The EU's system of knowledge-based liability for hosting service providers in respect of illegal user content – between the e-Commerce Directive and the Digital Services Act

by **Folkert Wilman***

Abstract: Over the past two decades the principle of knowledge-based liability has been the backbone of the EU's regime regulating the liability of social media companies, online marketplaces, cloud storage providers and many other online service providers that store and disseminate user-generated content. This article traces the origins, identifies the rationale, assesses the continued relevance and discusses the main strengths and shortcomings of this approach. It is argued that, counter-intuitive as it may seem to some, there are good grounds for retaining the key features of the current liability system, which conditionally shields such service providers from liability for their users' content. Most important is the system's ability to strike a fair balance between the conflicting rights and interests of the parties involved – not only the service providers and the users, but also the parties aggrieved by the content. That is not to say, however, that the system has no shortcomings. In particular, it is shown that the system's effectiveness in terms of tackling illegal user content causing serious 'public' harm could be improved, whilst the system also involves significant risks of unjustified removal of user content. These shortcomings do not mean that the current knowledge-based liability system should be disgcarded, however. Instead, it should be improved. Not by excluding certain service providers from the scope of the liability exemption or adding conditions, but rather by enacting complementary requirements. Against this background the article assesses to which what extent the recently proposed Digital Services Act addresses the identified shortcomings.

Keywords: intermediary liability; hosting service providers; notice and action; e-Commerce Directive; Digital Services Act (DSA)

Recommended citation: Folkert Wilman, The EU's system of knowledge-based liability, 12 (2021) JIPITEC 317 para 1

A. Introduction

1 If somebody came up today with the idea of laying down in law a provision exempting online service providers such as Facebook, YouTube and Twitter from liability for the user content that they store and disseminate, the idea would likely not be well received. These online giants are subject to increasingly critical public and political scrutiny, both in the European Union (EU) and the United States (US). The controversy surrounding the decisions by Twitter and Facebook to suspend (then) US President Trump's account for inciting violence in early 2021[1]

* Member of the Legal Service of the European Commission. The views expressed in this article are personal and cannot be attributed to the author's employer. The article is in part based on research carried out for the author's recent book: F Wilman, *The responsibility of online intermediaries for illegal user content in the EU and the US* (Edward Elgar 2020). All online sources cited were last visited on 13 June 2020. The author thanks Irene Roche Laguna and Miquel Peguera Poch for their

is only the latest example of a long-standing and broader debate about the responsibilities of such service providers. The criticism mostly turns around the perception that users, competitors and society at large are not sufficiently protected against the downsides of their ways of doing business and the power they exercise – not that the service providers themselves need protection. Yet, in both the EU and the US, there are rules in place that do precisely that: protecting the service providers concerned. For over two decades now, in both jurisdictions laws ensure that they are exempted from liability relating to the content that they store for their users, provided they do not have knowledge of the content's illegality and act expeditiously to remove the content once they obtain such knowledge. In the EU, the rule applies to all kinds of illegal content and has been laid down in Article 14 of the e-Commerce Directive (ECD), adopted in 2000.[2] The rule was inspired by a comparable rule of US law applicable specifically in relation to copyright-infringing user content, laid down in Section 512(c) of the 1998 Digital Millennium Copyright Act (DMCA).[3]

2 What is more, in its proposal for a new Digital Services Act[4] (DSA), tabled in December 2020, the European Commission ('the Commission') suggests leaving the aforementioned rule essentially unaltered. It stated that the current liability regime is "*by now established as a foundation of the digital economy*".[5] As will be seen below, whilst the DSA proposal provides for a range of new measures, it largely reproduces Article 14 ECD.[6] That implies that the basic principle would remain that of knowledge-based liability. Indeed, it appears that the Commission never even seriously questioned the continued validity of the principle; an in-depth analysis of its pros and cons is not provided for.[7] In the US, the laws in question are under review, too. A study of Section 512 DMCA by the US Copyright Office was critical on several points, but recommended some fine-tuning rather than any wholesale change.[8] But it is the second cornerstone of US liability law applicable to online service providers – Section 230 of the Communication Decency Act (CDA),[9] adopted in 1996 – that tends to be criticised most broadly and strongly.[10] This law unconditionally exempts such providers from most

comments on earlier drafts of the article.

1 See <https://blog.twitter.com/en_us/topics/company/2020/suspension.html>; <https://www.facebook.com/zuck/posts/10112681480907401> (announcing and explaining the decisions of Twitter and Facebook, respectively). More recently, see also <https://about.fb.com/news/2021/06/facebook-response-to-oversight-board-recommendations-trump/>.

2 Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the internal market, [2000] OJ L 178/1 ('ECD').

3 17 USC Section 512. Although Section 512(c) DMCA was not the sole source of inspiration for Article 14 ECD, it is widely believed to have played an important role, as is also evident from the similar wording. See eg M Husovec, 'How Europe wants to redefine global online copyright enforcement', in T Synodinou (ed), *Pluralism or universalism in international copyright law* (Kluwer Law International 2019), 514; P Przemyslaw Polanski, 'Rethinking the notion of hosting in the aftermath of Delfi: shifting from liability to responsibility?', (2018) *Computer Law and Security Review* 34, 871; J Urban, J Karaganis and B Schofield, 'Notice and takedown in everyday practice', UC Berkeley Public Law Research Paper No 2755628 2017, 22; P Van Eecke, 'Online service providers and liability: a plea for a balanced approach', (2011) *Common Market Law Review* 48, 1456.

4 Commission, Proposal for a Regulation on a single market for digital services (Digital Services Act), COM(2020) 825 ('DSA proposal').

5 Commission, Explanatory memorandum DSA proposal, COM(2020) 825, 3.

6 See further section H below.

7 See eg the inception impact assessment relating to the DSA proposal, available via <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12417-Digital-Services-Act-deepening-the-Internal-Market-and-clarifying-responsibilities-for-digital-services> (indicating that, whilst certain adjustments might be necessary, "*the underpinning basis is as valid today as it has been 20 years ago*"). See also Commission, Impact assessment DSA proposal, SWD(2020) 348, 150 ("*the logic behind the liability regime remains valid today. [...] Hence, any update of the existing rules needs to bear in mind that the main principle of non-liability for third party content remains*").

8 US Copyright Office, 'Section 512 of Title 17: a report of the register of copyrights', 2020, 7. See also the draft bill for the Digital Copyright Act 2021, available via <https://www.tillis.senate.gov/services/files/97A73ED6-EBDF-4206-ADEB-6A745015C14B> (suggesting more substantial changes, in particular a partial staydown obligation to complement the knowledge-based liability system).

9 47 USC Section 230.

10 Critics include both former President Trump and current President Biden. President Biden (when not yet elected) called for the repeal of Section 230 CDA; see *New York Times*, 'Joe Biden, former vice president of the United States', 17 January 2020. Former President Trump and his administration (when still in office) criticised the law on several occasions. See in particular Executive Order 13925, 'Preventing Online Censorship', 85 FR 34079, 2020 (attempting to limit the law's scope of application; since revoked).

forms of liability for user content.[11] That means that – unlike under Article 14 ECD and Section 512(c) DMCA – the liability exemption is available also where the providers had been notified and nonetheless decided not to act against illegal content.[12] For now, it is uncertain whether, when and how Section 230 CDA will be reformed. It may be widely criticised, but this is done on different grounds.[13] Still, a common suggestion is to align the law with Section 512(c) DMCA and thus to make knowledge-based liability the basic principle.[14]

3 It thus appears that the principle of knowledge-based liability for online service providers in respect of the content that they store for their users is – and in all likelihood will continue to be – a key component of the liability regimes of both the EU and the US. Already for this reason it is important to properly understand this approach and especially its main strengths and shortcomings. That holds true all the more so precisely because in both jurisdictions the relevant regimes are now under review and additional measures are being considered. Given that such possible additional measures are generally not meant to *replace*, but rather to come *on top of* the current rules, the former should be designed to build on the latter's strengths and address their shortcomings. In other words, when new proposals are tabled it may be tempting to jump straight to the novel parts, such as the diligence obligations or reinforced enforcement powers set out in the DSA proposal. Yet in many respects those parts cannot properly function – and cannot be properly understood – without having regard to the foundation that the principle of knowledge-based liability provides. Developments in this field are often said to entail an evolution 'from liability to responsibility'.[15] Noteworthy as that evolution may be, a more accurate description might be 'liability *and* responsibility'.[16] The latter complements but does not replace the former.

4 That being so, this article aims to assess the continued relevance and identify the main strengths and shortcomings of the principle of knowledge-based liability as applied in the context of efforts aimed at tackling illegal content that online service providers store and often disseminate for their users. That also requires tracing the principle's origins and identifying its rationale. In doing so, the article seeks to contribute to the understanding, and allowing for the assessment, of EU law developments in this regard – most notably, the transition from the system currently laid down in Article 14 ECD to the one to be contained in the DSA. While this article accordingly mainly focuses on EU law, an account is also taken of developments in the US. That is done for several reasons. First, the US is the country where the knowledge-based liability model, as codified in law and applied in this particular context, originates. Second, many large online service providers active in the EU originate and continue to be based in the US. Their behaviour is therefore shaped by the country's legal set-up.[17] Third, in the US much experience has been gained in applying the model in practice, which offers valuable insights also for the EU's efforts to update it legal framework.

11 Section 230 CDA does not cover liability under intellectual property law. It also contains certain other exclusions, most notably in respect of liability under Federal criminal law. See Section 230(e) CDA.

12 See eg US Court of Appeals DC Circuit, *Marshall's Locksmith Service v Google*, 925 F3d 1263 (2019); US Court of Appeals 1st Circuit, *Universal Communications Systems v Lycos*, 478 F3d 413 (2007); US Court of Appeals 4th Circuit, *Zeran v America Online*, 129 F3d 327 (1997).

13 In as far as criticism by politicians is concerned, Democrats tend to criticise Section 230 CDA for being overly protective of large online service providers, whereas Republicans tend to criticise it for disadvantaging conservative viewpoints. See further F Wilman, *The responsibility of online intermediaries for illegal user content in the EU and the US* (Edward Elgar 2020), 119-130 (giving an overview of opinions of stakeholders, academics and courts on Section 230 CDA).

14 See eg J Balkin, 'Free speech is a triangle', (2018) *Columbia Law Review 118*, 2046; M Roter, 'With great power comes great responsibility: imposing a "duty to take down" terrorist incitement on social media, (2017) *Hofstra Law Review* 45, 1404; O Medenica and K Wahab, 'Does liability enhance credibility: lessons from the DMCA applies to online defamation', (2007) *Cardozo Arts and Entertainment Law Journal* 25, 265-267. Similar suggestions have occasionally been made in the case law; see eg US Court of Appeals 9th Circuit, *Batzel v Smith*, 33 F3d 1018 (2003). See also the US Senate bill with a proposal to reform Section 230 CDA that was put forward in June 2020: 'Platform Accountability and Consumer Transparency Act' (PACT Act), available via <https://www.schatz.senate.gov/imo/media/doc/OLL20612.pdf>.

15 Eg A Kuczerawy, 'General monitoring obligations: a new cornerstone of Internet regulation in the EU?', 2019, available via <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3449170>, 1; Przemyslaw Polanski (n 3); G Frosio, 'Why keep a dog and bark yourself? From intermediary liability to responsibility', (2018) *Oxford International Journal of Law and Information Technology* 26, 1–33.

16 Cf A Savin, 'The EU Digital Services Act: towards a more responsible internet', Copenhagen Business School Law Research Paper Series No. 21-04, 2021, 5 (speaking of "*a double-edged regime of liability*").

17 Cf L Klonick, 'The New Governors: the people, rules, and process governing online speech', (2018) *Harvard Law Review* 131, 1598–1670.

5 The remainder of this article is structured as follows. First a brief overview is given of the EU's legal framework, in particular the liability exemption for hosting service providers as currently laid down in Article 14 ECD (section B). Next, the rationale of the knowledge-based liability model is explained (section C). Attention then turns to the developments – both in practice and in law – that have taken place since the principle of knowledge-based liability was enshrined in EU law about two decades ago (sections D and E). The following two sections focus on the shortcomings associated with this regime. A distinction is made between shortcomings relating to the aim of tackling illegal user content on the one hand and those relating to the protection of users on the other hand (sections F and G). Lastly, against the background of the foregoing the relevant parts of the DSA proposal are assessed (section H), before terminating with a brief conclusion (section I).

B. Current EU legal framework

6 As mentioned, in the EU, the principle of knowledge-based liability is currently enshrined in Article 14 ECD. In essence, the article states that providers of so-called 'hosting' services cannot be held liable for the content that they store for their users, unless they obtain knowledge of the illegality of the content and fail to act expeditiously by removing the content.[18] It is disputed precisely which sorts of services qualify as 'hosting' within the meaning of this provision. In itself, it is clear that the concept of 'hosting' refers to the storage by a service provider of content provided by and stored at the request of users of the service in question.[19] A broad range of services could therefore, in principle, qualify. The case law captures the activities undertaken by social media companies such as Facebook, by online marketplaces such as eBay and by video-sharing platforms such as YouTube.[20] Yet a broad range of other activities, such as those performed by cloud storage providers and consumer review sites, should normally be able to qualify as well. The concept is therefore considerably broader than traditional website hosting.[21]

7 The Court of Justice of the EU ('Court of Justice' or 'Court') has specified that, for the hosting activities to be covered by Article 14 ECD, the service providers concerned must not "*play an active role of such as kind as to give them knowledge of, or control over*" the user content in question.[22] This serves as a reminder that the liability exemption at issue here is not available where the content potentially giving rise to liability is the provider's 'own' content.[23] Yet the Court's criterion is broader. It also relates to content in respect of which the provider departed from the neutral position that it is expected to retain as an intermediary.[24] In the context of the activities of an online marketplace the Court has clarified that the service provider retains a neutral position where it "*stores offers for sale on its server, sets the terms of its service, is remunerated for that service and provides general information to its customers*". By contrast, the service provider is considered not to have retained such a neutral position where it "*provided assistance which entails, in particular, optimising the presentation of the offers for sale in question or promoting those offers*".[25]

8 A degree of uncertainty exists as to where the line should be drawn precisely, however.[26] That is so especially because many service providers do not merely store user content, but also conduct certain additional activities in relation thereto. For instance, organising the user content by indexing it, making it searchable or recommending it to other users.

18 For reasons of ease of reference and readability, some matters are simplified in this article. First, Art 14(1) ECD covers not only the situations where the service providers *obtain* knowledge, but also where they already *have* it. Second, the reference to 'knowledge' is meant to cover both types of knowledge that Art 14(1) distinguishes, namely, 'actual knowledge' and 'awareness' (the latter being applicable specifically in relation to actions for damages and entailing construed knowledge). Third, Art 14(1) provides, as an alternative to the *removal* of illegal content, also for the possibility of *disabling access* thereto.

19 The term 'storage' refers to the holding of data in the memory of a server. See CJEU, *L'Oréal v eBay*, C-324/09, ECLI:EU:C:2011:474, 110.

20 See, respectively, CJEU, *Glawischnig-Piesczek v Facebook Ireland*, C-18/18, ECLI:EU:C:2019:821; CJEU, *L'Oréal v eBay* (n 19); CJEU, *YouTube*, C-682/18 and C-683/18, ECLI:EU:C:2021:503.

21 Cf Przemyslaw Polanski (n 3), 875-877 (making a similar point). See also J Van Hoboken, J Quintas, J Poort and N Van Eijck, '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 Commission, 2018, 9-16 (containing a typology of hosting services).

22 CJEU, *L'Oréal v eBay* (n 19), 113. See also CJEU, *YouTube* (n 20), 106.

23 This includes content that has been provided by a user that is under service provider's control or authority (Art 14(2) ECD). See also CJEU, *Papasavvas*, C-291/13, ECLI:EU:C:2014:209.

24 Cf CJEU, *YouTube* (n. 20), 105-105; CJEU, *L'Oréal v eBay* (n 19), 112.

25 Ibid, 115-116.

26 See eg Commission, Impact assessment DSA proposal, SWD(2020) 348, 31-32. See also para 46 below.

Arguably, many of such activities are needed to enable users to have meaningful access to the large quantities of user content that many service providers store.[27] Importantly, the aforementioned criterion articulated by the Court of Justice does not require absolute passivity[28] – it implies that the service provider *can* be active to some extent, provided its involvement is not such as to give it knowledge of or control over the user content concerned. The recent judgment by the Court of Justice in the *YouTube* case provided some further guidance in this respect, at least in situations involving allegedly copyright-infringing user content stored on video-sharing and file-sharing platforms.[29] The judgment implies that the mere fact that the service providers concerned conduct the aforementioned kinds of activities does not mean that they are, necessarily and a priori, excluded from the scope of Article 14 ECD for being 'too active'. The Court appeared to assess the matter rather under the conditions on the providers acting expeditiously upon obtaining knowledge. At the same time, the judgment still leaves uncertainty. That is so especially in relation to the question identified therein whether the service providers contribute, 'beyond merely making the platform available', to giving the public access to the stored user content in breach of copyright. The main conclusion therefore appears to be that there are few bright-line rules. Rather, a case-by-case assessment is required to determine whether the provider's role is a neutral one.

9 When it comes to the types of liability stemming from illegal user content covered by the liability exemption, the scope of the protection offered by Article 14 ECD is wide. Although the Court of Justice has to date not expressly confirmed this, it is generally believed that the term 'liability' refers to liability regardless of whether it is civil, administrative or criminal in nature.[30] The liability exemption is 'horizontal' also in another sense: it applies irrespective of the field of law at issue. Consequently, covered is possible liability under laws on, inter alia, intellectual property, defamation, privacy, anti-terrorism, child pornography and hate speech.[31]

10 It is important to underline that we are dealing here with an *exemption* from liability. The rules potentially *establishing* the liability of the service providers are in principle to be found in the laws of the Member States (and, occasionally, EU law).[32] Therefore, where a hosting service provider fails to meet the conditions of the liability exemption of Article 14 ECD – in particular, expeditiously removing the item of illegal content upon obtaining knowledge thereof – this does not necessarily mean it is liable for the user content in question. Rather, it means that the hosting service provider is not a priori *shielded* from such liability. One 'type' of liability is carved out from the liability exemption, however. National courts or administrative authorities can, in accordance with the applicable rules of national law, require a hosting service provider to "*terminate or prevent an infringement*", irrespective of whether or not the conditions of the liability exemption are met.[33] In other words, injunctive relief is excluded from the scope of the liability exemption.

11 Under Article 14 ECD, the knowledge of the illegality of items of stored user content, which in turn triggers the expectation for hosting service providers to expeditiously remove such content (if they want to benefit from the liability exemption, that is), can be obtained in several manners.[34] The

27 See also para 14 and 20 below (expanding on the quantities of user content stored).

28 The discussion is therefore sometimes wrongly simplified as being about the active or passive role of the service provider. In this regard, it is noticeable that, in CJEU, *L'Oréal v eBay* (n 19), the word 'passive' is not mentioned at all, although that is different in other rulings, most notably CJEU, *YouTube* (n. 20), 105 and CJEU, *Google France*, C-236/08 to C-238/08, ECLI:EU:C:2010:159, 113-114. See also Opinion Advocate General (AG) Jääskinen, *L'Oréal v eBay*, C-324/09, ECLI:EU:C:2010:757, 138-146 (strongly criticising the approach seemingly requiring strict neutrality taken in *Google France*). Cf Van Hoboken et al (n 21), 31 and 33 (arguing that in this connection the terms 'neutral', 'active' and 'passive' should be understood as terms of art and as non-binary, encompassing a range of meanings along a spectrum of potential activities).

29 CJEU, *YouTube* (n. 20), in particular 108 and 114. See also the opinion of AG Saugmandsgaard Øe in that case, ECLI:EU:C:2020:586, 143-168.

30 See eg AG Saugmandsgaard Øe, *YouTube* (n 29), 138; Opinion AG Szpunar, Case C-484/14, *McFadden*, ECLI:EU:C:2016:170, 64; Commission, Proposal for a Directive on certain legal aspects of electronic commerce in the internal market, COM (1998) 586 ('Proposal ECD'), 27 and 29.

31 Cf Recital 16 Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, [2001] OJ L 167/10 ("*Liability for activities in the network environment [...] is addressed horizontally in [the ECD]*"). Cf also Commission, Proposal ECD, COM(1998) 586, 27. See however also para 50 below (regarding the specific regime applicable to certain service providers in relation to copyright-infringing content contained in Art 17 CDSM Directive, which deviates from Art 14 ECD).

32 Cf eg CJEU, *Google France* (n 28), 107; Commission, Proposal ECD, COM(1998) 586, 27.

33 Art 14(3) ECD. Cf CJEU, *Facebook Ireland* (n 20), 25.

34 CJEU, *L'Oréal v eBay* (n 19), 122.

knowledge will frequently be obtained through the reception of a notice – that is, a message sent by a third party informing the service provider of the presence of allegedly illegal content on its service and typically requesting its removal. As such, the liability exemption provides the basis for a system of 'notice and takedown', also known as 'notice and action'.[35] The resulting notice-and-action system is and remains in many respects the "*most popular internet enforcement mechanism*".[36] However, this does not mean that the service providers concerned cannot obtain knowledge of illegal user content on their services in other manners. That can occur, most notably, through investigations carried out on their own initiative. Large service providers, in particular, are increasingly proactive in scanning and moderating the content that they store for their users.[37]

C. Knowledge-based liability: rationale

12 Why is that providers of hosting services should be allowed to benefit from a conditional liability exemption of the type outlined above? Why not make them subject, for instance, to specific rules imposing strict liability for the content that they store and often disseminate for their users? These questions can be approached from two viewpoints: that of the hosting service providers themselves, and that of the other parties involved.

13 Starting with the former, there are two main elements that together argue against holding hosting service providers strictly liable. The first element is that, as was touched upon above, the content in question is by definition not their 'own'. The service providers do not create or submit the content themselves and they normally do not have knowledge of or control over the content either, at least initially. It seems natural to apply stricter liability standards only to parties that know of or exercise control over certain illegal material or conduct – or that are at least reasonably *capable* of obtaining such knowledge or exercising such control. For example, as a general rule, producers are strictly liable for their products and employers are strictly liable for the acts of their employees.[38]

14 The second main element that argues against holding hosting service providers strictly liable for user content relates to the large quantities of such user content that they tend to intermediate. This point is probably best exemplified by the ruling by an US court in *Netcom*, the case that lay the groundwork for Section 512(c) DMCA's notice-and-action mechanism, which in turn was a source of inspiration for the EU regime.[39] The case arose in 1995, in the early days of the popular internet. The court held that "*billions of bits of data flow through the Internet and are necessarily stored on servers throughout the network*" and that it is "*practically impossible to screen out infringing bits from non-infringing bits*".[40] It therefore refused to hold the online services providers concerned primarily liable for the infringements in question, but did not rule out secondary liability. Likewise, the "*staggering*" amounts of user content at issue also played an important role in *Zeran*, the case that decisively shaped the broad manner in which Section 230 CDA's liability exemption is construed in the US.[41] This does not appear to be fundamentally different when it comes to Article 14 ECD.[42] In fairness, the quantities of user content involved do not, in themselves, necessarily *rule out* the service providers having knowledge of or control over the content. It rather means that they would have to take quite far-going measures to obtain such knowledge or control. In this regard, a comparison can be drawn with distributors of third-party materials in the offline world, such as postal service providers or bookshops. These parties could theoretically be required to examine all such materials that they transmit or sell, with a view to screening out illegal materials. Yet it would be, as the

35 Cf Recital 40 ECD.

36 J Riordan, *The liability of internet intermediaries* (Oxford University Press 2016), 63. See eg also Urban et al (n 3), 114 (concluding, based on an extensive study carried out in the US, that the notice-and-action system "*continues to provide an efficient method of enforcement in many circumstances*").

37 See eg J Kosseff, *The twenty-six words that created the internet* (Cornwell University Press 2019), 241-242; Klonick (n 17), 1619-1621. More generally, see T Gillespie, *Custodians of the internet: platforms, content moderation, and the hidden decisions that shape social media* (Yale University Press 2018).

38 Cf A Yen, 'Internet service provider liability for subscriber copyright infringement, enterprise liability, and the First Amendment', Boston College Law School Research Paper No 2000-03, 2000, 25-28.

39 US District Court Northern District of California, *Religious Technology Center v Netcom*, 907 F.Supp. 1361 (1995). See also HR Rep No 105-551, pt 1 (1998), 11 (noting that the bill that was to become Section 512 DMCA essentially codifies the ruling in *Netcom*).

40 Ibid, 1372-1373.

41 US Court of Appeals, *Zeran* (n 12), 331.

42 Cf AG Saugmandsgaard Øe, *YouTube* (n 29), 175 and 183.

US Supreme Court put it, "*altogether unreasonable to demand so near an approach to omniscience*" from these intermediaries.[43]

15 That leads us to the second perspective: that of the other parties involved. Apart from the service providers, there are two such other parties in a typical situation: the *users* of the services and the *parties aggrieved* by the illegal content stored. Starting with the users, the key point is that the service provider's burden resulting from the imposition of strict liability may well become the public's burden, to again echo the US Supreme Court.[44] The measures that the service providers may feel obliged to take in order to avoid being held strictly liable will have adverse consequences for the users, too. The consequences could be economic in nature, such as higher costs for the use of the services. They could also consist of invasion of the users' privacy resulting from extensive and intrusive monitoring. What is more, the consequences could consist of reduced possibilities for users to express themselves and to receive information. That could occur for several reasons, including for example: because the measures taken by the service providers are inaccurate and block or remove user content wrongly thought to be illegal; because the service providers decide to no longer provide certain services in view of the liability risks; or because such measures deter users from uploading content in the first place. All this underlines the *instrumental* nature of the knowledge-based liability exemption. It serves not only to protect the service providers, but also – and arguably even primarily – the users.

16 In addition, one should take account of the interests of the aggrieved parties, such as the persons who hold the intellectual property right that is infringed or who are defamed by the user content. These parties would generally benefit from the imposition of strict liability, because that would strongly incentivise the service providers to take the aforementioned measures aimed at tackling the user content that infringes their rights. However, as noted, that approach would have significant downsides not only for the service providers, but also for their users. If, conversely, the service providers were to be broadly or even completely exempted from any form of liability, the aggrieved parties would likely encounter serious difficulties in enforcing their rights. This is one of the main reasons why the broad and unconditional liability exemption of Section 230 CDA is criticised.[45] True, aggrieved parties could then still have redress against the users who provided the content. However, this possibility may well be remote or even largely meaningless in practice, considering how difficult it tends to be to identify those users and hold them accountable.[46] Put differently, by excluding aggrieved parties' redress against the service provider involved, one thwarts their possibilities to obtain effective redress. That would occur despite the fact that the service providers are typically in a good position to terminate the violation of the aggrieved parties' rights and limit the negative consequences thereof. Indeed, their position as "*single point of control*" and their "*superior ability to avoid harm*"[47] is the main reason to involve them in efforts aimed at tackling illegal online content in the first place.[48]

17 The knowledge-based liability model thus aims to strike a middle-way. It avoids the negative consequences of stricter forms of liability that would impact not only the service providers themselves, but also their users. At the same time, it does not completely preclude the possibility for aggrieved parties to have recourse to the service provider concerned where their rights are at stake. Indeed, given that submitting a takedown notice typically requires relatively little effort and expense from aggrieved parties and may lead to swift results,[49]

43 US Supreme Court, *Smith v California*, 361 US 147 (1959), 153–154.

44 Ibid.

45 See Wilman (n 13), 121 (with further references).

46 See eg Kosseff (n 37), 221-222 ("*Given the uncertainty of the unmasking process, it is disingenuous to simply dismiss the harms suffered by plaintiffs [...] because they did not sue the [user providing the illegal online content concerned]*"); European Court of Human Rights (ECtHR), *Høiness v Norway*, Appl no 43624/14 (2019), 70 ("*Turning to the possibilities for the applicant to pursue claims against the anonymous individual or individuals who had written the comments, the Court sees no reason to contest the applicant's allegation that she would have faced considerable obstacles in attempting to do so*").

47 See, respectively, F Wu, 'Collateral censorship and the limits of intermediary immunity', (2011) *Notre Dame Law Review* 87, 314; J Balkin, 'Free speech and hostile environments', (1999) *Columbia Law Review* 99, 2302. See eg also M Rustad, and T Koening, 'Rebooting cybertort law', (2005) *Washington Law Review* 80, 390 (referring to online service providers as 'least-cost avoiders' of harm).

48 See eg Recital 2 Recommendation (EU) 2018/344 on measures to effectively tackle illegal online content, [2018] OJ L 63/50 ('Illegal Content Recommendation') ("*In the light of their central role and the technical means and capabilities associated with the services that they provide, online service providers have particular societal responsibilities to help tackle illegal content disseminated through the use of their services*"); Recital 59 Infosoc Directive (explaining the creation of the possibility to issue injunctions against online intermediaries by noting that they tend to be "*best placed to bring [...] infringing activities [by the users of their services] to an end*").

49 Cf K Wallberg, 'Notice and takedown of counterfeit goods in

the principle normally provides these parties with a realistic prospect of redress.

D. Developments in practice

18 There are obvious changes – especially in the online world – since laws such as the ECD in the EU and Sections 230 CDA and 512 DMCA in the US were adopted over two decades ago. That was a time when judges still felt the need to explain in judgments relating to online matters what the internet actually was.[50] Back then, internet users worldwide numbered in the tens of millions, not the billions of today.[51] It is true that some of the services involved already existed in embryonic form. Social networks can trace their origins to bulletin boards, for example. Nonetheless, such services are hardly comparable, both in terms of their key features and the manner in and extent to which they are used. Most of today's well-known service providers such as YouTube, Facebook, Twitter, Instagram and TikTok did not yet exist at the time. Bandwidth has also grown exponentially. That has greatly facilitated the possibilities to transmit user content, both of the legal and the illegal kind. The introduction of smart phones means that many people are almost continuously online.

19 While highly significant in many ways, in and of themselves, those changes tell us little about the continued relevance and suitability of the legal framework sketched above, however. In order to establish that, the following three points should be considered in particular.

20 To begin with, the quantities of content that some hosting service providers store for their users are nowadays larger than ever before. To illustrate the point: reportedly YouTube's over two billion monthly active users upload around 500 hours of video per minute and Twitter's 330 million monthly active users send around 500 million tweets a day.[52] In line with what was said above, these staggering numbers arguably reinforce the need for limiting the liability of the service providers to only user content that they know (or should know) to be illegal. However, there is also another noteworthy development: the typically increased ability of service providers to *obtain* knowledge of or control over the content that they store. The best-known example is probably YouTube's Content ID tool, which automatically checks uploaded user content and allows for the blocking of content that matches with copyright-protected works. YouTube is by no means alone in using such tools. Many large hosting service providers do so, not only in respect of copyright-infringing content but also of content depicting nudity, self-harm, terrorist content and hate speech, among other things.[53] As already touched upon above, they also tend to be increasingly active in relation to the user content stored, especially by improving accessibility and moderating the content. In addition, they apply increasingly sophisticated means that allow them to specifically target advertising as well as gather and process large amounts of data relating to their users. In this light, the commercial internet has said to have developed into "*the most surveilled zone of human activity in history*".[54] Although the proactive tackling of illegal user content certainly

the Digital Single Market: a balancing of fundamental rights', (2017) *Journal of Intellectual Property Law & Practice* 12, 933 (noting that the formal requirements imposed by hosting service providers are "*few and easy to satisfy*"). As to the speed of removals, as mentioned, Art 14(1) ECD is conditional upon hosting service providers removing notified illegal content "*expeditiously*". In practice, that often means removal within at most a few days. Cf Commission, Code of conduct on countering illegal hate speech online – fourth evaluation confirms that self-regulation works, 2019, 2 (indicating that service providers meet their commitment to remove illegal hate speech within 24 hours pursuant to the 2016 Code of Conduct on Countering Illegal Hate Speech Online in 89% of the cases); Commission, Report assessing the implementation of the measures referred to in Article 25 of Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography, COM(2016) 872, 9–10 (indicating that 93% of child sexual abuse material notified by hotlines in Europe is removed within 72 hours).

50 Eg US Supreme Court, *Reno v ACLU*, 521 US 844 (1997), 849-850.

51 Ibid, 850. In January 2021, the number of active internet users worldwide reportedly stood at over 4,66 billion. See <https://www.statista.com/statistics/617136/digital-population-worldwide/#:~:text=Almost%204.66%20billion%20people%20were,percent%20of%20total%20internet%20users>.

52 See <https://www.statista.com/statistics/259477/hours-of-video-uploaded-to-youtube-every-minute/#:~:text=As%20of%20May%202019%2C%20more,for%20online%20video%20has%20grown>; <https://www.brandwatch.com/blog/twitter-stats-and-statistics/>.

53 See Wilman (n 13), 255-256 (with further references).

54 D Keats Citron and N Richards, 'Four principles for digital expression (you won't believe #3!)', (2018) *Washington University Law Review* 95, 1375. See also D Keller, 'Who do you sue? State and platform hybrid power over online speech', Hoover Institution Essay Aegis Series Paper No. 1902, 2019, 1 ("*Facebook and other large internet companies can monitor every word users share and instantly delete everything they don't like. No communications medium in human history has ever worked this way*").

involves challenges,[55] the argument that services providers cannot reasonably be required to do more in this respect than 'just' reacting to notices (and, occasionally, injunctions) thus no longer seems entirely convincing.

21 What was said in the previous paragraph comes with an important qualifier, however, which is the second point to be noted. The foregoing may hold true for a comparatively limited number of large hosting services providers, which have very considerable technological, human and financial means at their disposal. However, it does not – or at least not to the same extent – hold true for many other, smaller hosting service providers. In the EU, there are estimated to be over 10,000 hosting service providers, 85% of which are either micro or small enterprises.[56] The rise of 'mega-platforms' such as Facebook and YouTube raises all kinds of concerns, including competition-related ones, which largely fall outside the scope of this article.[57] Nonetheless, it is a widely shared concern that imposing on hosting service providers increased obligations to tackle illegal user content would reinforce the position of the incumbents.[58] The latter generally have the means to take the necessary measures to meet such obligations, even if they involve considerable investments. YouTube's Content ID tool, for instance, costs an estimated total of 100 million USD to develop and operate,[59] whilst Facebook employs tens of thousands human content moderators.[60] Their smaller competitors, including new entrants and start-ups, may not have the means to meet such obligations. The pockets of the 'mega-platforms' may also be deep enough for them not to be overly fearful of damages claims for any illegal content that their users may upload. For many others, however, the decision not to remove potentially illegal content can boil down to 'betting the company'[61] – something that they are understandably not very inclined to do. Therefore, whilst the knowledge-based liability exemption may not solely be about protecting hosting service providers, many of them still need the protection afforded to them. The protection is arguably needed now even more than before if smaller providers are to stand a chance to compete with the large incumbents.

22 As a third point, the generally large – and sometimes enormous – quantities of user content stored illustrate how broadly hosting services are used for all kinds of economic, social, recreational, cultural and political purposes. Whether you want to buy or sell a second-hand product, listen to music, stay in touch with friends, rent a holiday home or check out consumer reviews before booking a restaurant – all of these activities will in many cases involve the use of hosting service providers. It has been said that, fundamentally, "*there is not a single online service or activity that does not involve the activity of one or more hosting service providers*".[62] The online sphere is also an important battlefield in any modern political campaign, just as the services at issue here are widely used for people to organise themselves for all kinds of other purposes, stay informed and exchange information. Many of these activities are of course perfectly legitimate and even socially beneficial. Yet, there is no denying that the services are also widely used for all kinds of illegal purposes. This is not new; the liability exemptions of the ECD and its US counterparts were drafted in part with the aim of combatting illegal activities conducted online.[63] Nonetheless, difficult as this may be to quantify, it seems safe to say that the scale of the problem has increased. In relation to child sexual abuse material it has been observed, for instance, that "*[t]echnology has generated a paradigm shift in both the victims' online exposure and the offenders' ability to*

55 For instance, relating to the accuracy of automated means used (particularly in context-sensitive situations) and the psychological toll for human content moderators.

56 Commission, Impact assessment DSA proposal, SWD(2020) 348, 24.

57 See in this regard in particular the DSA's 'sister act': Commission, Proposal for a Regulation on contestable and fair markets in the digital sector (Digital Markets Acts), COM(2020) 842.

58 See eg G Frosio and C Geiger, Taking fundamental rights seriously in the Digital Services Act's platform liability regime', 2020, available via <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3747756>, 31 ("*Imposing new burdensome obligations on [online service providers] would decrease innovation by making it more expensive for new players to enter the market*"); A Bridy, 'Three notice failures in copyright law', (2016) *Boston University Law Review* 96, 791 ("*For large, well-capitalized providers like the Googles and Facebooks of the world, taking on extra enforcement burdens may not be onerous. For new entrants and smaller providers, however, those extra costs may be unbearable*"). See also AG Saugmandsgaard Øe, *YouTube* (n 29), 194.

59 A Bridy, 'The price of closing the "value gap": how the music industry hacked EU copyright reform', (2020) *Vanderbilt Journal of Entertainment and Technology Law* 22, 350.

60 M Zuckerberg, 'Blueprint for content governance and enforcement', 15 November 2018.

61 Urban et al (n 3), 43.

62 Van Hoboken et al (n 21), 11-12.

63 Cf Commission, Proposal ECD, COM(1998) 586, 4 (explaining that the aim is to establish a balanced regime "*in order to stimulate cooperation between different parties thereby reducing the risk of illegal activity online*").

share [such material] securely and interact anonymously with children and other offenders online".[64] The head of the EU Fundamental Rights Agency has called online hate speech "*a plague of our times*", adding that "*things are getting worse*".[65] A US judge observed that "*[r]ecent news reports suggest that many social media sites have been slow to remove the plethora of terrorist and extremist accounts populating their platforms, and that such efforts, when they occur, are often underinclusive*".[66]

23 In conclusion, whilst not unidirectional, the developments outlined above confirm and broadly reinforce the need for a 'middle way' approach like the one embodied in the knowledge-based liability model. In essence, that is because for all parties involved – and, by extension, for society as a whole – the stakes have increased. That goes for persons negatively affected by, for example, copyright infringement, defamation or privacy violations occurring online, in view of the broad reach of many of services in question and the internet's inability to 'forget'.[67] At the same time, the stakes for users who may be wrongly targeted by, or who may otherwise suffer adverse consequences of, service providers' measures to tackle illegal online content appear to have increased as well. For instance, having your account or the entire service provision suspended can significantly limit your ability to express yourself, obtain information or engage in social interactions and legitimate commercial activities online. Furthermore, if even some of your most intimate and sensitive communications take place online, it becomes all the more important that they remain private. As to the service providers themselves, whilst the relatively few large ones could reasonably be made subject to further-going requirements, it appears that for many others the current liability exemptions are as important today as they were two decades ago.

64 WeProtect Global Alliance, Threat Assessment Report 2018, 2018, 7.

65 M O'Flaherty, Director EU Agency for Fundamental Rights, 'Opening address at the roundtable on artificial intelligence and online hate speech', 31 January 2019.

66 Partially concurring and partially dissenting opinion Judge Katzmann, US Court of Appeals 2nd Circuit, *Force v Facebook*, 934 F3d 53 (2019), 84–85 (with further references).

67 See eg ECtHR, *Delfi v Estonia*, Appl no 64569/09 (2015), 110 ("*Defamatory and other types of clearly unlawful speech, including hate speech and speech inciting violence, can be disseminated like never before, worldwide, in a matter of seconds, and sometimes remain persistently available online*").

E. Developments in EU fundamental rights law

24 The continued and reinforced need for a 'middle way' approach in relation to the liability of online service providers for the user content that they store and often disseminate comes to the fore even more when another evolution, which is not factual but legal in nature, is taken into account. Namely, the rise of the fundamental rights dichotomy in the EU legal order. To be sure, fundamental rights-related concerns emerging in the present context are not new, either. The ECD highlights in its recitals the importance of the fundamental right to freedom of expression, for instance.[68] Yet it seems clear that, especially in the EU, the issue at stake is increasingly framed in terms of fundamental rights. A few examples include: rightsholders confronted with online copyright infringement are not merely suffering economic damage, but may have their fundamental right to protection of intellectual property violated;[69] persons affected by online defamation may act to protect not only their reputation, but also their fundamental right to a private and family life;[70] the dissemination of child sexual abuse material is not only problematic in and of itself, but can involve violations of several fundamental rights, notably the prohibition of inhumane and degrading treatment, the right to respect for private and family life, and the rights of the child;[71] requirements imposed on online service providers to tackle illegal user content are not merely burdensome, but can call into question their fundamental right to freedom to conduct a business;[72] and filtering and blocking measures taken by service providers can be not only

68 See in particular Recitals 9 and 46 ECD.

69 See eg CJEU, *McFadden*, C-484/14, ECLI:EU:C:2016:689, 81; CJEU, *UPC Telekabel*, C-314/12, ECLI:EU:C:2014:192, 47 (both referring to Art 17(2) Charter).

70 See eg ECtHR, *Delfi v Estonia* (n 67), 137 (referring to Art 8 of the European Convention of Human Rights (ECHR), which corresponds to Art 7 Charter).

71 See eg CJEU, *La Quadrature du Net*, C511/18, C512/18 and C520/18, ECLI:EU:C:2020:791, 128 (referring to Art 4 and 7 Charter); Commission, Proposal for a Regulation on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by number-independent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse online, COM(2020) 568, 4 (referring to Art 24 Charter).

72 See eg CJEU, *McFadden* (n 69), 88; CJEU, *Scarlet Extended v SABAM*, C-70/10, ECLI:EU:C:2011:771, 48 (both referring to Art 16 Charter).

annoying for their users, but may negatively affect their fundamental rights to privacy, protection of personal data and freedom of information.[73]

25 All this reflects in part the increased use and importance of the services in question, described earlier. However, it also reflects the fact that EU fundamental rights law itself has evolved significantly over the past two decades. To start, it was not until 2009 that the Charter of Fundamental Rights of the EU ('the Charter') became legally binding.[74] Although fundamental rights were already protected beforehand (as general principles of EU law), this development has undoubtedly increased the visibility and importance of fundamental rights protection in the EU. This results not only from their codification as such, but also from the fact that the Charter expressly recognises several relatively novel rights, such as protection of personal data, the freedom to conduct a business, protection of intellectual property and the rights of the child.[75] As indicated in the previous paragraph, these rights may well be at issue in cases arising in the present context.

26 Furthermore, the requirement to strike a 'fair balance' in situations where several conflicting fundamental rights are at stake is by now well established under the case law of the Court of Justice. As such, it constitutes a cornerstone of the EU fundamental rights regime. Yet the requirement was only first clearly articulated in 2008.[76] That is well after the adoption of the ECD. Tellingly, the ECD frames the issue in terms of balancing the conflicting *interests*.[77] It appears that, at the time, the EU legislator primarily had economic interests in mind, such as ensuring the affordability of access to online services and stimulating the development of electronic commerce.[78] Under said case law, these interests have since been 'upgraded' to conflicting *fundamental rights* that are to be balanced.

27 To this should be added the emerging – and still very much developing – case law of the Court of Justice on three other fundamental rights doctrines.[79] First, a main driver behind the developments in the US in this area is the risk that imposing liability for user content that online service providers intermediate may have a 'chilling effect' on freedom of expression.[80] This term refers to the indirect negative effect that such liability may have on the dissemination and reception of legitimate expressions online.[81] Without having expressly used the term thus far, the Court has acknowledged that such a chilling effect must be avoided also as a matter of EU fundamental rights law.[82] This reinforces the argument against imposing overly strict forms of liability on hosting service providers.

28 In addition, there is the doctrine on the 'horizontal direct effect' of the Charter.[83] This refers to the obligations on private parties to respect the rights enshrined in the Charter in their relationship with other private parties. To date, the Court of Justice has recognised such a horizontal direct effect only in respect to some of those rights,[84] whilst it is for now

73 CJEU, *GS Media*, C-160/15, ECLI:EU:C:2016:644, 31 and 45 (referring to Art 11 Charter); CJEU, *Scarlet Extended* (n 72), 51-52 (referring to Art 8 and 11 Charter).

74 The Charter became legally binding through the Treaty of Lisbon, which entered into force in December 2009. The Charter has the same legal value as the EU Treaties (Art 6(1) Treaty on European Union.

75 Art 8, 16, 17 and 24 Charter, respectively.

76 CJEU, *Promusicae*, C-275/06, ECLI:EU:C:2008:54, 68.

77 Recital 41 ECD.

78 See AG Saugmandsgaard Øe, *YouTube* (n 29), 194; Commission, First report on the ECD, COM(2003) 702, 14 and 20.

79 Note that the doctrines referred to above are novel in as far as the Charter and the case law of the CJEU is concerned. The former ('chilling effects') and the latter doctrine (positive obligations) have both been extensively articulated in case law of the ECtHR. As regards the former, see eg T Baumbach, 'Chilling effect as a European Court of Human Rights' concept in media law cases', (2018) *Bergen Journal of Criminal Law and Criminal Justice* 6, 92–114. As regards the latter, see eg the case law cited in para 29 below.

80 See eg US Court of Appeals, *Zeran* (n 12), 331 ("*The specter of tort liability in an area of such prolific speech would have an obvious chilling effect*").

81 See further L Kendrick, 'Speech, intent and the chilling effect', (2013) *William & Mary Law Review* 54, 1633–1691; F Schauer, 'Fear, risk and the First Amendment: unravelling the chilling effect', (1978) *Boston University Law Review* 58, 685–732. See also para 15 above.

82 CJEU, *La Quadrature du Net* (n 71), 128; CJEU, *Digital Rights Ireland*, C-293/12 and C-594/12, ECLI:EU:C:2014:238, 28 (both in the context of the retention of personal data). Cf A Kuczerawy, *Intermediary liability and freedom of expression in the EU: from concepts to safeguards* (Intersentia 2018), 160 (making a similar point). Some AGs have been more explicit: see in particular Opinion AG Cruz Villalón, *eDate Advertising*, C-509/09 and C-161/10, ECLI:EU:C:2011:192, 46.

83 See in particular CJEU, *Cresco Investigation*, C-193/17, ECLI:EU:C:2019:43; CJEU, *Bauer*, C-569/16 and C-570/16, ECLI:EU:C:2018:871; CJEU, *Egenberger*, C-414/16, ECLI:EU:C:2018:257.

84 See eg CJEU, *Association de médication sociale*, C-176/12,

uncertain what this entails concretely.[85] Those rights include, however, the prohibition of discrimination and the right to an effective remedy[86] – fundamental rights that may well be of relevance in the present context. The Court has also indicated that providers of certain online services themselves (as imposed to the public authorities concerned) are under certain circumstances to ensure the aforementioned fair balance between conflicting fundamental rights.[87] It is not inconceivable, therefore, that hosting service providers have certain obligations directly under EU fundamental rights law. Possible obligations could include being particularly attentive when it comes to racist and xenophobic expressions or ensuring that aggrieved parties can effectively address stored illegal content. Rather than making secondary law redundant, this development may well create uncertainty that is best addressed through adopting acts of secondary EU law that give concrete expression to any such obligations.

29 Lastly, the Court of Justice has acknowledged even more recently the existence of 'positive obligations' resulting from the Charter.[88] That means that relevant public authorities should not only ensure that they do not violate fundamental rights, but also take active steps to safeguard those rights. Again, this probably does not hold true for all Charter rights and it remains to be seen what this means in operational terms.[89] The implications for the present purposes could nonetheless be considerable. For instance, it has long been argued that to adequately protect the rights of all parties involved, the EU legislator should lay down binding rules on notice-and-action procedures.[90] Such arguments are (even) more convincing now that they can potentially rely on this recent line of case law. The case law of the European Court of Human Rights[91] suggests that one could, depending on the circumstances, also think of positive obligations to establish a legal framework through which: anonymous perpetrators can be identified and prosecuted;[92] infringements of intellectual property rights do not go unsanctioned;[93] and safeguards against abuse are provided for and access to a remedy before a court is ensured.[94]

30 In summary, the fundamental rights landscape has evolved quite drastically. The above jurisprudential developments are not specific to matters relating to the liability of hosting service providers. Nonetheless, they have important implications for the present purposes, especially since the issues emerging in this context so often involve the exercise of (conflicting) fundamental rights. More specifically, the increased emphasis on fundamental rights suggests that the EU legislator's discretion may be limited in several respects.[95] For one thing, its discretion *not*

EU:C:2014:2, 48 (indicating that Art 27 Charter does not have horizontal direct effect).

85 There is, for instance, the question as to precise consequences of any such horizontal direct effect, beyond the disapplication of incompatible rules of national law. In addition, see K. Lenaerts, President CJEU, speech at the conference 'Making the EU Charter of Fundamental Rights a reality for all: 10th anniversary of the Charter becoming legally binding', 12 November 2019 (suggesting that 'only' the essence of the relevant fundamental rights could work directly in relationships between private parties). In any event, the effects are limited to fields covered by EU law (see Art 51(1) Charter).

86 CJEU, *Egenberger* (n 83), 76 and 78 (relating to Art 21 and 47 Charter). See also CJEU, *Veselības ministrija*, C243/19, ECLI:EU:C:2020:872, 36 (regarding Art 21 Charter).

87 CJEU, *GC v CNIL*, C-136/17, ECLI:EU:C:2019:773, 75-76 (relating to the 'right to be forgotten' as established in EU law on the protection of personal data).

88 See in particular CJEU, *La Quadrature du Net* (n 71), 126 (referring to Art 3, 4 and 7 Charter).

89 Cf L Woods, 'Article 11', in S Peers, T Hervey, J Kenner and A Ward (eds), *The EU Charter of Fundamental Rights: a commentary*, Hart 2014, 311–339, 332 (referring to the "*uncertain realm of states' positive obligations*"). Cf also ECtHR, *Osman v UK*, Appl no 23452/94 (1998), 116 (pointing out that a positive obligation "*must be interpreted in a way which does not impose an impossible or disproportionate burden on the authorities*").

90 See (among many others) eg A Savin, *EU internet law* (Edward Elgar 2017), 153; A Kuczerawy, 'The power of positive thinking: intermediary liability and the effective enjoyment of the right to freedom of expression', (2017) *Journal of Intellectual Property, Information Technology Law and Electronic Commerce Law* 3, 237; Riordan (n 36), 384; Van Eecke (n 3), 1463; R Julià-Barceló, and K Koelman, 'Intermediary liability in the e-Commerce Directive: so far so good, but it is not enough', (2000) *Computer Law & Security Report* 16, 231.

91 The case law of the ECtHR on the ECHR can be of indirect yet significant importance in the EU legal order. See in particular Art 52(3) Charter (indicating that, in as far as Charter rights correspond to rights guaranteed under the ECHR, the meaning and scope of the former are the same as the latter).

92 ECtHR, *K.U. v Finland*, Appl no 2872/02 (2008), 48–49 (in the context of the protection of minors).

93 ECtHR, *Sunde v Sweden*, Appl no 40397/12 (2013), D (regarding the protection of copyright).

94 ECtHR, *Barbulescu v Romania*, Appl no 61496/08 (2017), 115, 120 and 122 (relating to a situation involving employers monitoring their employers' communications).

95 Cf also, more generally, CJEU, *Digital Rights Ireland* (n 82), 47–48 (indicating that in situations where fundamental rights play

to regulate relevant issues in any detail may have been reduced.[96] For another thing, especially in view of the requirement of fair balance, its discretion to opt for stricter forms of liability than knowledge-based liability might be limited too. That holds even more true when the case law of the European Court of Human Rights is taken into account. That case law suggests that a 'rigid', strict liability approach might not be feasible from a fundamental rights viewpoint, since it "*effectively precludes the balancing between the competing rights*".[97] In contrast, a knowledge-based (and, more specifically, a notice-based) liability model can "*function in many cases as an appropriate tool for balancing the rights and interests of all those involved*",[98] although the imposition of stricter requirements can be acceptable in certain cases.[99] It thus appears that the 'middle way' approach embodied in the knowledge-based liability model is generally well suited to achieve the fair balance that EU fundamental rights law requires.[100]

F. Effectively tackling illegal user content

31 None of the aforementioned arguments should be taken to mean that the knowledge-based liability model does not having certain shortcomings. The shortcomings fall into two broad categories. The first one relates to the objective of effectively tackling illegal user content. It has already been seen that this objective continues to be highly relevant, considering the broad use made of the services in question to store and spread illegal content of all kinds.

32 The current EU system of knowledge-based liability leaves room for improvement in this regard because, first of all, it is ultimately voluntary. Any hosting service provider is free, legally speaking, to ignore a notice received, no matter how manifest the notified illegality and how precise and well-substantiated the notice may be. To be sure, national notice-and-action schemes may impose certain procedural requirements and most service providers will generally not ignore such notices because it would deny them the benefit of the liability exemption of Article 14 ECD. However, rogue operators – which do not even feel the need to give the *appearance* of being bona fide economic actors – may have little incentive to act upon such notices, especially if they are established outside the EU. In fact, the ECD, and therefore also its Article 14, only applies to online service providers established in the EU.[101] Providers based in third countries therefore cannot benefit from the liability exemption, no matter how expeditiously they act upon the notices that they may receive. The fact that such providers are established outside the EU can also make it difficult in practice to apply and enforce national liability rules. Thus, the paradoxical effect is that under the current system hosting service providers that facilitate the most damaging and blatantly illegal conduct of their users may be the least incentivised to act against such conduct.[102]

33 Second, the EU system, like any system that mostly relies on notices for service providers to obtain knowledge of and act against illegal content, is inherently dependent on notifying parties. The system will therefore only function well if there are parties that are willing and able to first detect and then notify (alleged) illegal content to the hosting service providers that store it (and take judicial action if need be). For most content causing 'private' harm that will generally not be an insurmountable problem. The monetary, reputational or emotional harm inflicted by intellectual property right infringements, defamation or invasions of privacy, as examples, means that the persons concerned gen-

an important role and the interference with those rights is serious, the EU legislature's discretion is reduced and the judicial review of the exercise of the discretion by EU courts is strict).

96 This may result not only from uncertainty relating to horizontal direct effects and the positive obligations mentioned above, but also from the 'quality' of the law requirement applicable under Art 52(1) Charter, which means inter alia that laws limiting the exercise of fundamental rights must be formulated with sufficient precision. See eg CJEU, *Chodor*, C-528/15, ECLI:EU:C:2017:213, 38.

97 ECtHR, *Magyar Tartalomszolgáltatók Egyesülete (MTE) v Hungary*, Appl no 22947/13 (2016), 89. See also ECtHR, *Magyar Jeti v Hungary*, Appl no 11257/16 (2018), 83 ("*objective liability may have foreseeable negative consequences on the flow of information on the Internet, impelling article authors and publishers to refrain altogether from hyperlinking to material over whose changeable content they have no control. This may have, directly or indirectly, a chilling effect on freedom of expression on the Internet*").

98 Ibid, 91.

99 ECtHR, *Delfi v Estonia* (n 67) (relating to a situation involving manifestly illegal hate speech).

100 See further Frosio and Geiger (n 58).

101 Recital 58 ECD.

102 Cf Commission, Impact assessment proposal TCO Regulation, SWD(2018) 408, 6 (noting that a large part of the service providers storing terrorist content are established outside the EU). On the other hand, see Commission, EU strategy for a more effective fight against child sexual abuse, COM(2020) 607, 2 (referring to reports indicating that, globally, most child sexual abuse material is hosted in the EU).

erally have every interest in actively trying to have the content taken down. That is often different, however, for content causing 'public' harm – that is, illegal content that primarily affects certain groups or society as a whole, rather than specific individuals. Think of terrorist content, child sexual abuse material or certain forms of racist or xenophobic speech. Of course, under the EU system any user remains free to notify such content when he or she encounters it, and some users certainly do so. However, ordinary users will generally not make an elaborate effort to this effect and their notifications are not always very helpful.[103] Other parties have stepped in to try to close the resulting 'enforcement gap'. Think, for instance, of non-governmental organisations dedicated to tackling child sexual abuse material by notifying it to service providers. However, whilst the activities of such organisations are undoubtedly important, their means are often limited and not evenly distributed.[104] Europol and certain national law enforcement authorities essentially do the same thing in relation to terrorist content online. However, such activities are not uncontested and may not be sufficient.[105] All this means that some of the worst and most harmful types of illegal user content may not be tackled in a sufficiently effective manner.

34 Third, the type of redress available in the context of the notice-and-action system for which the knowledge-based liability exemption provides the basis is limited to the removal of (or the disabling of access to) illegal user content. Removal is obviously helpful in addressing the immediate problem. However, in practice, the content in question may already have been spread further, or the same or other users may simply re-upload the removed content.[106] That naturally reduces the practical effectiveness of the removal. As the ECD stands, hosting service providers are not legally incentivised – let alone obliged – to try to prevent such further spreading or re-uploading of illegal content from happening. In other words, there is no 'notice-and-*stay*down' mechanism. More generally, the system established by the ECD does not encourage or oblige hosting service providers to make any structured effort to address the problem of illegal content provided by their users.[107] At EU level no provision has been made either for measures aiming to hold users who provide illegal content accountable, such as rules requiring hosting service providers to provide, upon justified requests, information about those users, or to bar those users from using their services.[108] The current EU system is, one could say, purely focused on combatting the symptoms (illegal content) rather than addressing those at the root of the problem (users providing illegal content).

35 In many ways, the shortcomings outlined above are related to the knowledge-based liability system's origin and nature. As pointed out earlier, the EU system was inspired by the US system laid down in Section 512(c) DMCA. The First Amendment to the US Constitution leaves the US legislature relatively little scope to regulate speech-related matters. This is one of the reasons why when enacting the DMCA, the US legislature decided to *encourage* but not legally *require* the tackling of illegal content, by offering the services providers concerned that meet certain conditions a 'safe harbour' (namely, the liability exemption).[109] From a European viewpoint,

103 See eg Internet Watch Foundation, Annual Report 2018, 2019, 18 (stating that only 28% of reports about alleged child sexual abuse material were accurate); T Wischmeyer, 'Making social media an instrument of democracy', (2019) *European Law Journal* 25, 176 (noting that, in the first six months of 2018, large hosting service providers found only between 11 and 27% of users' complaints submitted under the German NetzDG (*Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken*; Network Enforcement Act) justified).

104 See Wilman (n 13), 280-281 (with further references).

105 As regards the activities not being sufficient, see Commission, Impact assessment proposal TCO Regulation, SWD(2018) 408, 12-13. The activities are not uncontested because some consider it inappropriate for public authorities to use the notice-and-action mechanism, in particular where user content is notified for alleged violations of the providers' terms and conditions rather than alleged violations of the applicable law. Cf European Parliament, Legislative resolution on the proposal for a Regulation on preventing the dissemination of terrorist content online, P8_TA(2019)0421 (suggesting deleting the parts of the Commission proposal for the TCO Regulation intended to facilitate the submission and processing of these particular kinds of notices, known as 'referrals').

106 Cf CJEU, *Facebook Ireland* (n 20), 36 ("*Given that a social network facilitates the swift flow of information stored by the host provider between its different users, there is a genuine risk that information which was held to be illegal is subsequently reproduced and shared by another user of that network*").

107 See also para 46 below (explaining that the argument is sometimes made that the current EU system does, in fact, the very opposite - that is, *dis*couraging such efforts, in view of the risk that hosting service providers undertaking such voluntary activities might be deemed 'too active' to be able to benefit from the liability exemption).

108 Cf Art 15(2) ECD (indicating that the matter is essentially left to each Member State).

109 M Sag, 'Internet safe harbors and the transformation of copyright law', (2018) *Notre Dame Law Review* 93, 513; W Seltzer, 'Free speech unmoored in copyright's safe harbor: chilling effects of the DMCA on the First Amendment, (2010) *Harvard Journal of Law & Technology* 24, 176. Something similar applies in respect of Section 230 CDA; see Kosseff (n 37), 74.

this is a somewhat unusual legislative technique. Normally, the EU legislator lays down certain legal requirements which are then enforced principally under the administrative (or criminal) law of the Member States.[110] In addition, as also noted earlier, the DMCA is focused solely on copyright-infringing content. Copyright is principally an 'individual' right. It is, moreover, a right that can represent a considerable monetary value. That means that a 'supply' of notifying parties (and, by extension, parties that may bring actions for injunctions or damages if their notices are not acted upon) is virtually ensured. As has been seen, that cannot be taken for granted in relation to other types of illegal content that the EU system – unlike the DMCA – also covers, especially not where it concerns illegal content causing 'public' harm.

36 More fundamentally, the notice-and-action model is meant as a sort of 'first aid':[111] a quick, inexpensive and uncomplicated (as compared to judicial proceedings) way of getting rid of illegal user content. In many respects the model achieves that objective fairly well.[112] As noted earlier, submitting a notice is generally easy and inexpensive, and it can lead to swift removal. However, precisely because of the emphasis on informality, affordability and speed – and most of all the absence of a truly objective and impartial arbiter – the type of redress available is limited. That holds true especially for the current EU system, which is purely focused on removal. The DMCA, in contrast, provides for complementary requirements, including for the service providers concerned to disclose information on users allegedly involved in unlawful activities upon request and to operate a repeat infringer policy.[113] Experience in the US shows that the imposition of such requirements in the context of a system of simplified and 'privatised' enforcement tend to raise complex questions, both of principle and practical implementation.[114] This is unlikely to be different in the EU. Think of challenges in terms of ensuring compliance with the requirements resulting from the Charter and from secondary EU law, such as the General Data Protection Regulation[115] (GDPR) and the prohibition of general monitoring or active fact-finding obligations of the ECD.[116] While important to ensure that illegal content is effectively tackled, it is doubtful whether other remedies should be provided for systems such as the ones at issue here. Arguably, such complex questions cannot be properly dealt with by means of 'first aid', but rather call for the involvement of a specialist – that is, a court or an independent administrative authority.

G. Protecting users' rights and interests

37 The second category of shortcomings of the EU's current knowledge-based liability system consists of the risks it creates for the rights and interests of the users of hosting services. The risks referred to here relate not to the dissemination of illegal content, but rather to the measures that hosting service providers may take to tackle such content. The 'bias towards takedown'[117] that is inherent in any system of this kind is of particular importance in this regard. The bias results from the unequal incentives for service providers when they have to decide whether or not to remove user content when its legality has been called into question. As touched upon earlier, the decision *not* to remove such content can have serious legal consequences. Most notably, it may lead to damages claims, but potentially also liability under criminal law. The decision to *remove* the content in question, by contrast, tends to have only limited consequences for hosting service providers. The legal risks relating to such a decision are generally limited. That is because the monetary value at stake will often be modest. The users concerned are therefore unlikely to sue and, even if they do, they might struggle to prove that they suffered serious

110 That does not mean, of course, that under EU law there is no scope to claim damages for violations of that law. The point is rather that damages claims are generally not the *principal* enforcement mechanism.

111 S Bar-Ziv and N Elki-Koren, 'Behind the scenes of online copyright enforcement: empirical evidence on notice & takedown', (2017) *Connecticut Law Review* 50, 383.

112 See eg Kuczerawy, 'The power of positive thinking' (n 90), 228–229 (stating that notice-and-action systems provide relief "*far quicker than the relief typically provided by the judiciary*"); Riordan (n 36), 64 (observing that notice-and-action systems tend to be effective, cheap and rapid).

113 See Section 512(h) and (i) DMCA, respectively.

114 See Wilman (n 13), 140-141 and 150-152, respectively (explaining that the above requirements raise, among other things, critical questions as to the possibility to address the matters without the involvement of a court as well as the many uncertainties left by the relevant provisions of US law).

115 Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, [2016] OJ L 119/1 ('GDPR').

116 Art 15(1) ECD.

117 Urban et al (n 3), 126.

and quantifiable damage. In addition, hosting service providers tend to contractually limit or exclude their liability towards their users for these kinds of decisions.[118]

38 It is true that non-legal considerations should also be taken into account. Removal decisions that are unjustified (or *perceived* as unjustified) can result in angry users and negative publicity, for example. The latter seems an especially relevant consideration for many hosting service providers. This could make them hesitant to remove user content. Nonetheless, such considerations are counter-balanced by certain other non-legal factors. Think of negative publicity that may result from the decision not to remove contested content, the 'stickiness' of many of the services in question (resulting from the effort involved in migrating to another service), the network effects benefitting many of the service providers and the lack of transparency as to their content removal policies and decisions. The chances of users leaving on a significant scale over contested content removal decisions may therefore be rather limited. In view of the often large quantities of user content stored, the attractiveness and profitability of hosting services is generally unlikely to suffer too much from the removal of a few – or even quite a few – individual items of allegedly illegal user content.[119]

39 Furthermore, other than in cases of manifest illegality, hosting service providers may well struggle when seeking to determine the legality of specific items of user content that they store. To be able to do so, one generally needs to know the relevant *factual* context. For example, whether a certain allegation is true (in cases of possible defamation), or whether certain material is disseminated with the consent of the persons involved (in cases of possible violations of privacy or intellectual property rights). This can be hard for the providers to determine. Moreover, the *legal* assessment is often not straightforward either. For example, it can be challenging to determine whether a given item of user content not just reports on certain terrorist activities but glorifies them, or whether a statement is not just offensive or ironic but instead constitutes a prohibited racial slur. Extra complexity is added by the fact that the laws of the Member States still tend to differ considerably despite being harmonised in some fields and to some extent.[120] Even determining which law applies in the first place may not be straightforward in the online sphere. Working all this out tends to be complex and (therefore) costly for service providers. It is often not only legally safer, but also easier and cheaper for them simply to remove user content that could, potentially, be illegal.

40 Thus, hosting service providers may well decide to remove the user content in question, especially in 'grey area' cases – of which there are many in practice. That means that it is unavoidable that user content that is *not* actually illegal is removed as well. This naturally has a negative effect on users' possibilities to lawfully express themselves and gather information online. In this connection, it should be recalled that a system relying on the submission of notices offers aggrieved parties a low-threshold manner to enforce their rights. The threshold is so low, in fact, that risks of mistakes and abuse exist. While hard to assess and quantify (largely due to the lack of transparency), research conducted in the US indicates that these risks are real and should be taken seriously.[121] Some unjustified removals result from honest mistakes, which may be hard to avoid. Yet, it appears that grossly erroneous or outright abusive notices, for instance to supress criticism or disadvantage competitors, are not uncommon.

118 Ibid, 16. See also Sag (n 109), 535.

119 Cf E Goldman, 'Why Section 230 is better than the First Amendment', (2019) *Notre Dame Law Review* 95, 41 (noting that online service providers rarely make a lot of money from any single item of user content); Balkin, 'Free speech is a triangle' (n 12), 2017 (noting that denying access to small numbers of speakers does not damage the providers' business model).

120 That relates not only to secondary EU law, but also eg the freedom of expression. See CJEU, *Google v CNIL*, C-507/17, ECLI:EU:C:2019:772, 67.

121 See also Urban et al (n 3) (reporting on two studies finding that 31 respectively 70% of the takedown notices assessed raised substantive questions; whilst also noting that nearly every intermediary and several copyright holders interviewed expressed concern about the takedown of non-infringing content); D Seng, 'Who watches the watchmen? An empirical analysis of errors in DMCA takedown notices', 2015, available via <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2563202> (finding error rates of up to 8,3% in relation to 'functional' requirements, such as adequately specifying a takedown request, while also finding misidentification of the copyright holder and requests to remove content which is no longer available); J Urban and L Quilter, 'Efficient process or chilling effects: takedown notices under Section 512 of the Digital Millennium Copyright Act', (2006) *Santa Clara High Technology Law Journal* 22, 621–693 (finding that at least a third of the assessed takedown notices contained major flaws, notably as regards the underlying claims). See also Bar-Ziv and Elki-Koren (n 111), 344 (regarding the use of the notice and takedown procedure in accordance with Section 512 DMCA in Israel, finding that the procedure offers "*fertile ground for misuse*").

41 There are of course certain relevant differences between the legal systems in the EU and the US. For example, unlike in the US, punitive or statutory damages are not commonly provided for in the EU. That means that the financial risks associated with a provider's decision not to remove user content – in view of the risk of damages claims – may be more limited. On the other hand, in the EU it is in principle possible for *anyone* to submit a notice that might lead to knowledge on the side of the hosting service provider.[122] In the US, this possibility is reserved for what will generally be more or less professionally operating actors (namely, copyright holders), who are legally required to state their good faith belief that the use of the content in question is not authorised.[123] Furthermore, the fact that, unlike in the US, there are at present no binding EU rules on notice-and-action procedures enlarges the uncertainty and thus the 'grey area' referred to above, in which service providers may well remove allegedly-yet-not-manifestly illegal content just to be on the safe side. As importantly, the absence of such EU rules on notice-and-action procedures means that the availability of the principal safeguard of the US system to protect users' rights and interests – the so-called counter-notice procedure[124] – is not legally guaranteed. Such counter-notice procedures allow affected users to contest the claims of infringement made in relation to the content that they provided. It is true that the US counter-notice procedure is little used in practice.[125] That is likely due in part to the design of the procedure.[126] In any event, this fact does not alter the principal point that it is important to afford users a realistic opportunity to defend their interests if not before, then at least immediately after the removal of their content.

42 In addition, it has increasingly become clear over the past years that risks to the rights and interests of users also result from the content moderation measures that hosting service providers take to tackle content that may not be *illegal*, but that is against their *terms of service*. Providers' terms and conditions are often stricter than the law.[127] They may preclude, for instance, the provision of content containing nudity, offensive expressions or controversial political views. The decisions by Facebook and Twitter to suspend (then) President Trump's account, referred to earlier, illustrate both how powerful some of these providers are and how controversial their decisions can be.[128] In principle, providers are free to set and enforce such contractual rules, even in respect of content that may be perfectly legal, as an exercise of their freedom of contract that is part of the freedom to conduct a business.[129] Nonetheless, this development implies that the challenge is not only to ensure that 'what is illegal offline is also illegal online', as the adage has long been.[130] The challenge is also, and increasingly, to ensure that, conversely, what is *not* illegal offline is not 'illegal' (contractually prohibited) online either. Not, at least, where the contractual prohibitions unduly restrict users' freedom of expression and information or where the manners in which those prohibitions are enforced are arbitrary, excessive or not transparent.

122 Considering the 'horizontal' nature of Art 14 ECD and the fact that neither this article nor the case law relating thereto available to date contains any restriction in this respect.

123 Section 512(c)(3)(A) DMCA.

124 Section 512(g)(2) DMCA.

125 See ICF, Grimaldi and 21c Consultancy, 'Overview of the legal framework of notice-and-action procedures in Member States', Study for the Commission, 2018, 119 (reporting on 'counter-notice rates' – that is, the percentage of removals that lead to counter-notices – of often less than 1%, although for some online service providers the rate can be over 10%). See also Sag (n 109), 504 and 535; E Asp, 'Section 512 of the Digital Millennium Copyright Act: user experience and user frustration', (2018) *Iowa Law Review* 103, 770–773; Urban et al (n 3), 44 and 118 (all pointing to the limited use made of the DMCA's counter-notice procedure).

126 Wilman (n 13), 160.

127 See J Balkin, 'Free speech in the Algorithmic Society: big data, private governance and new school speech regulation', (2018) *University of California, Davis* 51, 1194–1195 ("*Online communities enforce speech norms that protect far less expression than the corresponding obligations of government under the American First Amendment*"); D Keller, 'Internet platforms: observations on speech, danger, and money', Hoover Institution Essay Aegis Series Paper No. 1807, 2018, 4 ("*Most well-known platforms take down considerably more content than the law requires*"); Gillespie (n 37), 34 ("*In most cases [online service providers'] ceaseless and systematic policing cuts much, much deeper than the law requires*").

128 See para 1 above. Note that the question whether President Trump acted illegally seems only of secondary importance in the context of this discussion; the reason for taking the suspension decisions was that he violated the providers' (broadly drawn) terms of service.

129 Cf CJEU, *Sky Österreich*, C-283/11, ECLI:EU:C:2013:28, 42–43.

130 Eg Commission, Tackling illegal content online: towards an enhanced responsibility of online platforms, COM(2017) 555, 2.

H. DSA proposal

I. Liability regime

43 The Commission's decision to retain, in the DSA proposal, the knowledge-based liability model for hosting services providers seems understandable in view of the foregoing, even if the reasons for doing so may perhaps not have been very well explained. Indeed, as noted, from a legal viewpoint the Commission arguably had little scope to opt for a fundamentally different approach.[131] This has to do, in particular, with the suitability of this model to achieve the required fair balance between conflicting fundamental rights. More specifically, the need to avoid 'chilling effects' on users' freedom of expression appears to have also played a role in the Commission's decision-making.[132] Considering the EU legislator's seemingly reduced discretion *not* to act in situations where fundamental rights may be infringed, the DSA proposal could be seen as reflecting not only a political and policy choice to act, but to some extent also a legal imperative to do so under EU fundamental rights law. In any event, it is noticeable that whilst the ECD only makes a few mentions of fundamental rights in its recitals, the protection thereof has been 'upgraded' to the very objective of the DSA proposal.[133] In line with that objective, the relevant fundamental rights are not only concretised in numerous specific legal obligations for hosting services providers and corresponding rights for users; in certain cases the proposal also requires the providers to take fundamental rights as such into account.[134]

44 The decision to retain the knowledge-based liability model is certainly not a purely legal one, though. The broad support for the key features (although not necessarily all specific aspects) of the current model is likely to have played a role, too. Such support is evident, for instance, from the public consultation,[135] academic studies[136] and the position taken by the European Parliament shortly before the publication of the DSA proposal.[137] The fact that the existing liability exemption would be 'transplanted' from the ECD to the new DSA Regulation could help address one of the main points of criticism: the diverging ways in which the current rules are understood and applied across the EU. Unlike directives, regulations do not require transposition into national law but instead apply directly and in the same way across the entire EU.

45 When zooming in on Article 5 DSA proposal, which is to replace current Article 14 ECD, it becomes apparent that in this respect the proposal seeks to change relatively little. The former is largely a copy of the latter. Drafting changes are limited and can mostly be explained by the fact that the DSA is a regulation, not a directive. Even the corresponding recitals of the DSA proposal echo those of the ECD to some extent, although they also provide certain clarifications. While helpful, these clarifications are hardly spectacular. The relevant recitals of the DSA proposal mostly recall case law of the Court of Justice relating to the current law or address

131 See section E above (on relevant developments in EU fundamental rights law).

132 See Commission, Explanatory memorandum DSA proposal, COM(2020) 825, 12; Commission, Impact assessment DSA proposal, SWD(2020) 348, 19.

133 Art 1(2) DSA proposal.

134 See Art 12(2) (requiring hosting service providers to take due account of the fundamental rights of users when applying the restrictions contained in their terms and conditions) and Art 26(1)(b) DSA proposal (requiring certain very large hosting service providers to assess significant systematic risks relating to their service provision inter alia for the exercise of certain fundamental rights). As such, the DSA proposal can be seen as a further step in the process of 'horizontalisation' of EU fundamental rights law, be it that the horizontal effects stem not directly from the Charter but rather arise via secondary EU law.

135 Commission, Impact assessment DSA proposal, SWD(2020) 348, 26 ("*On the topic of the liability of intermediaries, a large majority of stakeholder groups broadly considered the principle of the conditional exemption from liability as a precondition for a fair balance between protecting fundamental rights online and preserving the ability of newcomers to innovate and scale*").

136 See eg Frosio and Geiger (n 58), 4 (arguing that, despite shortcomings, the ex post knowledge-and-takedown mechanism of the ECD remains fully justified and pertinent from a fundamental rights perspective); A De Streel and M Husovec, 'The e-Commerce Directive as the cornerstone of the internal market: assessment and options for reform', Study for the IMCO Committee of the European Parliament, 2020, 47 (arguing that, given its success, the liability exemption of Art 14 ECD should be preserved); J Nordemann, 'The functioning of the internal market for digital services: responsibilities and duties of care of providers of digital services', Study for the IMCO Committee of the European Parliament, 2020, 46 (arguing that, despite being almost 20 years old, Art 14 ECD does not seem outdated); Urban et al (n 3), 28 (answering the question whether the notice-and-action model is still relevant in view of the many changes over the past two decades with "*a resounding 'yes'*").

137 See eg European Parliament, Resolution on the Digital Services Act: improving the functioning of the single market, 20 October 2020, P9_TA(2020)0272, 57 (calling maintaining the liability regime of Art 14 ECD "*pivotal*").

relatively uncontroversial matters.[138] However, on the following three main points the DSA proposal would mark a more substantial change as compared to the current liability system applicable to hosting services set out in the ECD.

46 The first change, which consists of several elements, has to do with the scope of the proposed new regime. To begin with, the DSA, and therefore also the liability exemption contained in its Article 5, would apply to *all* providers that offer relevant services in the EU.[139] That means that the question whether the providers are based inside or outside the EU would no longer be relevant.[140] That is a logical yet important change, which, besides contributing to a level playing field, should help better protect EU users against illegal content.[141] In addition, the DSA proposal's recitals state that the liability exemption does not apply to hosting service providers that play an active role of such a kind as to give them knowledge of or control of the content that they store for their users.[142] This is a restatement of existing case law and thus not a substantial change.[143] It is important nonetheless, since the degree to which such providers can play an active role without losing the benefit of the liability exemption is an issue that has led to confusion and debate.[144] Retaining and codifying (although only in a recital) the standard developed by the Court of Justice improves clarity and implies that the clarifications resulting from over a decade worth of case law on the matter are retained. However, it also means that some uncertainty remains, especially when it comes to the *application* of the standard in specific cases.[145] Yet another (although related) element is the introduction of a so-called 'Good Samaritan' clause. The clause is meant to address concerns that EU law as it stands discourages hosting service providers from undertaking voluntary activities to tackle illegal content, because doing so could mean that they are seen as 'too active' to qualify for the liability exemption.[146] The clause indicates essentially that no such conclusion is to be drawn.[147] This proposed new rule is hardly surprising given that it is in line with earlier guidance provided by the Commission,[148] although opinions on the need for introducing it differ and some might find the protection that the rule would afford still insufficient.[149]

138 Eg, Recitals 17, 18, 19 and 22 DSA proposal state that the present rules are about exemption from liability and not about liability itself: that the liability exemption is 'horizontal' in nature; that it does not apply in respect of liability relating to the providers' own content; that the rules are activity-based and not provider-based; and that service providers can obtain knowledge of illegality in particular through own-initiative investigations and third-party notices. As regards the situation under current law, including references to the relevant case law, see section B above.

139 Art 1(3) DSA proposal. See also Art 2(d) thereof (defining the term 'offering services in the Union').

140 It is only relevant in relation to Art 11 DSA proposal (requiring providers based in third countries to designate legal representatives within the EU to facilitate enforcement).

141 Recital 7 DSA proposal.

142 Recital 18 DSA proposal.

143 See in particular CJEU, *L'Oréal v eBay* (n 19), 113. See further para 7 above.

144 See eg Commission, Impact assessment DSA proposal, SWD(2020) 348, 31 (pointing to diverging national case law); European Parliament Research Service, 'Reform of the EU liability regime for online intermediaries', 2020, 5 (arguing that the Court of Justice's current case law lacks clarity); Van Hoboken et al (n. 21), 33 (referring to confusion and complexity relating to the scope of Art 14 ECD's liability exemption).

145 See para 8 above.

146 See Commission, Impact assessment DSA proposal, SWD(2020) 348, 33. See further also J Barata, 'Positive intent protections: incorporating a Good Samaritan principle in the EU Digital Services Act', 2020, available via <https://cdt.org/wp-content/uploads/2020/07/2020-07-29-Positive-Intent-Protections-Good-Samaritan-principle-EU-Digital-Services-Act-FINAL.pdf>, 12.

147 Art 6 DSA proposal. Recital 25 indicates that the voluntary activities must have been undertaken in good faith and in a diligent manner. Note that Art 6 differs from the 'Good Samaritan' protection afforded under Section 230(c)(2)(A) CDA especially in that the article does not entail a liability exemption in its own right, covers only activities aimed at tackling *illegal* user content and covers not only voluntary but also *legally required* activities of that kind.

148 See in particular Recital 26 Illegal Content Recommendation. Cf CJEU, *YouTube* (n. 20), 109.

149 See eg C Angelopoulos, 'On online platforms and the Commission's new proposal for a Directive on Copyright in the Digital Single Market', 2017, available via <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2947800>, 43–44; Nordemann (n 132), 10 (arguing in favour respectively against introducing such a clause). See eg also Van Hoboken et al (n 21), 42 (arguing in relation to the Commission's earlier guidance that the approach does not protect providers against liability in case they failed to detect and remove content despite having taken certain voluntary measures to that end); S Stalla-Bourdillon, 'Internet intermediaries as responsible actors? Why it is time to rethink the e-Commerce Directive as well', in M Taddeo and L Floridi (eds), *The Responsibilities of Online Service Providers* (Springer 2017), 290 (arguing that not an express 'Good Samaritan' clause is required, but rather a clause protecting intermediaries where they in good faith refuse to takedown user content).

47 The second change is the proposed express disapplication of the notice-based liability exemption for hosting service providers in certain circumstances involving claims based on consumer protection law. The new rule, contained in Article 5(3) DSA proposal, would apply only to a particular subcategory of hosting service providers: online platforms allowing consumers to conclude distance contracts with traders.[150] Under the rule it is not so much the latter's (objective) knowledge of or control over the user content in question that is decisive, as is the case under the 'ordinary' liability exemption of Article 5(1). It is rather the (subjective) impression of the consumer as to whether the content (or the 'underlying' product or service to which the content relates) is provided by the service provider that is decisive for the question whether the liability exemption can be relied on.[151] The rule aims to improve the protection of consumers when they engage in intermediated commercial transactions online.[152] Whilst certainly novel when considered from the viewpoint of the current liability system, it brings to mind case law of the Court of Justice issued in the context of EU consumer protection law.[153] Although some may fear that the proposed rule could undercut the certainty that the conditional liability exemption is meant to provide, others may feel it does not go far enough in better protecting consumers.[154]

48 The third change consists of the introduction of EU rules on notice-and-action mechanisms. As noted earlier, the ECD provides the basis for a system of notice and action. But when adopting this directive the EU legislator decided to leave it to self-regulation to work out the procedural arrangements on the sending and processing of notices, whilst allowing Member States to set national rules on these matters.[155] Such self-regulatory and national rules have been established only to a limited extent, however, and where they exist, they diverge.[156] Article 14 DSA proposal would require hosting service providers to establish mechanisms that allow individuals or entities to notify them about allegedly illegal content. The mechanisms would have to be easy to access, user-friendly and allow for the submission of notices exclusively by electronic means. Importantly, the notices are to relate to *specific* items of content – broad, general notices could therefore not be submitted under these mechanisms.[157] Article 14 incorporates the standard set by the Court of Justice that notices should be sufficiently precise and adequately substantiated for them to be able to give rise to knowledge within the meaning of the liability exemption.[158] The article goes into further detail by listing the elements that notices should contain, including the reasons why the notifier thinks the content is illegal, its name and

150 Cf Art 2(h) DSA proposal (defining the concept of 'online platform' essentially as a hosting service provider which not only stores but also stores user content). Cf also Art 2(j) DSA proposal (defining the term 'distance contract'). In practice, one should probably mainly think of e-commerce platforms.

151 Although the test under Art 5(3) DSA proposal is objectivised, in the sense that the belief of an average and reasonably well-informed consumer is decisive. See also Recital 23. Pursuant to Art 5(3), the consumer's belief must, moreover, be based on the acts or omissions of the service provider, such as the manner in which it presents the content in question.

152 Recital 23 DSA proposal.

153 See in particular CJEU, Case C-149/15, *Wathelet*, ECLI:EU:C:2016:840, 41. For a suggestion somewhat similar to Art 5(3) DSA proposal, see De Streel and Husovec (n 132), 48.

154 See eg C Busch, 'Rethinking product liability rules for online marketplaces: a comparative perspective', 2021, available via <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3784466>, 27 (criticising the DSA proposal for not taking a clear stance on whether and when online marketplaces are subject to product liability); C Cauffman and C Goanta, 'A new order: the Digital Services Act and consumer protection', 2021, available via <https://www.researchgate.net/publication/348787835_A_New_Order_The_Digital_Services_Act_and_Consumer_Protection>, 9 (questioning whether Art 5(3) DSA proposal would offer consumers sufficient protection).

155 See in particular Art 14(3) and 16 DSA proposal. See also Commission, First report on the ECD, COM(2003) 702, 14; E Crabit, 'La directive sur le commerce électronique: le projet "Méditerranée"', (2000) *Revue du droit de l'Union européenne* 4, 814; Commission, Proposal ECD, COM(1998) 586, 29. In 2018, the EU legislator inserted a (rather rudimentary) requirement of this kind in Art 28b(3)(d) Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services, [2010] OJ L 95/1 (as amended by Directive (EU) 2019/1808) ('AVMSD').

156 Commission, Impact assessment DSA proposal, SWD(2020) 348, 31-32 (and Annex 6 thereto). See also Wilman (n 13), 48.

157 See also Recital 40 DSA proposal (indicating that it should be possible to notify *multiple* specific items of allegedly illegal user content). Cf CJEU, *YouTube* (n. 20), 112-113.

158 Art 14(2) and (3) DSA proposal. See CJEU, *L'Oréal v eBay* (n 19), 122 (implying that insufficiently precise or inadequately substantiated notices do not lead to knowledge within the meaning of Art 14 ECD). See also CJEU, *YouTube* (n. 20), 116 (adding that notices must contain sufficient information to enable the service provider to satisfy itself, without a detailed legal examination, that the content in question is illegal and that removing that content is compatible with freedom of expression).

e-mail address and a confirmation of its good faith belief that the notice is accurate and complete.[159] Service providers are to process notices in a timely, diligent and objective manner.[160] Article 14 does not establish a counter-notice procedure; the matter is covered by other provisions of the DSA proposal, notably those on the provision of information to users in case of removal and on providers' internal complaint-handling systems.[161] The proposed new rules on notice-and-action mechanisms should contribute to the aim of tackling illegal content more effectively, whilst also better protecting users against unjustified removals.[162] The rules are broadly in line with the guidance contained in the Commission's Illegal Content Recommendation of 2018. Most will probably welcome them.[163] That does not mean, however, that there is no scope left for debate. Opinions could differ, for instance, as to whether the right balance is struck between, on the one hand, ensuring that notices are precise and substantiated enough to be actionable and that abuses of the mechanisms are prevented and, on the other hand, not deterring 'ordinary' users from using the mechanism by imposing overly demanding or 'threatening' requirements.[164] Another question is whether notices that do not contain all elements listed in Article 14 could in certain cases still lead to knowledge within the meaning of Article 5.

II. Effectively tackling illegal user content

49 In light of the above discussion regarding the shortcomings of a knowledge-based liability model, the question arises of how, beyond liability-related matters strictly speaking, the DSA proposal should be assessed. When it comes to measures aimed at tackling illegal user content more effectively, what is *not* proposed is perhaps most noticeable. In particular, whilst the DSA proposal retains the prohibition on general monitoring obligations,[165] it contains no general requirement for hosting service providers to detect and tackle illegal user content on their services in a proactive manner. The latter is an important change as compared to certain other measures recently proposed and adopted in this domain. Most notably, Article 17 Copyright in the Digital Single Market (CDSM) Directive,[166] the Commission's proposal for the Terrorist Content Online (TCO) Regulation[167] and the Illegal Content Recommendation[168] all contain provisions on proactive measures. It is further noticeable that the DSA proposal does not contain any rules that would empower national courts or administrative authorities to issue injunctions involving measures

159 Art 14(3) DSA proposal. Strictly speaking, the provision does not state that notices *must contain* such elements; rather, it states that service providers are to *facilitate* the submission of notices containing such elements. This reflects the fact that the provision imposes obligations on the providers, not on the notifying parties.

160 Art 14(6) DSA proposal. This requirement comes on top of, and appears to apply independently from, the 'expeditious action' condition set as part of the liability exemption of Article 5. Notices submitted by 'trusted flaggers' – such as the aforementioned organisations combatting child sexual abuse or Europol – are, moreover, to be treated with priority (Art 19 and Recital 46 DSA proposal).

161 Art 15 and 17 DSA proposal, respectively. See also para 55 below (discussing redress-related provisions of the DSA proposal). This approach implies that, unlike under Section 512(g) DMCA, the counter-notice procedure is not crafted as a condition attached to a separate liability exemption for removal decisions that turn out to be unjustified.

162 As explained in para 41 above, the latter results especially from the reduction of uncertainty on the side of the service providers ('grey area') and from the strengthened redress possibilities of affected users.

163 Given the many calls made over the years for introducing EU rules on notice-and-action procedures (see n 90). See also European Parliament (n 133), 52 (calling for harmonised rules on notice-and-action mechanisms); Commission, Impact assessment DSA proposal, SWD(2020) 348, 42 (noting that, in response to the public consultation, the general public, online intermediaries and civil society organisations especially advocated for a harmonisation of notice-and-action procedures across the EU).

164 In this regard, see also Art 20 DSA proposal (requiring providers to suspend the processing of notices by parties that frequently submitted manifestly unfounded notices). Note that, in comparison, Section 512(c)(3)(A) and (f) DMCA are more demanding where it comes to the elements that notices must contain and more 'threatening' in view of the liability in damages for 'misrepresentations' in notices for which it provides.

165 Art 7 DSA proposal (essentially restating Art 15(1) ECD).

166 Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market, [2019] OJ L 130/92 ('CDSM Directive').

167 Commission, Proposal for a Regulation on preventing the dissemination of terrorist content online COM(2018) 640 (see in particular its Art 6, proposing introducing an obligation for hosting service providers to take certain proactive measures aimed at tackling terrorist content).

168 See Points 18, 36 and 37 Illegal Content Recommendation (encouraging hosting service providers to take proactive measure where appropriate and in any event in relation to terrorist content, including to prevent the resubmission of removed terrorist content).

such as staydown obligations or the provision of information on users suspected of illegal conduct, or temporarily barring infringers from using the services in question. This despite the fact that, notwithstanding certain challenges, there is no need to think that such forms of injunctive relief are legally precluded per se.[169] Apart from increasing effectiveness in terms of tackling illegal user content, they could help reduce the current heavy reliance on a system of 'privatised' enforcement, with which many feel uneasy.[170] Yet under the DSA proposal – as under the ECD – injunction-related issues would largely be left to be regulated under national law.[171]

50 The DSA proposal's comparatively modest approach on the matters discussed in the previous paragraph likely has to do with recent experiences showing how polemic possible EU rules on proactive measures, staydown obligations and injunctions can be.[172] Take the 2019 reform of EU's regime on the liability of certain service providers for online copyright infringements, which resulted in Article 17 CDSM Directive. Under the article service providers are, inter alia, to make 'best efforts' to ensure the unavailability of copyright-protected works and to prevent them from being re-uploaded after removal.[173] The reform was extremely controversial.[174] Probably largely because of the starkly diverging views, the new rules are seen as complex and unclear at best, if not plain inconsistent.[175] A case contesting their compatibility with the fundamental right to freedom of expression is currently pending.[176] Debates about the Commission's guidance on Article 17 CDSM Directive show that the matter remains highly sensitive.[177] Although generating somewhat less attention, the TCO Regulation, adopted in April 2021,[178] similarly generated strongly diverging views.[179] Its rules on

169 See eg CJEU, *Facebook Ireland* (n 20), 46 (on staydown obligations); CJEU, *L'Oréal v eBay* (n 19), 141 (on the suspension of the provision of services to users engaged in illegal conduct).

170 See European Parliament, Resolution on the Digital Services Act: adapting commercial and civil law rules for commercial entities operating online, P9_TA(2020)0273, G ("*delegating decisions regarding the legality of content or of law enforcement powers to private companies undermines transparency and due process*"). See eg also S Dusollier, 'The 2019 Directive on copyright in the digital single market: some progress, a few bad choices, and an overall failed ambition', (2020) *Common Market Law Review* 57, 1016; M Bassini, 'Fundamental rights and private enforcement in the digital age', (2019) *European Law Journal* 25, 186; Barata (n. 142), 10; Kuczerawy, *Intermediary liability and freedom of expression in the EU* (n 82), 5–6; K Kaesling, 'Privatising law enforcement in social networks: a comparative model analysis', (2018) *Erasmus Law Review* 12, 159–160.

171 See in particular Art 5(4) DSA proposal (echoing Art 14(3) ECD). Note that Art 8 and 9 DSA proposal provide for rules on orders addressed to hosting service providers to act against illegal content or to provide information, respectively. However, those rules do not actually *empower* national courts or administrative authorities to issue such orders, but rather set a framework within which any such powers attributed under national law (or other acts of EU law) are to be exercised. See also Recitals 29-33.

172 Cf also Commission, Impact assessment DSA proposal, SWD(2020) 348, 19 ("*The issue of the use of automated tools to automatically detect illegal content, services and goods is considered very controversial among respondents [to the public consultation]*").

173 Art 17(4)(b) and (b) CDSM Directive.

174 See C Angelopoulos and J Quintas, 'Fixing copyright reform: a better solution to online infringement', (2019) *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 10, 147 ("*The proposal [for the CDSM Directive] was controversial from the start. Almost every step of the legislative process was the subject of intense lobbying and debate*"). See also G Spindler, 'The liability system of Art 17 DSMD and national implementation: contravening prohibition of general monitoring duties', (2019) *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 10, 344; T Spoerri, 'On upload-filters and other competitive advantages for big tech companies under Article 17 of the Directive on copyright in the Digital Single Market', (2019) *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 10, 174 (both making similar statements).

175 See eg Dusollier (n 166), 1008 and 1010-1011 (describing Art 17 CDSM Directive as a "*monster provision*" and as "*a complex construction and the outcome of many political compromises*"); Angelopoulos and Quintas (n 170), 153 (stating that the rules "*create more questions than they answer*"); Husovec (n 3), 537 (describing the new system as "*a mechanism with too many moving parts*"). See also Joint Statement by the Netherlands, Luxembourg, Poland, Italy and Finland, Council doc. 7986/19, 15 April 2019, 1 ("*we feel that [the CDSM] Directive lack legal clarity, will lead to legal uncertainty for many stakeholders concerned and may encroach upon EU citizens' rights*").

176 CJEU, *Poland v European Parliament and Council*, C-401/19 (pending).

177 See eg 'Commission and Parliament in 'secret talks' on EU copyright directive', Euractiv, 12 February 2021; 'EU civil society says Commission's copyright guidance violates 'fundamental rights'', Euractiv, 15 September 2020. For the guidance, provided pursuant to Art 17(10) CDSM Directive, see Commission, Guidance on Article 17 of Directive 2019/790 on Copyright in the Digital Single Market, COM(2021) 288.

178 Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online, [2021] OJ L 172/79 ('TCO Regulation').

179 See eg EU Agency for Fundamental Rights, Opinion on the

proactive measures and on the issuance of removal orders were among the main bones of contention.[180] The situation does not seem fundamentally different in the US, where bitter disputes linger over recent and potential future updates of Section 512(c) DMCA and Section 230 CDA.[181] It therefore appears that any suggestion to introduce measures of this kind leads almost by definition to controversy. That being so, whilst some may be disappointed in the comparatively modest ambitions of the DSA proposal in this regard,[182] others may well welcome the approach as more balanced or politically realistic.

51 The comparatively modest approach when it comes to tackling illegal user content contained in the DSA proposal also reflects the fact that the DSA is conceived as horizontally applicable 'baseline' measure. The DSA Regulation is meant to complement sector- or content-specific acts, such as Article 17 CDSM Directive, the TCO Regulation and the Audiovisual Media Service Directive (AVMSD) as amended in 2018.[183] Precisely because these other acts tend to provide for specific – and more demanding – requirements, there is arguably less of a need for the DSA proposal to go into these issues.[184] At the same time, relying on these specific acts also means that the overall picture is not always consistent or self-evident. Is it entirely logical, for instance, that EU law provides for staydown-like requirements only in respect of copyright-infringing content?[185] Such content can cause serious damage, but few would probably argue that the damage is more serious than that caused by, for example, child sexual abuse material or terrorist content. One could also wonder why it is that only video-sharing platforms are required to take certain measures to tackle hate speech contained in audiovisual content uploaded by users.[186] These platforms and the audiovisual content that they disseminate for their users surely are an important part of the broader problem of online hate speech. But so are, it would appear, social media companies and the written texts that they disseminate for their users, for instance.[187]

52 Despite this, it would be wrong to conclude that the DSA proposal does not contain any measures at all that aim at tackling illegal user content more effectively. The proposal would, in fact, subject hosting service providers[188] to what could be called an EU-level duty of care to this effect. This does not

proposal for a Regulation on preventing the dissemination of terrorist content online and its fundamental rights implications, 2/2019; European Data Protection Supervisor, Formal comments on the proposal for a Regulation on preventing the dissemination of terrorist content online, 2019; J Van Hoboken, 'The proposed EU Terrorism Content Regulation: analysis and recommendations with respect to freedom of expression implications', Transatlantic Working Group, 2019; J Barata, 'New EU proposal on the prevention of terrorist content online: an important mutation of the e-commerce intermediaries' regime', Center for Internet and Society, 2018; E Coche, 'Privatised enforcement and the right to freedom of expression in a world confronted with terrorist propaganda online', (2018) *Internet Policy Review* 7, 1–17.

180 See in particular European Parliament (n 105) (suggesting reserving the power to issue removal orders only to the Member State of establishment of the service provider concerned and deleting all references to proactive obligations for hosting service providers).

181 As regards Section 512(c) DMCA, see eg US Copyright Office (n 8), 73 (noting a "*stark division of opinion*" between the main stakeholders). As regards Section 230 CDA, see in particular the amendment of Section 230 CDA adopted in 2018 through a law known as FOSTA (Allow States and Victims to Fight Online Sex Trafficking Act, incorporated in Section 230(e)(5) CDA). See E Goldman, 'The complicated story of FOSTA and Section 230', (2019) *First Amendment Law Review* 17, 279–293, 292 ("*FOSTA may be one of Congress' worst achievements in Internet regulatory policy*"). See also Kosseff (n 37), 272; D Citron and Q Jurecic, 'Platform justice: content moderation at an inflection point', Hoover Institute Essay, Aegis series paper No. 1811, 2018, 3; D Keller, 'SESTA and the teachings of intermediary liability', Center for Internet and Society, 2017 (all containing critical assessments of FOSTA).

182 See eg Nordemann (n 132), 30 and 42 (arguing for provisions on injunctions and staydown).

183 See n 155 (regarding the AVMSD and its amendment in 2018). On the interaction between the DSA proposal and Art 17 CDSM Directive, see further J Quintais and S Schwemer, 'The Interplay between the Digital Services Act and sector regulation: how special is copyright?', May 2021 (draft), available via https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3841606>.

184 See Art 1(5) and Recitals 9-11 DSA proposal (indicating that the DSA would "*complement, yet not affect*" said other acts).

185 Art 17(4) CDSM Directive.

186 Art 28b(1) AVMSD.

187 Art 1(aa) AVMSD defines the term 'video-sharing platform service' broadly, meaning that social media companies could in certain cases also be covered by the relevant rules. However, on the substance, the rules only apply to audiovisual material, not to written texts.

188 Note that most of the obligations mentioned here would in fact apply to a particular subcategory of hosting service providers, namely 'online platforms' (as defined in Art 2(h) DSA proposal). For reasons of consistency and simplicity, the general term 'hosting service provider' is nonetheless used here. Furthermore, references made to *very large* hosting service providers should be understood as references to very large online platforms within the meaning of Art 25 DSA proposal (setting the threshold at 45 million users in the EU).

only mean that mandatory (as opposed to ultimately voluntary) requirements for hosting service providers to take certain measures are introduced. It also marks a notable change as compared to the ECD in that the latter leaves it to the Member States to decide whether to impose such a duty under national law.[189] Three additional measures stand out, apart from the measures already mentioned (broadening the scope to also cover third country-based providers active in the EU; the new EU rules on notice-and-action mechanisms; the 'Good Samaritan' clause, which would not *oblige* but nonetheless *encourage* the taking of proactive measures to tackle illegal user content). First, the providers would be required to act against users who provide illegal content.[190] This is a sort of repeat infringer requirement. It implies that – at least to some extent – the focus is no longer solely on illegal content as such, but also on the users providing it. The DSA proposal seeks to address the aforementioned complexities that arise in this regard by limiting the obligation to content that is *manifestly* illegal and to users that *frequently* provide such content.[191] Providers would be required to assess that on a case-by-case basis and to set out their policies in this respect in their terms and conditions.[192] Second, the providers would be required to notify suspicions of certain serious criminal offences to the competent authorities.[193] Finally, very large providers would be obliged to annually assess any significant systemic risks stemming from their service provision, inter alia for the dissemination of illegal user content, and to take measures to mitigate any such risks.[194] These requirements are worded rather broadly, meaning their practical effects are somewhat uncertain. Nonetheless, they could play an important role in achieving the objective of tackling the type of illegal user content causing serious 'public' harm, mentioned earlier, in a more effective manner.

III. Protecting users' rights and interests

53 The DSA proposal's ambitions to better protect the rights and interests of EU users of hosting services – in particular to freely express themselves, to be able to access legitimate content and to be treated in a fair and transparent manner – are by no means modest. Indeed, when assessed at the general level it seems fair to say that this is the DSA's primary focus. This entails a notable change of approach as compared to earlier acts such as Article 17 CDSM Directive and the TCO Regulation. Unlike the DSA proposal, those earlier acts focus primarily at tackling illegal content, while seemingly considering the provision of safeguards to protect users' rights and interests more as secondary issue, instead of considering the latter as an objective in its own right. Thus, if the measures discussed in the previous subsection are seen as entailing an EU-level duty of care aimed at tackling illegal content, then the measures discussed in the present subsection could be seen as being aimed at ensuring that the duty is *doubled-sided* in nature, in the sense that the service providers concerned should also – and equally – take account of these kinds of rights and interests of the users when moderating the user content that they intermediate.

54 The DSA proposal would certainly not preclude content moderation as such, irrespective of whether the activities in question are aimed at tackling illegal content or terms of service-infringing content.[195] Thus, hosting service providers would in principle retain the possibility to set and enforce their terms of service, including where those terms of service are more restrictive than the applicable law when it comes to the types of content that they are willing to store and disseminate for their users. However, the DSA proposal would – on top of the limits that already result from generally applicable acts of EU law, such as the GDPR and the Unfair Terms Directive[196] – create an extra layer of user protection. In essence, the DSA proposal seeks to ensure that

189 Recital 48 ECD. Member States appear to make increasing use of that possibility. See eg the NetzDG in Germany and the so-called Avia law in France (although key parts of the latter bill were declared unconstitutional by the French Constitutional Council; see its Decision 2020-801 DC, 18 June 2020). See further D Savova, A Mikes and K Cannon, 'The Proposal for an EU Digital Services Act — A closer look from a European and three national perspectives: France, UK and Germany' (2021) *Computer Law Review International* 22, 38-45.

190 Art 20(1) DSA proposal. Pursuant to Art 20(2), providers would also be required to take measures against parties that frequently submit manifestly unfounded notices or complaints.

191 See para 36 above (regarding said complexities).

192 Art 20(3) and (4) DSA proposal. See also Recital 47 (expanding on the concept of 'manifestly illegal content').

193 Art 21 DSA proposal. Specifically, the proposed obligation relates to "*serious criminal offence[s] involving a threat to the life or safety of persons*". In this regard, see also Recital 48 (indicating that this term covers offences involving child sexual abuse, among other things).

194 Art 26 and 27 DSA proposal.

195 Cf Art 2(p) DSA proposal (defining the concept 'content moderation' essentially as any activities undertaken by providers to tackle content that is either illegal or violates their terms and conditions).

196 Directive 93/13/EEC on unfair terms in consumer contracts, [1993] OJ L 95/29.

content moderation takes place within a procedural framework set not by the providers themselves in view of their own commercial interests, but rather by the legislator in view of the public interests at stake. It is especially this aspect of the DSA proposal that is novel and may have the potential to become a sort of international standard, just as occurred with the GDPR in relation to the protection of personal data.[197]

55 Leaving aside the proposed rules already discussed above, again, three sets of provisions of the DSA proposal can be mentioned in particular. First, there is a strong emphasis on transparency, particularly in respect of content moderation-related matters. The proposed obligations range from providing clarity upfront in the terms and conditions, to the provision of reasons for the providers' decisions in individual cases, to ex post reporting to the public.[198] Such increased transparency is important for several reasons. It allows users to take informed decisions as to whether or not they wish to use the services in question, it reduces the scope for arbitrary decisions and it facilitates accountability. Second, users' redress possibilities would be improved, inter alia in relation to decisions to remove their content or suspend their account. Such redress would be possible not only through the aforementioned internal complaint-handling systems, but also through out-of-court dispute settlement and rules on the lodging of complaints to supervisory authorities and on representative actions.[199] As mentioned, the complaint-handling systems are essentially an EU version of the counter-notice procedures known in the US (although they are broader in scope). Finally, public oversight and enforcement would be significantly reinforced.[200] Rather extensive powers would be granted to national competent authorities, including to conduct on-site inspections, impose hefty fines (up to 6% of annual turnover) and block websites.[201] There is also a novel system of enhanced supervision of very large hosting service providers, the most notable feature of which is that it equips the Commission with direct investigatory and sanctioning powers.[202] Strengthening oversight and enforcement in this manner is important. That is due to the public interests at stake, but also because one should probably be realistic about what can be expected from users' redress mechanisms. The limited use made of the counter-notice procedure provided for in US law may be in part due to the design of that procedure,[203] but it probably also tells us something about the limited willingness or ability of users to actively defend their interests themselves. That does not mean that such redress mechanisms should not be provided for. But it does mean that the task of ensuring that the system works as intended cannot solely be left to users; public authorities may therefore need to step in.

I. Conclusion

56 In 1996 – that is, a few years before tabling the proposal for the ECD – the Commission stated that it sought to assist "*host[ing] service providers, whose primary business is to provide a service to customers, to steer a path between accusations of censorship and exposure to liability*".[204] A lot may have changed in the 25 years that followed, but the essence of the challenge remains unaltered. It is evident from the DSA proposal that the Commission considers that this path should continue to be founded on the knowledge-based liability model. This article has shown that that decision is understandable and perhaps even unavoidable. This finding constitutes, however, no more than a starting point for discussions on that proposal. Indeed, whilst the foundations of the proposed approach may be sound, room remains for diverging views on a range of matters relating to the liability of hosting service providers for stored user content. Especially if recent experiences are any guide, one can expect interesting and perhaps intense debates as to whether or not the measures that the Commission has put forward to refine and complement the existing model succeed in the ambition to steer a path for the next 25 years.

197 Savin (n 16), 16.

198 Art 12, 15, 13, 23 and 33 DSA proposal, respectively. In addition, very large hosting service providers are to provide, upon request, competent authorities or vetted researchers with access to data (Art 31 DSA proposal).

199 Art 17, 18, 43 and 68 DSA proposal, respectively.

200 The ECD does contain some provisions in this regard (Art 17-20), but those are, on the whole, neither very specific nor very demanding.

201 Art 41 and 42 DSA proposal.

202 Art 50-66 DSA proposal.

203 See para 41 above.

204 Commission, Illegal and harmful content on the internet, COM(96) 487, 12-13.