Obligations in Civil Law Jurisdictions?' in Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (OUP 2020).

Stalla-Bourdillon
Sophie Stalla-Bourdillon, 'Internet Intermediaries as Responsible Actors? Why It Is Time to Rethink the E-Commerce Directive as Well' in Mariarosaria Taddeo and Luciano Floridi (eds), *the Responsibilities of Online Service Providers* (Springer 2017).

De Streel and others
Alexandre de Streel and others, *Online Platforms' Moderation of Illegal Content Online. Law, Practices and Options for Reform* (Study for the European Parliament PE 652.718, 2020).

Schmon
Christoph Schmon, 'EFF Responds to EU Commission on the Digital Services Act: Put Users Back in Control' (*EFF* 4 September 2020) <https://www.eff.org/deeplinks/2020/09/eff-responds-eu-commission-digital-services-act-put-users-back-control> accessed 5 February 2021.

Senden
Linda Senden, *Soft Law in European Community Law* (Hart Publishing 2004).,

van der Sloot
van der Sloot Bart, 'Welcome to the Jungle: The Liability of Internet Intermediaries for Privacy Violations in Europe' (2015) 6 Journal of Intellectual Property, Information Technology and Electronic Commerce Law 211

Svantesson
Dan Jerker B. Svantesson, 'Internet Jurisdiction and Intermediary Liability' in Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (OUP 2020).

Taddeo
Mariarosaria Taddeo, 'The Civic Role of OSPs in Mature Information Societies' in Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (OUP 2020).

The Greens/EFA
The Greens/EFA, 'Regulation on procedures for notifying and acting on illegal content and for content moderation under terms and conditions by information society services', (2020)

Tworek and Leerssen
Heidi Tworek and Paddy Leerssen, 'An Analysis of Germany's NetzDG Law' (Working paper of the Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression, 2019).

Ullrich, 'Standards for Duty of Care?'
Carsten Ullrich, 'Standards for Duty of Care? Debating Intermediary Liability from a Sectoral Perspective' (2017) 8 JIPITEC 111

Ullrich, 'A risk-based approach towards infringement prevention on the internet'
Carsten Ullrich, 'A risk-based approach towards infringement prevention on the internet: adopting the antimoney laundering framework to online platforms' (2018) 26 ILJIT 226.

Verbiest and others
Thibault Verbiest and others, *Study on the liability of internet intermediaries* (2007).

Walree
T.F. Walree, 'De onrechtmatige verwerking van persoonsgegevens: geen concrete gevolgen, wel schadevergoeding?' [2020] RMThemis 167.

Walree and Wolters
Tim F. Walree and Pieter T.J. Wolters, 'The right to compensation of a competitor for a violation of the GDPR' (2020) 10 IDPL 346.

WePROTECT Global Alliance
WePROTECT Global Alliance, 'The WePROTECT Global Alliance: Our Strategy to End the Sexual Exploitation of Children Online' (2016).

Wilman
Folkert Wilman, *The Responsibility of Online Intermediaries for Illegal User Content in the EU and the US* (Edward Elgar 2020).

Wolters
P.T.J. Wolters, 'Search Engines, Digitalization and National Private Law' [2020] ERPL 795.

Yannopoulos
Georgios N. Yannopoulos, 'The Immunity of Internet Intermediaries Reconsidered?' in Mariarosaria Taddeo and Luciano Floridi, *The Responsibilities of Online Service Providers* (Springer 2017).

Appendix 1. Steering committee Ministry of Economic Affairs and Climate Policy

Name	Department	Role
René van Eijk	Digital Economy	Chairman
Marieke Sluijters	Competition and Consumers	Member
Angela van der Meer	Innovation and Knowledge	Member
Maarten van Waveren	Digital Economy	Member
Bob van Engelen	Digital Economy	Member
Fleur Gribnau	European and International Affairs	Member
Feike Kuipers	European and International Affairs	Member
Mathijs Tollerton	Legislation and Legal Affairs	Member
Lubna Safeer	Digital Economy	Member
Members from other ministries		
Bastiaan Winkel	Ministry of Justice and Security	Member
Inge Welbergen	Ministry of Education, Culture and Science	Member