

# Towards a better notice and action mechanism in the DSA

by Pieter Wolters and Raphaël Gellert\*

**Abstract:** The adoption of the DSA will bring important changes in the content moderation landscape in the EU. By harmonising, codifying, and further developing a notice and action mechanism, the DSA addresses many content moderation-related challenges, and in so doing also affects the balance that existed thus far between the protection of victims of illegal content, the safeguarding of fundamental rights and the economic interests of hosting service providers. This contribution answers the following question: Does the notice and action mechanism of the DSA create an adequate balance between the various involved interests?

As far as the economic interests of hosting service providers are concerned, the harmonisation of the mechanism should certainly be a welcome change for economic operators. Further, even though the DSA contains many new procedural obligations, they entail reasonable efforts.

The requirement of a harmonised, efficient, effective and user-friendly notification procedures should fix

the existing limitations and can be seen as an important step for the protection of the victims' interests. However, the lack of an obligation to provide a statement of reasons to notifiers is a missed opportunity.

Finally, the safeguards of content providers' fundamental rights are also enhanced. Not only through the creation of new redress mechanisms, but also through the hosting provider services' obligation to provide decisions that are objective, non-arbitrary, diligent and timely, and to justify them through a statement of reasons. Although the applicability of the safeguards is still too narrow in some respects, the new safeguards and their requirements should improve the current situation in which hardly any binding legal provisions exist.

All in all, even though it contains various shortcomings that prevent it from truly striking an adequate balance, the DSA's notice and action mechanism does represent a significant step forward for all the parties that have a stake in the moderation of online content.

**Keywords:** Digital Services Act; Notice-and-Action; Freedom of Expression; Illegal Content; Online platforms  
Notice-and-action

© 2023 Pieter Wolters and Raphaël Gellert

Everybody may disseminate this article by electronic means and make it available for download under the terms and conditions of the Digital Peer Publishing Licence (DPPL). A copy of the license text may be obtained at <http://nbn-resolving.de/urn:nbn:de:0009-dppl-v3-en8>.

Recommended citation: Pieter Wolters and Raphaël Gellert, Towards a better notice and action mechanism in the DSA, 14 (2023) JIPITEC 403 para 1.

## A. Introduction

1 On 15 December 2020, the European Commission published its long-awaited proposal for the Digital Services Act ('DSA proposal').<sup>1</sup> More than twenty

\* Pieter Wolters is an associate professor at the Radboud University and the Radboud Business Law Institute. Raphaël Gellert is an assistant professor at the Radboud University and the Radboud Business Law Institute. Both are affiliated to Radboud University's interdisciplinary hub

years after the adoption of the e-Commerce Directive,<sup>2</sup> the DSA revised the European framework

on digitalization and society (iHub).

1 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.

2 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information

for the liability and responsibilities of ‘intermediary services’.<sup>3</sup> Following the ‘General approach’<sup>4</sup> of the Council and ‘Amendments’<sup>5</sup> by the European Parliament, the DSA was adopted on 19 October 2022.<sup>6</sup>

- 2 The core of the framework remains the same. Like the e-Commerce Directive, the DSA holds that these providers cannot be held liable for transmitting or storing information that is provided by the ‘recipients of the service’ (the ‘content providers’).<sup>7</sup> However, ‘hosting’ service providers can be held liable if they know about the illegal content and do not act expeditiously to remove or disable access to the information.<sup>8</sup>
- 3 At the same time, the DSA also introduces new obligations for the providers of intermediary services.<sup>9</sup> Notably, ‘online platforms’ and other providers of ‘hosting’ services have a duty to take reactive steps against ‘illegal content’.<sup>10</sup> Article 16 of the DSA obligates providers to put a notice and action mechanism in place, allowing anyone to notify them of hosted illegal content. The hosting service providers must subsequently remove or

disable access to the illegal content or face liability.<sup>11</sup> Although such a mechanism is already used by many online platforms and imposed by various specific European rules, national laws and codes of conduct (Section 3), the DSA harmonises, codifies and develops the existing practices and rules. It imposes a notice and action mechanism that applies to all hosting services<sup>12</sup> and for all types of illegal content. Furthermore, the DSA develops the mechanism by providing detailed rules and safeguards, including a statement of reasons (Article 17) and redress mechanisms (an internal complaint-handling system and a system for out-of-court dispute settlements).<sup>13</sup> For the purpose of this article, these safeguards are considered an integral part of the notice and action mechanism.

- 4 In accordance with the aims of the DSA, the notice and action mechanism is designed to strike a proper balance between the various competing interests.<sup>14</sup> In this article, we analyse how the mechanism has considered the various interests and whether it has succeeded in creating a proper balance. We answer the following question: *Does the notice and action mechanism of the DSA create an adequate balance between the various involved interests?*

---

society services, in particular electronic commerce, in the Internal Market [2000] OJ L178/1.

- 3 DSA, arts 1(2)(a), 3(g).
- 4 Council of the European Union, ‘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 - General approach’ 13203/21.
- 5 European Parliament, ‘Digital Services Act: Amendments adopted by the European Parliament on 20 January 2022 on the 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’ P9\_TA(2022)0014.
- 6 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L277/1.
- 7 DSA, arts 3(b), 4-6; e-Commerce Directive, arts 12-14.
- 8 DSA, arts 3(g), 6(1)(a), (b); e-Commerce Directive, art 14(1) (a), (b). See DSA, arts 3(g), 4-5; e-Commerce Directive, arts 12-13 about the conditions under which providers of ‘mere conduit’ and ‘caching’ services can be held liable.
- 9 See also DSA, art 1(2)(b).
- 10 DSA, art 3(h), (i); n 15.

- 5 We consider the balance as ‘adequate’ if the DSA addresses the limitations of the current legal framework (see Section 4) and creates a framework that leads to a proper balance of the various involved interests. The notice and action mechanism should strengthen *both* the protection of society and individual victims against illegal content *and* the involved fundamental rights without disproportionately affecting the economic interests of hosting service providers. As a minimum requirement, Article 52 of the Charter of Fundamental Rights of the European Union should be respected. Any limitation of a fundamental right should be proportional and respect the essence of this right. Within the bandwidth that the Charter provides, the heterogeneity of the various involved interests makes the determination of the ‘best’ way

---

11 DSA, arts 6(1)(b), 16(3).

12 However, some exclusions exist for micro and small enterprises. DSA, art 19.

13 DSA, arts 20, 21.

14 DSA, recital 52. About the aims of the DSA in general, see also DSA, recitals 3, 4, 40, art 1(1). The e-Commerce Directive has the same goals. See eg Case C-360/10 SABAM [2012] ECLI:EU:C:2012:85, para 51; e-Commerce Directive, recital 41; 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), 563.

to balance them subjective. However, it is possible to formulate general requirements that should be fulfilled. First, the protection of one interest (such as the protection of victims through the removal of illegal content) should not disproportionately affect other involved interests (such as the freedom of information). Furthermore, the balance is not adequate if the protection of one of the interests can be improved with either no or only minimal adverse effects to the other involved interests.

- 6 The article is structured as follows. Section B provides a short description of the most important involved interests. Next, we give a birds-eye overview of the current practices and rules (Section C) and their limitations (Section D). Section E discusses the notice and action mechanism in the DSA. It analyses how the mechanism has considered the various interests and whether it leads to an adequate balance. Section 6 provides a conclusion: Although the notice and action mechanism in the DSA is a significant step forward, it contains various shortcomings that prevent it from truly striking an adequate balance.
- 7 Importantly, this article is focussed on the notice and action mechanism of the DSA. For this reason, it is necessary to at least tentatively accept some of the propositions underlying the adoption of such a mechanism. Most importantly, it is necessary to tentatively accept that it has the potential to limit the dissemination of illegal content without unduly affecting other concerned interests. The conditions that are necessary for this result are discussed in Section B. Furthermore, the article does not discuss the role of other forms of ‘content moderation’ such as (voluntary) proactive monitoring and the role of ‘trusted flaggers’.<sup>15</sup> Furthermore, we do not discuss provisions that are relevant but not directly part of the notice and action mechanism such as reporting and transparency obligations.<sup>16</sup>

## B. The involved interests

- 8 A proper balance between the various interests can only be achieved through an adequate understanding of what these interests involve. For this reason, this Section gives an overview of the most important interests in relation to notice and action mechanisms. It subsequently discusses the protection of the victims of illegal content (Section B. I.), the fundamental rights of the recipients of the hosting services (Section B. II.) and the economic interests of hosting services (Section B. III.).

<sup>15</sup> e-Commerce Directive, art 15; DSA, arts 3(t), 7-8, 22.

<sup>16</sup> Eg DSA, arts 14, 15, 24, 42.

## I. Protecting victims of illegal content

- 9 ‘Illegal content’ has a broad definition. Pursuant to Article 2(h) of the DSA, it includes “any information, which, in itself or in relation to an activity, including the sale of products or the provision of services, is not in compliance with Union law or the law of any Member State, irrespective of the precise subject matter or nature of that law”. It includes information that is illegal in itself, such as terrorist content, illegal hate speech or child pornography, but also information that relates to illegal activities such as online stalking, the sale of counterfeit goods, non-authorised use of copyright protected material or infringements of consumer law.<sup>17</sup>
- 10 Due to this broad definition, the ‘victims’ of illegal content also come in all shapes and forms. A victim can be a defrauded consumer, a child who is depicted in pornography, a rights holder whose content is disseminated without permission or a recipient that is exposed to shocking or otherwise inappropriate content. The victim can be a recipient of the hosting service, but this is not necessary. For example, a victim of hate speech may be targeted by reactions on his or her pictures on social media, but also by posts on a forum of which they are not a user. Finally, illegal content such as terrorist content is not always aimed at individual victims. It (also) threatens society as a whole. Because of the differences between these victims, their interests and needs may be different. However, there are also strong similarities.
- 11 First, the notice and action mechanism should be effective. It should lead to the speedy removal of the illegal content.<sup>18</sup> The longer the illegal content stays up, the more harm it can cause.<sup>19</sup> Furthermore, a successful notification should also provide some future protection. This can be directly achieved by preventing the illegal content from being

<sup>17</sup> DSA, recital 12.

<sup>18</sup> Some victims may not always be interested in removal. For example, rights holders may prefer monetization of the infringing content. Cf Annemarie Bridy, ‘The Price of Closing the Value Gap: How the Music Industry Hacked EU Copyright Reform’ (2020) 22 *Vand J of Ent & Tech L* 323, 330-331; Henning Grosse ruse-Khan, ‘Transition through automation’ in Niklas Bruun and others (ed), *Transition and coherence in Intellectual Property Law* (Cambridge University Press 2021) 160.

<sup>19</sup> Eg, Joris van Hoboken and others, *WODC-onderzoek: Voorziening voor verzoeken tot snelle verwijdering van onrechtmatige online content* (IViR 2020) 73.

reuploaded,<sup>20</sup> but also indirectly by suspending or otherwise punishing the content providers. The notifier should be informed about the decision concerning the notified content.<sup>21</sup>

- 12 The victim may also benefit from further redress such as a right to damages from the content provider. A notice and action mechanism can be used to facilitate this right. Although a successful notification typically leads to the removal of the illegal content, a notifier could also require other actions from the hosting service provider such as the provision of information about the identity of the content provider. An order to share information about content providers of illegal content can already be obtained in some jurisdictions.<sup>22</sup> However, such an order is only useful if the hosting service providers know the identity of the content providers with some degree of certainty. This is not the case with most online platforms<sup>23</sup> and other hosting service providers.<sup>24</sup> Furthermore, the DSA does not impose a general<sup>25</sup> ‘know-your-customer-obligation’ on hosting service providers. For these reasons, a duty to share information about the content providers is not part of the notice and action mechanism in the DSA. It is also not discussed further in this article.
- 13 Second, the notice and action mechanism should be efficient. Submitting a notification should be free, accessible, fast and user-friendly.<sup>26</sup> Submitting

a notification should not have any negative consequences. For example, a notifier should not have to fear retaliation from the user that uploaded the content. This can be achieved by allowing anonymous notifications.<sup>27</sup>

- 14 In the end, the attractiveness of the notice and action mechanism depends on its costs and benefits. Victims are less likely to submit notifications if it takes a long time and seldomly leads to speedy removal. In contrast, they will submit more notifications if it can be done with a few clicks and the illegal content is actually removed within a short timeframe.

## II. Safeguarding fundamental rights

- 15 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 recipients of the services. However, 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.<sup>28</sup> Furthermore, the illegal content may also affect fundamental rights. For example, child sexual abuse material affects the fundamental rights of children protected in Article 24 of the

20 A notice and stay down mechanism. See Section 3.

21 Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online [2018] OJ L 63/50, point 8.

22 Cf HR 25 November 2005, ECLI:NL:HR:2005:AU4019 (*Lycos/Pessers*) (for providers that host websites, in the Netherlands); Case C-275/06 *Promusicae* [2008] ECLI:EU:C:2008:54 (for internet service providers, in Spain); Rb. Amsterdam (vzr.) 25 June 2015, ECLI:NL:RBAMS:2015:3984 (for Facebook, in the Netherlands); n 24.

23 Although Facebook has a ‘real name’ requirement, it is possible to use a pseudonym. About this requirement on Facebook and other online platforms, see eg Shun-Ling Chen, ‘What’s in a name? – Facebook’s real name policy and user privacy’ (2018) 28 *Kan J L & Pub Pol’y* 146.

24 For examples, see <<https://www.kybc.eu/case-studies-research/>>.

25 DSA, art 30 only contains a know-your-customer obligation in relation to (professional) traders for platforms that allow consumers to conclude distance contracts with traders.

26 Eg Recommendation on measures to effectively tackle illegal content online (n 21), point 5; Alexandre de Streeel and others, *Online Platforms’ Moderation of Illegal Content*

*Online. Law, Practices and Options for Reform* (Study for the European Parliament PE 652.718, 2020) 40, 49, 69, 79.

27 Recommendation on measures to effectively tackle illegal content online (n 21), point 7; De Streeel and others (n 26) 51.

28 Commission, ‘Tackling Illegal Content Online. Towards an enhanced responsibility of online platforms’ (Communication) COM (2017) 555 final, 2; European Parliament, ‘Digital Services Act: Improving the functioning of the Single Market’ (Resolution) P9\_TA(2020)0272, point 6; 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) 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 John P. Barlow, ‘A Declaration of the Independence of Cyberspace’ (Electronic Frontier Foundation, 8 February 1996) <<https://www.eff.org/cyberspace-independence>> accessed 9 September 2021; Dan Jerker B. Svantesson, ‘Internet Jurisdiction and Intermediary Liability’ in Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (OUP 2020) 692–693. See also P.T.J. Wolters, ‘Search Engines, Digitalization and National Private Law’ [2020] *ERPL* 795, 799 for more examples of internet exceptionalism in law.

Charter. In contrast, this section primarily focusses on the fundamental rights of *other* users.

- 16 Content moderation is often imprecise and it can lead to over-removal. This risk is especially relevant if the permissibility of certain content is unclear. 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.<sup>29</sup> Furthermore, for many types of illegal content, this line may be drawn differently in each member state.<sup>30</sup> In these circumstances, a hosting service provider may be induced to err on the side of caution. For them, the direct legal risk of liability for permitting content that is ultimately deemed illegal outweighs the indirect<sup>31</sup> adverse effects of removing lawful content.<sup>32</sup> This leads to a limitation of the freedom

of expression and freedom of information.

- 17 The removal of online content can also affect other fundamental rights and lead to discrimination. Content moderation may disproportionately affect certain groups. For example, 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.<sup>33</sup> Furthermore, certain types of over-removal may be more damaging to the society as a whole. For example, the removal of news also affects the freedom of the press.<sup>34</sup>

- 18 The fundamental rights can be protected by only removing online content that is undoubtedly or 'manifestly' (see Section 3.1) illegal.<sup>35</sup> Furthermore, a notice and action mechanism (and content moderation in general) should include safeguards to prevent the removal of permissible content.<sup>36</sup> This does not mean that content moderation should never go beyond the removal of manifestly illegal online content. Different platforms with different content moderation practices can cater to different people and different types of content. For example, removing legally permissible insults may stimulate other recipients to express themselves more freely and thus facilitate freedom of information and freedom of expression.<sup>37</sup> At the same time, these moderation practices should be non-discriminatory, transparent, well-balanced, and consistently applied.<sup>38</sup>

- 19 By submitting a notification, the notifier forces the hosting service provider to judge whether the

29 Thibault Verbiest and others, *Study on the liability of internet intermediaries* (2007) 14-15; Georgios N. Yannopoulos, 'The Immunity of Internet Intermediaries Reconsidered?' in Mariarosaria Taddeo and Luciano Floridi, *The Responsibilities of Online Service Providers* (Springer 2017) 50; Christophe Geiger, Giancarlo Frosio and Elena Izyumenko, 'Intermediary Liability and Fundamental Rights' in Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (OUP 2020) 146; 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) 483; Maria Lilla 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) 304; De Streeel and others (n 26) 40, 43, 52.

30 Verbiest and others (n 29) 14-15; Montagnani (n 29) 304; De Streeel and others (n 26) 40, 51, 56-57, 61.

31 Strict content moderation may affect the popularity of a service. Cf De Streeel and others (n 26) 44. The terms and conditions of the hosting services are generally stricter than the law and also prohibit certain kinds of undesirable content that is not (always) illegal. For this reason, the removal of such content does not constitute a breach of contract towards the recipients. Eg Verbiest and others (n 29) 16; Yannopoulos (n 29) 50; Giancarlo Frosio, 'Mapping Online Intermediary Liability' in Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (OUP 2020) 26; De Streeel and others (n 26) 10, 14, 40, 43, 61.

32 Eg Joined Cases C-682/18 and C-683/18 *Youtube* [2020] ECLI:EU:C:2020:586, Opinion of AG Saugmandsgaard Øe, para 189; European Commission, 'Impact assessment Accompanying the 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 PART 1/2' SWD (2020) 348 final, box 1; Frosio (n 31) 26; 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) 527; McGonagle (n 29) 483; De Streeel and others (n 26) 23.

33 DSA, recital 81; 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](https://www.theguardian.com/technology/2019/sep/26/tiktoks-local-moderation-guidelines-ban-pro-lgbt-content)> accessed 13 September 2021.

34 Cf Geiger, Frosio and Izyumenko (n 29) 143; De Streeel and others (n 26) 83.

35 Geiger, Frosio and Izyumenko (n 29) 140-147; De Streeel and others (n 26) 77.

36 Commission, 'Tackling Illegal Content Online' (n 28) 3, 20; Commission, 'Impact Assessment Digital Services Act' (n 32), points 51-52, 54.

37 Cf Commission, 'Impact Assessment Digital Services Act' (n 32), point 62.

38 Commission, 'Impact Assessment Digital Services Act' (n 32), points 54, 57.

content is permissible. Although it is broadly argued that hosting service providers should not be the ones to make these complex decisions, or to determine the balance between the protection of victims and fundamental rights and become the judges of online legality,<sup>39</sup> the fact that they carry the *responsibility* to separate illegal and permissible content after receiving a notification is not necessarily undesirable. After all, their services also facilitate the dissemination of illegal content.

- 20 At the same time, the ultimate *power* to make the distinction should not lie with the hosting service providers: it should lie with judges. In theory, both victims and content providers can go to a court when they disagree with a decision to (not) remove certain content.<sup>40</sup> In practice, this opportunity is used infrequently. The costs and efforts generally outweigh the benefits.<sup>41</sup>
- 21 This issue is exacerbated by the influence of hosting services, and online platforms in particular. Depending on the message or type of online content, platforms can become so ubiquitous that their services are the only way to effectively disseminate information.<sup>42</sup> In these situations, the platforms become the *de facto* judges about the permissibility of online content.<sup>43</sup>
- 22 Because of the *de facto* influence and responsibility of the hosting services, the dispute resolution in relation to content moderation affects the fundamental right to a fair trial of both the victim and the content provider. Although not every form

39 Eg Joined Cases C-682/18 and C-683/18 *Youtube* [2020] ECLI:EU:C:2020:586, Opinion of AG Saugmandsgaard Øe, para 187; 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), 290; Frosio (n 31) 26; Kuczerawy (n 32) 527; De Streel and others (n 26) 45; Svantesson (n 28) 693.

40 Cf e-Commerce Directive, art 18.

41 Eg 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, 351, with references to further literature.

42 About this issue, see eg Commission, 'Impact Assessment Digital Services Act' (n 32), points 85-86; Yannopoulos (n 29) 46, 53-56; Geiger, Frosio and Izyumenko (n 29) 138-139; Kuczerawy (n 32) 527; McGonagle (n 29) 479-480; De Streel and others (n 26) 80-81; Mariarosaria Taddeo, 'The Civic Role of OSPs in Mature Information Societies' in Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (OUP 2020), 134-136.

43 N 39, 42.

of content moderation can, or should, be the same as a court proceeding, accessible forms of alternative dispute resolution should exist, be fair and have adequate safeguards. Finally, judicial oversight can be reinforced through transparency. When a notice and action mechanism is used, the hosting service provider should provide clear reasons for its decisions to both the notifier and (when an action is taken) the content providers. This allows both the involved parties and the courts to understand and critically assess the decisions. Furthermore, the costs and efforts to go to court should not be too high.

### III. The economic interests of hosting service providers

- 23 The liability and responsibilities of hosting service providers come at the expense of their economic viability and their fundamental right to freedom of business.<sup>44</sup> 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.<sup>45</sup> 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 services or start charging a (higher) price.
- 24 The economic interests of the hosting service providers can be protected by only imposing a notice and action mechanism and certain requirements or safeguards when they are proportional and can be fulfilled at a reasonable cost.<sup>46</sup> Furthermore, the responsibilities should be clear, harmonised, consistently applied and technology-neutral.<sup>47</sup>

44 About this right, see DSA, recital 52; Geiger, Frosio and Izyumenko (n 29) 148-149.

45 DSA, recital 1; Commission, 'Online Platforms and the Digital Single Market. Opportunities and Challenges for Europe' (Communication) COM (2016) 288 final, 2-3; Commission, 'Tackling Illegal Content Online' (n 28) 2.

46 DSA proposal 8, 13; DSA, recital 4; European Parliament, 'Improving the single market' (n 28), point 10.

47 DSA, recital 4; Commission, 'Online Platforms and the Digital Single Market' (n 45) 4; Commission, 'Impact Assessment Digital Services Act' (n 32), points 70-71, 75-76; European Parliament, 'Improving the single market' (n 28), points 10, 12, 14.

## C. Notice and action in current law and practice

### I. Notice and action in the e-Commerce Directive and national law

- 25 Pursuant to Article 14 of the e-Commerce Directive, a hosting service provider can be held liable if it has actual knowledge of the illegal content and does not act expeditiously to remove or disable access to the information. However, the e-Commerce Directive does not clarify how the actual knowledge is supposed to be obtained. Although a notice and action mechanism is an important tool for gaining this knowledge, the e-Commerce Directive does not impose an obligation to facilitate or respond to notifications.<sup>48</sup>
- 26 This obligation is imposed for specific situations by other European rules (Section C. II.), but also generally by various (but not all) national laws and codes of conduct. The details of these national obligations vary from member state to member state.<sup>49</sup> 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.<sup>50</sup>
- 27 A notification can only lead actual knowledge if it sufficiently specific. Unless the hosting service is specifically designed to facilitate the dissemination of illegal content,<sup>51</sup> a provider cannot be held liable

for abstract knowledge that its service may be used for this purpose.<sup>52</sup> For this reason, a notification should contain a link to the illegal content.<sup>53</sup> In practice, this is usually facilitated by the notice and action mechanism (Section 3.3). If a single URL refers to a plurality of content, it might be necessary to provide more information. For example, a notifier should include a timestamp if the illegal content is included in a long (and otherwise permissible) video.<sup>54</sup>

- 28 Furthermore, the notification should trigger knowledge about *the illegal nature* of the content. In most member states, a hosting service provider can only be held liable if the illegal nature is sufficiently clear or ‘manifest’.<sup>55</sup> This approach prevents over-removal (Section B. II.), but also causes more illegal content to stay available. Furthermore, it allows hosting service providers to escape or delay their responsibilities by claiming that the illegality of certain content is unclear. In contrast, more recent provisions such as § 3(2) of the German NetzDG impose an obligation to remove any illegal content.<sup>56</sup> In any case, the notification should be adequately substantiated and provide information about why the content is illegal. It should allow a diligent

48 Commission, ‘Impact Assessment Digital Services Act’ (n 32), point 91.

49 Commission, ‘Impact Assessment Digital Services Act’ (n 32), points 93-99; Verbiest and others (n 29) 41-47; Kuczerawy (n 32) 530.

50 Verbiest and others (n 29) 14-15, 36, 42-46. See also Stalla-Bourdillon (n 39) 291. This requirement can also depend on the type of liability. 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. Dutch Criminal code, art 54a; Dutch Civil code, art 6:196c.

51 *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; 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), 38-39; Frosio and Mendis (n 14) 552.

52 Case C-324/09, *eBay* [2011] ECLI:EU:C:2011:474, para 122; Joined Cases C-682/18 and C-683/18 *Youtube* [2021] ECLI:EU:C:2021:503, para 111; Verbiest and others (n 29) 37; Van Hoboken and others (n 51) 38.

53 For example, see the French ‘Avia law’, Avia Law Loi no 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet, art 2(1).

54 Cf European Parliament, ‘Digital Services Act: adapting commercial and civil law rules for commercial entities operating online’ (Resolution) P9\_TA(2020)0273, Annex B, art 9(1)(a); Folkert Wilman, *The Responsibility of Online Intermediaries for Illegal User Content in the EU and the US* (Edward Elgar 2020) 301.

55 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 (n 29) 38-41; Stalla-Bourdillon (n 39) 290.

56 *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 15 September 2021. Note that uncertainty about the illegal nature does affect the period for the analysis of the permissibility. A provider has 24 hours for obviously illegal content, ‘*offensichtlich rechtswidrigen Inhalt*’, and seven days in other situations.

hosting service provider to realise that the content is illegal.<sup>57</sup> Although a notifier cannot be expected to provide a detailed legal clarification of the illegality, the notification should at least provide the necessary facts. For example, a notification about a copyright violation should clarify who owns the copyright and that no permission has been given.<sup>58</sup>

## II. Notice and action in other European rules

29 The e-Commerce Directive does not provide for a notice and action mechanism. However, due to its increasing popularity, this mechanism has been formally adopted in a number of relevant European instruments. Whereas some of these instrument are binding (Section C. II. 1.), others are not (Section C. II. 2.). This section provides a rapid overview of the most relevant instruments.

### 1. EU binding instruments

30 Since its 2018 revision, the EU's Audiovisual media services Directive (AVMSD),<sup>59</sup> contains specific obligations for so-called Video Sharing Platform services (VSPs).<sup>60</sup> VSPs must offer transparent and user-friendly mechanisms to allow users to report and flag content,<sup>61</sup> which includes a follow-up explanation on the manner in which the flagging has been internally handled.<sup>62</sup>

31 Next, Article 25 of Directive 2011/93/EU on combatting children sexual abuse and exploitation

57 Case C-324/09, *eBay* [2011] ECLI:EU:C:2011:474, para 122; Joined Cases C-682/18 and C-683/18 *Youtube* [2021] ECLI:EU:C:2021:503, para 115. See also *Verbiest and others* (n 29) 16; *Stalla-Bourdillon* (n 39) 291.

58 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.

59 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 (herein after AVMSD).

60 AVMSD, art 1(1aa).

61 AVMSD, art 28b(3)(d).

62 AVMSD, art 28b(3)(e).

(CSAED) obligates member states to take measures to remove or block access to websites that contain child sexual abuse material.<sup>63</sup> In order to comply with this obligation, various member states have implemented a notice and take down mechanism. This approach is based upon a network of organisations that serve as hotlines; the best known probably being INHOPE.<sup>64</sup>

32 Further, the recently adopted Copyright in the Digital Single Market Directive (CDSMD) provides for an advanced notice and take down mechanism known as notice and stay down. That is, so-called content-sharing service providers must not only take down illegal content, they must also make sure that such content cannot be re-uploaded after having been removed.<sup>65</sup>

### 2. EU non-binding instruments

33 In 2018 the European Commission adopted a Recommendation on Measures to Effectively Tackle Illegal Content Online ("Recommendation"). The latter builds upon the European Commission's 2017 Communication on Tackling Illegal Content Online, and is arguably a forerunner of the DSA. It contains a general notice and action mechanism that applies to all types illegal content and all hosting service providers.<sup>66</sup>

34 Several other soft-law instruments contain obligations that are more narrow in (either personal or material) scope. A so-called Code of Conduct on Countering Illegal Hate Speech online in the EU was adopted by some of the main platforms (e.g., Youtube, Microsoft, Facebook, Twitter) in 2016.<sup>67</sup>

63 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 (hereinafter CSAED), art 25(1),(2).

64 European 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 7.

65 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. (CDSMD), art 17(4).

66 See, Recommendation on measures to effectively tackle illegal content online (n 16), point 1 and Chapter II.

67 Hate speech is defined with reference to the EU's 2008

According to this Code, notified content is first assessed on the basis of the applicable terms and conditions and only then on basis of the relevant legal framework.<sup>68</sup>

- 35 Another soft-law instrument providing for a notice and action mechanism is the so-called Memorandum of Understanding on the sale counterfeit goods, meant to prevent the violation of intellectual property rights in the context of counterfeit goods. It was adopted in 2011 and revised in 2016.<sup>69</sup>
- 36 In 2018 and with the support of the European Commission, a number of stakeholders adopted the Product Safety Pledge. The goal of this initiative is to be able to better detect products sold online into the European Market and which do not comply with product safety requirements.<sup>70</sup> A notice and take down mechanism to allow users to flag unsafe products is one of the 12 commitments contained in the Pledge.<sup>71</sup>

### III. Notice and action in practice

- 37 Despite the legal fragmentation and the lack of a general European obligation to put a notice and action mechanism in place, (almost) all major online platforms<sup>72</sup> implemented a procedure to facilitate notifications.<sup>73</sup> Typically, these mechanisms allow a

---

Counter-Racism Framework Decision, which refers to: “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”, 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, art 1(a).

- 68 Code of Conduct on Countering Illegal Hate Speech Online (2016) 2.
- 69 Memorandum of understanding on the sale of counterfeit goods via the internet (2016), para 11-19.
- 70 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) 1.
- 71 Product Safety Pledge (n 68) 2.
- 72 Notice and action mechanisms are not common with other types of hosting services.
- 73 For a general description of these mechanisms, see eg Frosio and Mendis (n 14) 556; De Streele and others (n 26) 40, 46-51; Raphaël Gellert and Pieter Wolters, *The revision*

user to ‘flag’ illegal content by clicking a dedicated button and subsequently selecting the reason for the perceived illegality. The effectiveness of the mechanism depends on its accessibility (Section 2.1), which varies from platform to platform.<sup>74</sup> The platforms typically have specific channels or procedures for law enforcement agencies and other privileged or ‘trusted’ flaggers.

- 38 Although differences exist between the various platforms and types of illegal content, most platforms react relatively fast. They claim to usually remove terrorist-related content and child pornography with-in one hour and other illegal content within 24 hours of the notification.<sup>75</sup> Although most platforms do allow them to appeal against the removal of their online content through a ‘counter-notice’ procedure, the content providers are not always notified or given a clear explanation about the reasons for the removal.<sup>76</sup>

### D. Limitations

- 39 The current system of notice and action mechanisms is subject to various limitations and flaws, which affect each of the identified interests.

#### I. Limitation 1: lack of harmonization and preservation of the economic interests

- 40 A first limitation has been evidenced in Section C. The current framework is fragmented. There is no general European obligation to put a notice and action mechanism in place. The fragmentation is visible at various levels. The scope of the various mechanisms varies according to the member state, reason for the illegality and type of service. Furthermore, the mechanism’s content and requirements themselves vary greatly. There is a lack of consistency and uniformity between the various mechanisms.
- 41 Some have minimum quality requirements concerning the notices, this includes reasons to

---

*of the European framework for the liability and responsibilities of hosting service providers* (Report for the Dutch Ministry of Economic Affairs and Climate Policy, 2021) 27-28.

- 74 De Streele and others (n 26) 40, 48-49, 51.
- 75 See also De Streele and others (n 26) 44, 47, 49.
- 76 De Streele and others (n 26) 50; Gellert and Wolters (n 73) 28.

believe why the content is illegal or where it can be found,<sup>77</sup> others may make more general references to notices submitted in good faith.<sup>78</sup> Some mechanisms allow anonymous notices while others do not.<sup>79</sup> A few insist on the user-friendly nature of the mechanism,<sup>80</sup> while others also contain broader language on the efficient nature of the mechanism.<sup>81</sup> The time in which the service providers have to respond also differs from mechanism to mechanism. Some require action within 24 hours<sup>82</sup> or 5 working days,<sup>83</sup> while others simply refer to the lack of undue delay.<sup>84</sup> Whereas most notice and action mechanisms are strictly speaking notice and take down, some go a step further and are known as notice and stay down and require that the provider prevents the content from being uploaded again.<sup>85</sup>

- 42 Finally, one can also mention the specific systems of the Dutch Notice and Take Down Code of Conduct and of the NetzDG, which make specific distinctions not found in the other instruments discussed. The NetzDG distinguishes between manifestly and non-manifestly illegal content. The former must be removed within 24 hours and the latter within seven days.<sup>86</sup> The Dutch Code of Conduct differentiates between unequivocally lawful and not unequivocally unlawful content.<sup>87</sup>

77 Recommendation on measures to effectively tackle illegal content online (n 21) points 5-8; AVIA law, art 2; Gedragscode Notice-and-Take-Down 2018 inclusief addendum 1 <<https://noticeandakedowncode.nl/ntd-code/>> last accessed 14 July 2022, art 4.

78 Memorandum of understanding on the sale of counterfeit goods via the Internet (n 67) point 15.

79 AVIA law, art 2; Recommendation on measures to effectively tackle illegal content online (n 21) point 5; NetzDG, § 3(1).

80 AVMSD, art 28b(3)(i).

81 Memorandum of understanding on the sale of counterfeit goods via the Internet (n 67) point 13.

82 NetzDG, § 3(2); Code of Conduct on Countering Illegal Hate Speech Online (n 65) 2.

83 Product Safety Pledge (n 68) 2.

84 Memorandum of understanding on the sale of counterfeit goods via the Internet (n 67) point 18; Gedragscode Notice-and-Take-Down 2018 (n 82) explanatory memorandum.

85 CDSMD, art 17(4)(b)-(c); Product Safety Pledge (n 68) 2.

86 NetzDG, § 3(2).

87 Gedragscode Notice-and-Take-Down 2018 (n 82), art 5-6.

## II. Limitation 2: Lack of quality and protection of the victims

43 The observed discrepancies also point to a lack of consensus as to what constitutes a notice and action mechanism of sufficient quality as far as the protection of victims is concerned. The latter stems from the lack of clear requirements in the legal provisions, which are general at best. For instance the CDMSD refers to “sufficiently substantiated notice[s] from the rights holders”,<sup>88</sup> whereas the AVMSD requires that VSPs put in place a “transparent and user-friendly mechanism” for flagging content.<sup>89</sup> These general provisions do not guarantee that the mechanism is effective and efficient (Section B. I).

44 In practice a lot will thus depend upon the hosting service providers’ willingness and resources. The implemented mechanisms are not always sufficiently user-friendly, and suffer in particular from a lack of sufficient information about the processing of the notices.<sup>90</sup> At the other end of the spectrum, one can point to the Memorandum of Understanding for counterfeit goods, which has been interpreted as allowing for bulk notifications.<sup>91</sup> This might be user-friendly, but can also foster the submission of notifications that are not detailed enough to justify the removal of all notified content.<sup>92</sup> The lack of quality also affects the use of the existing notice and action mechanisms. A 2020 survey in the Netherlands has shown that one third of the people that have been affected by illegal content have used the notice and action mechanism. The survey has also shown that many people are unfamiliar with the mechanism and that potential users value (among other things) the accessibility, user-friendliness, speed and effectiveness of such a mechanism.<sup>93</sup> An increase of quality of and familiarity with the

88 CDSMD, art 17(4)(c).

89 AVMSD, art 28b(3)(d).

90 See, Gellert and Wolters (n 73) 63.

91 See, European 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 24.

92 Similar criticisms apply to the Code of Conduct on Countering Illegal Hate Speech, see De Streel and others (n 21) 49.

93 Van Hoboken and others (n 19) 55-57. About the use of such mechanisms in the United States, cf Jennifer M. Urban, Joe Karaganis and Brianna L. Schofield, *Notice and takedown in everyday practice. Version 2* (UC Berkely Public Law Research Paper No. 2755628) 2017.

mechanism could thus increase its use.

### III. Limitation 3: lack of adequate safeguards for fundamental rights

- 45 Beyond the fragmentation of the framework and the lack of agreement on what constitutes an adequate notice and action mechanism from the victims' perspective, additional questions pertain to the safeguards that should accompany such mechanisms. The issue of safeguards exemplifies the way in which the three interests at stake are interwoven: adequate safeguards often entail more resources and have thus a bearing on the economic interests. Also, content providers are not the only ones who should benefit from such safeguards: victims are also entitled to a fair decision-making process. With that being said, the focus of this section is on the content providers.
- 46 Content providers frequently lack any guarantee that removal decisions are well-balanced, non-discriminatory, consistent, and more generally, fair (Section B. II.). Furthermore, in case they think a decision does not live up to these standards, they lack effective possibilities to challenge a notification or to contest decisions (typically, the removal of content) based on a notification.<sup>94</sup> Such possibilities ensure the protection of the third interest at play, namely that of the other users (and in particular content providers) by safeguarding their fundamental rights such as the right to a fair hearing, the right to equality of arms, or the right to adversarial proceedings.<sup>95</sup> Despite the importance of these possibilities, the AVMSD and the CDSMD are the two only binding European instruments that provide for them. However, both instruments limit themselves to general language without entering into the specifics of what such a mechanism should look like.<sup>96</sup> They therefore do not guarantee an effective protection.
- 47 Crucial to challenging decisions is the possibility to receive a motivation of the decision upon which a contestation of the decision can build (Section B. II.). However, as seen in section C. III. , the content providers are not always notified or given a clear explanation about the reasons for the removal.

94 Commission, 'Impact Assessment Digital Services Act' (n 27) 26; Kuczerawy (n 27) 535.

95 Kuczerawy (n 27) 535.

96 See, CDSMD, art 17(9), AVMSD art 28b(3)(i).

## E. The notice and action mechanism in the DSA

- 48 The DSA harmonises, codifies and develops the notice and action mechanism. It provides that all hosting service providers should put a notice and action mechanism in place (Article 16). The goal of this section is to see whether the notice and action mechanism in the DSA sufficiently addresses the needs of the three discussed interests, and in so doing addresses the identified limitations.

### I. The protection of the victims of illegal content

- 49 Articles 16 DSA contains harmonized requirements on the effectiveness and efficiency of the notice and action mechanism (see Section B. I.). The mechanisms must be user-friendly and easy to access, which entails among others that they should allow for exclusively electronic notices.<sup>97</sup> Notices submitted in accordance with the prescriptions of the DSA will lead to a presumption of knowledge of the illegality of the content. Although this does not directly obligate the hosting service providers to remove the content, they may face liability if they don't.<sup>98</sup> Hosting service providers must facilitate the submission of valid notices,<sup>99</sup> and must process the notices they receive in a timely, diligent, non-arbitrary, and objective manner.<sup>100</sup> They should also notify the notifier without undue delay of the receipt of and their decision on the notice.<sup>101</sup> These requirements go a long way in resolving limitation 2 (Section D. II.). By providing clear and detailed requirements, hosting service providers are obligated to ensure that their notice and action mechanism is adequate.

- 50 If the provider of an *online platform* decides not to

97 DSA, art 16(1).

98 DSA, art 16(3). An obligation to remove illegal content is imposed indirectly and implicitly through the obligation to apply and enforce their terms and conditions in a diligent, objective and proportionate manner and the obligation of the providers of very large online platforms to take measures to mitigate the risks of the dissemination of illegal content. DSA, arts 14(4), 34(1)(a), 28; P.T.J. Wolters, 'Privaatrechtelijke en consumentrechtelijke bescherming in het DSA-voorstel' [2022] TvC 18, 22.

99 DSA, art 16(2).

100 DSA, art 16(6).

101 DSA, art 16(4), (5).

remove the notified content, article 20 DSA grants the victim the right to lodge a complaint in the internal complaint-handling system of this platform. If this complaint is dismissed, it can take the dispute to a certified out-of-court dispute settlement body pursuant to article 21(1). The DSA thus follows the General approach of the Council. The notifier did not have these redress possibilities under the original DSA proposal.<sup>102</sup> We support this extended scope. After all, it would be an unfair limitation on the protection of the victims if they aren't able to contest a negative decision on their notice, especially in cases where they might not have enough resources to pursue the only other possible option, namely court proceedings. These redress possibilities and their limitation to online platforms are further discussed in Section E. II.

- 51 The DSA has also sought to ensure that potential victims would not abuse the notice and action mechanism. Article 16(3) states that 'notices referred to in this article' give rise to actual knowledge. Article 16(2) requires that the mechanism facilitates the submission of notices that contain 'all of the following elements', including the name and email address of the notifier. Furthermore, recital 53 states that the notice and action mechanism *should* ask the notifier to disclose its identity in order to avoid misuse. In contrast, recital 50 states that the mechanism should allow, but not require, the identification of the notifier. The DSA is thus unclear about the existence of a requirement that valid notices not be anonymous (except for cases of children sexual abuse material).<sup>103</sup> In this respect, the DSA may not adequately protect the interests of the victims. Non-anonymous notices can jeopardise online anonymity and may prevent victims from submitting notices out of fear of retaliation.<sup>104</sup> For this reason, requiring non-anonymous notices should be avoided as much as possible, except where unfeasible (e.g., alleging copyrights violations might require identification).<sup>105</sup>
- 52 Article 23(2) DSA contains additional measures against misuse of the notice and action system. However, rather than making the notice submission more cumbersome, these additional measures are

<sup>102</sup> Cf DSA proposal, art 17, 18; General approach, art 17, 18.

<sup>103</sup> Note that the DSA proposal was more explicit about this requirement by specifically referring to the elements of Article 14(2) in Article 14(3).

<sup>104</sup> Section 2.1. On the value of anonymity online, see, e.g., A Michael Froomkin, 'From Anonymity to Identification' (2015) 01 *Journal of Self-Regulation and Regulation* 120.

<sup>105</sup> On this point, see European Parliament, 'Adopting commercial and civil law rules', Annex B, art 9(1)(e).

of an *ex post* nature as they entail an obligation to suspend for a reasonable period of time the processing of notices and complaints from notifiers who frequently submit notices and complaints that are manifestly unfounded. This *ex post* nature is to be favoured. It provides safeguards for fundamental rights without limiting the effectiveness and efficiency of the notice and action mechanism and thus the protection of victims of illegal content.

- 53 However, it is important to make sure that these *ex post* measures can be applied relatively fast. In this light, the conditions of Article 23(2) DSA may be too strict. The processing of the notices can only be suspended if the notifier 'frequently' submits notices that are 'manifestly' unfounded and only after a prior warning. This suggests a high threshold. A prior warning should not be necessary if the notifier crosses this threshold and clearly acts in bad faith, especially because the suspension can only be 'for a reasonable period of time'. In this regard one should note that the DSA does not explicitly allow online platforms to determine a lower threshold compared to Article 23(2) via their terms and conditions.<sup>106</sup> Article 16(6) obligates the platforms to process 'any notices that they receive'. This implies that restrictions that go beyond Article 23(2) are not allowed.
- 54 Anonymous notices can further complicate the application of Article 23(2). However, even if a service provider does not know the (real) name and email address of the notifier, it may still be able to distinguish various notifiers through pseudonyms, IP-addresses or cookies. For this reason, we believe that the additional protection of victims of illegal content outweighs the additional risks of abuse, especially because the DSA also contains other safeguards for the fundamental rights of the (other) users.

## II. Safeguarding fundamental rights

- 55 Various provisions of the DSA make sure that the notice and action mechanism does not disproportionately encroach on fundamental rights. First, a notice only leads to actual knowledge, and thus potentially to liability, if it is sufficiently substantiated, precise and allows a diligent provider to identify the illegality without a detailed legal examination. Under this rule, a provider cannot be held liable if the illegality is uncertain,<sup>107</sup> the

<sup>106</sup> See, DSA, art 14(1). Cf DSA, art 23(1), recital 64, which allows online platforms to establish stricter measures in relation to the removal of illegal content.

<sup>107</sup> Either because the facts or the law is unclear, cf Gellert and

- hope being that hosting service providers will have less incentives to precautionarily remove content (see Section B. II.). As far as the quality of the decisions themselves are concerned we can also point to Article 16(6) DSA, which requires that decisions be taken in a diligent, non-arbitrary, and objective manner (Section E. I.). These safeguards also apply to the automated moderation of content. However, the exact meaning of these safeguards for automated moderation remain unclear. It may be necessary to formulate more specific requirements. For example, the General Data Protection Regulation and the proposed AI Act require specific safeguards in relation to possible errors and bias of automated means.<sup>108</sup> In contrast, Article 16(6) DSA only provides that a hosting service provider should inform the notifier of the use of automated means.
- 56** Next, Article 17 of the DSA provides for transparency with regards to decisions to remove or disable content. Hosting service providers shall inform content providers of a decision to demonetise or restrict the visibility of their content or to suspend or terminate the provision of the service or account. They must also provide the content providers with a clear and specific statement of reasons.<sup>109</sup> This requires to indicate the type of decision, the legal ground relied upon (or the Terms and Conditions provision), as well as the facts and circumstances supporting it (and the redress possibilities).<sup>110</sup>
- 57** It should not be construed as exceedingly affecting the economic interests of the hosting services providers since Article 17(4) DSA clarifies that it should be “as precise and specific as reasonably possible under the given circumstances”. We believe that general statement about the reason for the removal would comply with such an obligation. A hosting service provider should make clear which rule is violated by the content, but is not obligated to provide a detailed analysis.
- 58** In contrast, the DSA does not explicitly state that the hosting service provider should provide a statement of reasons to the notifier. It is only obligated to inform the notifier of the decision and redress possibilities (Section E. I.). This distinction is not justified. Like content providers, notifiers require a statement of reasons to understand the decision and to effectively exercise their redress possibilities. In this light, the lack of an explicit obligation in relation to the notifiers is a missed opportunity to strengthen judicial oversight and protect the victims of illegal content (Section B. II.) and fully address this limitation in current practice (Section D. III.).<sup>111</sup>
- 59** The DSA also devotes considerable attention to the redress possibilities of both the content provider and the notifier. It provides both for an internal complaint-handling mechanism and an out-of-court dispute settlement mechanism.<sup>112</sup>
- 60** Article 20 of the DSA is dedicated to the internal complaint-handling mechanism. As a fundamental rights safeguard it should provide content providers with adequate guarantees,<sup>113</sup> even though one cannot hold it to the same standards (e.g., independence, impartiality) as a regular court.<sup>114</sup> In this regard, the DSA refers to a free complaint-handling mechanism, which should be effective, ‘easy to access, user-friendly’, and should ‘enable’ and ‘facilitate’ the submission of ‘sufficiently precise and adequately substantiated’ complaints.<sup>115</sup> The complaints should also be processed in a ‘diligent, non-discriminatory, and non-arbitrary’ manner.<sup>116</sup> Finally, the decision must be taken under the control of appropriately qualified staff pursuant to Article 20(6) DSA. Unlike the initial decision on the notice (Article 16(6) DSA), it cannot be made solely on the basis of automated means.
- 61** The internal-complaint handling mechanism is limited to online platforms. This can be seen as an undue limitation on safeguarding the fundamental rights. After all, there is a case to be made that the internal complaint-handling mechanism
- 
- Wolters (n 73) 28-30.
- <sup>108</sup> 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, art 22(2)(b), (3); Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (WP251rev.01, 2018) 27; Commission, ‘Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts’ COM(2021) 206 final, 2, 11, recitals 33, 40, 44, 50, arts 10(2)(f), 15(3).
- <sup>109</sup> DSA, art 17(1).
- <sup>110</sup> DSA compromise, art 17(3)(a), (b), (d), (e), (f).
- <sup>111</sup> On this topic, see also Naomi Appelman and others, ‘Access to Digital Justice: In Search of an Effective Remedy for Removing Unlawful Online Content’ (2021) *Amsterdam Law School Legal Studies Research Paper No. 2021-35*, *Institute for Information Law Research Paper No. 2021-06*.
- <sup>112</sup> DSA, arts 20, 21.
- <sup>113</sup> See, Wilman (n 54) 373-374.
- <sup>114</sup> Wilman (n 54) 371.
- <sup>115</sup> DSA, art 20(1), (3).
- <sup>116</sup> DSA, art 17(4).

should be available to all users, as many relevant situations take place outside of online platforms. For example, a website offering legal content may be a victim of overzealous intellectual property-based notifications.<sup>117</sup>

- 62 Such an extension of the internal complaint-handling mechanism's scope might however be overly burdensome for the hosting service providers. However, this depends upon the way in which such mechanism is conceived. On the basis of the DSA provisions, this mechanism can take many shapes, but nothing says that all internal complaint-handling mechanisms should look like a court proceeding.<sup>118</sup> An alternative solution would be one that is closer in spirit to *ex post* counter notices,<sup>119</sup> in which the content providers have an opportunity to explain why the content is not illegal and have their content restored. Modelling the internal complaint mechanism on counter notices and essentially making the submission of complaints a similar procedure as the submission of notices could go a long way in addressing some of the concerns relating to the economic interests of hosting service providers. Furthermore, it could also facilitate rapid response times in order to avoid situations where content is rapidly deleted but only slowly reinstated. Article 17(3) of the DSA refers to 'timely' responses. Stronger language such as 'without undue delay' might be more useful, without going so far as giving strict deadlines such as the European Parliament's position which allocates 10 working days to reply to such a complaint.<sup>120</sup>
- 63 The out-of-court dispute settlement provided in the DSA strives to provide adequate safeguards for the fundamental rights of the content providers by allowing notifiers and content providers to take a dispute to the certified out-of-court dispute

settlement body of their choice.<sup>121</sup> The DSA further provides safeguards by imposing requirements in terms of impartiality and independence,<sup>122</sup> expertise,<sup>123</sup> online accessibility,<sup>124</sup> and procedural fairness.<sup>125</sup>

- 64 A couple of potential limitations on the safeguarding of fundamental rights and caveats can be highlighted here. Similar to the internal complaint-handling mechanism, out-of-court dispute settlement only applies to online platforms. However, here too there are many relevant situations outside of online platforms: many victims or interested parties in the context of 'regular' hosting service providers may also not have the sufficient resources concerning court proceedings (e.g., victim of online children sexual abuse and exploitation material, or a website offering legal content).
- 65 Contrary to the internal complaint-handling mechanism, the DSA does not require that the out-of-court dispute settlement be fully paid by the service provider. Here, one must observe that the system in the adopted DSA is much more friendly to the user (the notifier or content provider) than previous iterations. The DSA proposal was not entirely clear on the requirements of the fees. It merely stated that such fees could not exceed the costs.<sup>126</sup> The DSA distinguishes between the fees charged to online platform providers (which should be reasonable and not exceed the costs) and the fees charged to users (which should be either inexistent or nominal and should be refunded by the online platform provider if the dispute is decided in their favour).<sup>127</sup> This system seems to strike an adequate balance between the various interests at stake. A limited fee can prevent frivolous use of the mechanism and thus protect the economic interests of the service providers without unduly limiting independent oversight and thus the protection of the victims and fundamental rights.

117 On this topic, see for instance, Jason Mazzone, *Copyfraud and Other Abuses of Intellectual Property* (Stanford University Press 2011).

118 Cf Meta's Oversight Board, <<https://www.oversightboard.com/>>, last accessed 14 July 2022.

119 About counter notices and their limitations, see eg Commission, 'Impact Assessment Digital Services Act' (n 32) 26; 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* 280; Wilman (n 54) 370-374; Kuczerawy (n 32) 531-532, 535, De Streel and others (n 26) 49.

120 Amendment 227.

121 DSA, art 21(1).

122 DSA, art 21(3)(a), (c). But see also 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), art 22(2), for additional requirements.

123 DSA, art 21(3)(b).

124 DSA compromise, art 21(3)(d). The information about the mechanism should also be accessible online, see DSA compromise, art 21(1).

125 DSA compromise, art 21(3)(f).

126 DSA proposal, art 18(3).

127 DSA, art 18(5).

66 Finally, contrary to the original DSA proposal which only referred to a ‘swift, efficient, and cost-effective’ procedure,<sup>128</sup> the adopted DSA has supplemented this general formulation with more concrete timelines.<sup>129</sup> Namely, a decision should be taken within a reasonable period of time that does not exceed 90 days (or 180 days for the more complex cases). This text builds upon the European Parliament’s position.<sup>130</sup>

### III. The economic interests of hosting service providers

67 Article 16 DSA imposes a harmonised notice and action mechanism on all hosting service providers that applies to all types of content. Although some obligations to implement notice and action mechanisms already exist (Sections C. I. and C. II.), the DSA certainly increases the obligations of the hosting service providers. Furthermore, the requirements in terms of effectiveness and efficiency (Section E. I.) and the redress possibilities and safeguards for fundamental rights (Section E. II.) can impose significant costs. In this light, the DSA represents a new balance between the various interests. The economic interests of the providers of hosting services have been limited in favour of the protection of victims and fundamental rights.

68 It is noteworthy that the DSA does not exempt micro and small enterprises from the obligation to implement a notice and action mechanism.<sup>131</sup> This is justified, since the dissemination of illegal content through small hosting services can also have a significant adverse effect on victims.<sup>132</sup> Micro and small enterprises are exempted from the additional obligations for providers of online platforms pursuant to Article 19 DSA. The DSA does distinguish between online platforms and other hosting services. Articles 20, 21 and 23 DSA only apply to online platforms. In contrast, the notice and action mechanism applies to all hosting service providers. The reason for this inconsistency is not necessarily justified (Section E. II.). Recital 41 DSA merely states in general terms that the obligations should be adapted to the type and nature of the intermediary service. In any case, the additional obligations for online platforms lead to a better protection of both the victims of illegal

content and fundamental rights at the expense of the economic interests of the providers of online platforms.

69 At the same time, the new provisions do not completely ignore the economic interests of the service providers. First, the harmonised nature allows them to implement one mechanism throughout Europe. However, the lack of harmonisation (Limitation 1, Section D. I.) is only partially resolved by the DSA since the more specific rules in vertical instruments still apply (and can force hosting service providers to implement special procedures).<sup>133</sup>

70 Second, the rules in relation to the use of automated means for the processing of notices also balance the economic interests of the hosting service providers with the other involved interests. Hosting service providers are allowed to process notices automatically pursuant to Article 16(6) DSA. Similarly, the limitation of the statement of reasons to what is reasonable also facilitates automated and standardised motivations. In contrast, decisions in respect to the internal complaint-handling system cannot be made solely on the basis of automated means (Section E. II.).

71 Third, the DSA contains a number of provisions against abuses, specifically directed at online platforms. Article 23(2) allows them to refuse to process notices or complaints insofar as they are manifestly unfounded and originate from the same user who submits them frequently. This can reduce the economic burden of processing these unfounded notices and complaints. However, the high threshold of this provision (Section E. I.) means that online platforms can only benefit from it in limited cases. Furthermore, Article 23(2) does not apply to micro and small online platforms or other hosting services, which would force them to keep processing these notices pursuant to Article 16(6). Obviously, this goes against the intention of the DSA, which is to limit the obligations of micro and small online platforms and other hosting services. We therefore argue that these service providers can also suspend the processing of manifestly unfounded notices if the conditions of Article 23(2) DSA apply.

72 Further, and in relation to out-of-court dispute settlement, the adopted DSA added a new provision against abusive procedures which allows online platforms providers to refuse to engage in proceedings if the issue has already been previously resolved.<sup>134</sup> Also, the online platforms are entitled to a reimbursement of their fees if the notifier or content provider acted manifestly in bad faith

128 DSA proposal, art 18(2)(d).

129 The general formulation is still kept, see DSA, art 18(3)(e).

130 Amendment 240.

131 Cf DSA, arts 12(4), 19.

132 Gellert and Wolters (n 73) 95-96.

133 DSA proposal 4-5, 9; DSA, art 2(4).

134 DSA, art 21(2).

pursuant to Article 21(5) DSA.

- 73 Next, a notice only leads to actual knowledge, and thus potentially to liability, if it is sufficiently substantiated and precise, and allows a diligent provider to identify the illegality without a detailed legal examination (Section E. II.). Although the exact requirements of a ‘diligent’ provider will still need to be ironed out, it is clear that this provision limits the liability risks of the providers.
- 74 Finally, the provisions on the notice and action mechanism contain open-ended norms. They refer to a ‘diligent’ provider,<sup>135</sup> demand ‘timely’ action<sup>136</sup> as well as ‘good faith’ engagement<sup>137</sup> and limit the statement of reasons to what is ‘reasonably’ possible.<sup>138</sup> These open-ended norms make sure that the economic interests of the hosting service providers can also be taken into account when interpreting the various obligations. It allows for differentiation based on the size of the service provider. In addition to the explicit exemptions and additional obligations, the open-ended norms allow for stricter demands on large hosting service providers and less stringent requirements on smaller providers.<sup>139</sup> For example, it could affect the requirements in relation to the diligence, non-arbitrariness and objectiveness of the automated means that are used to process notices.<sup>140</sup>

## F. Conclusions

- 75 The adoption of the DSA will bring important changes to the content moderation landscape in the EU. By harmonising, codifying, and further developing a notice and action mechanism, the DSA addresses many content moderation-related challenges, and in so doing also affects the balance that existed thus far between the protection of victims of illegal content, the safeguarding of fundamental rights and the economic interests of hosting service providers.
- 76 As far as the economic interests of hosting service providers are concerned (Section B. III.), the harmonisation of the mechanism should certainly be a welcome change for economic operators

<sup>135</sup> DSA, arts 16(3), (6), 17(4), 23(3)

<sup>136</sup> DSA, arts 16(6), 20(4), 23(3).

<sup>137</sup> DSA, art 21(2).

<sup>138</sup> DSA, art 17(4); Section 5.2.

<sup>139</sup> See also Gellert and Wolters (n 73) 97.

<sup>140</sup> DSA, art 16(6).

(Section D. I.). Further, even though the DSA contains many new procedural obligations, they entail reasonable efforts (Section E. III.). One can point to the limitation of the statement of reasons to what is reasonable or the possibility to use automated tools. By stating that a notice only gives rise to ‘actual knowledge’ if it allows a diligent operator to identify the illegality, the DSA limits the operators’ liability and also contributes to the safeguarding of fundamental rights since it limits overcautious removals of content. Finally, the DSA also contains provisions against abusive notices and complaints. However, the high threshold of Article 23(2) limits its effectiveness. Interestingly, this provision does not help small and micro online platforms and other hosting service providers (Section E. III.). This is paradoxical since the economic interests also explain why these actors fall outside of the scope of the redress mechanisms. Whereas limiting the costs that these new fundamental rights safeguards can entail is a legitimate goal, we have also shown that there is a real fundamental rights interest to extend these mechanisms to all hosting service providers. We have also shown that this is possible and feasible depending upon the manner in which these mechanisms are conceived (Section E. II.).

- 77 Beyond excluding certain economic operators from redress mechanisms, the DSA also refuses notifiers the possibility to receive a statement of reasons for a (negative) decision taken pursuant to their notice. Whereas the adopted DSA can be seen as an improvement concerning notifiers’ right compared to the DSA proposal (they can now also benefit from the redress mechanisms), we consider the lack of an obligation to provide a statement of reasons as a missed opportunity. Furthermore, one can still lament the unclarity about the effect of anonymous notifications. Beyond that however, the requirement of a harmonised, efficient, effective, and user-friendly notification procedures should fix the existing limitations (Section D. II.) and can be seen as an important step for the protection of the victims’ interest (Sections B. I. and E. I.).
- 78 Finally, the safeguards of content providers’ fundamental rights are also enhanced (Sections B. II. and E. II.). Not only through the creation of new redress mechanisms, but also through the hosting provider services’ obligation to provide decisions that are objective, non-arbitrary, diligent and timely, and to justify them through a statement of reasons. Although the applicability of the safeguards is still too narrow in some respects, the new safeguards and their requirements should improve the current situation in which hardly any binding legal provisions exist (Section D. III.).
- 79 All in all, even though it contains various shortcomings that prevent it from truly striking

an adequate balance, the DSA's notice and action mechanism does represent a significant step forward for all the parties that have a stake in the moderation of online content.