REGULATING DIGITAL PLATFORMS: WILL THE DSA CORRECT ITS PREDECESSOR'S DEFICIENCIES?*

Berrak Genç-Gelgeç**

Abstract: The E-Commerce Directive 2000/31 (ECD) has been the law applicable to Internet intermediaries related to their liability for third-party content on their platform, electronic contracts, and e-commerce activities for more than twenty years. Its core is the harmonised immunity regime established in Articles 12–15. These rules grant immunity to the providers of mere conduit, caching, and hosting from liability arising from infringing content made available by their users on their platform. However, the ECD has been criticised for not fully achieving its objective of uniformity, not keeping up with the pace of the Internet, and not effectively protecting the parties' fundamental rights as it gives crucial discretion to the intermediaries. The ECD is to be replaced with the Digital Services Act (DSA). The aim is to regulate new means of digital services (especially Big Tech) while benefiting from their 'technical and operational ability to act against specific items of illegal content' in preventing the availability of illegal content and protecting fundamental rights. Its framework is based on the prevailing idea of acknowledging digital platforms as responsible actors. It establishes new sets of tiered due-diligence obligations for digital platforms to comply with while reproducing the immunity regime of the ECD. Its framework appears to target those issues arising from the ECD. However, whether it can deliver this promise calls for discussion. This paper aims to address this question. To do so, it will first try to identify the deficits of the ECD. Second, and more importantly, it will seek to scrutinise the DSA to evaluate if it provides the answers to the issues that the ECD fell short of.

Keywords: digital platforms, liability, immunity regime, E-Commerce Directive, Digital Services Act.

---

* This paper considers the consolidated version of the DSA that was adopted on 5 July 2022.

** (LLM, Soton; PhD, Sussex); Lecturer in Civil and Obligations Law, Istanbul Medeniyet University Law School; email: berrakgenc@hotmail.com (ORCID: 0000-0001-5166-8965).
DOI: 10.3935/cyelp.18.2022.485.

1 Introduction

The Digital Services Act (DSA),[1] proposed by the European Commission to update the rules on information society services in December 2020, was approved by the European Parliament in July 2022 following a legislation process. It will be in force once it is approved and published by the Council of the European Union (EU). It will then be applicable from either 15 months after that date or on 1 January 2024, whichever is the later.[2] This means that the E-Commerce Directive 2000/31 (ECD)[3] is to be replaced by the DSA at that time.

The ECD has been the applicable law regulating Internet intermediaries[4] since 2000. Intermediaries are the pillars of the Internet, as they 'bring together or facilitate transactions between third parties on the Internet'.[5] The ECD's main objective was to create a legal framework to facilitate the free movement of intermediaries within the EU so that innovation and e-commerce activities can also be encouraged. Arguably, the most effective way to do the latter is to establish rules enabling intermediaries to provide services easily and foster innovation.[6] Similarly, the European legislator's approach to the ECD was not to regulate intermediaries through hard law but to establish rules to tackle illegal content online without imposing strict duties. Henceforth, the immunity regime is established by Articles 12–15 ECD. These rules exempt intermediaries from liability for the illegal content made available on their platforms by third parties.

Information society services cover 'all services normally provided against remuneration, at a distance by electronic means and on the indi-

---

[1] European Parliament legislative resolution of 5 July 2022 on the proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (COM(2020)0825 – C9-0418/2020 – 2020/0361(COD)) (DSA).

[2] DSA, Art 74.

[3] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) [2000] OJ L178/1 (ECD).

[4] This term is used interchangeably with information society services in this article.

[5] OECD, 'OECD Report on the Economic and the Social Role of Internet Intermediaries' (April 2010) <http://www.oecd.org/internet/ieconomy/44949023.pdf> accessed 10 September 2022.

[6] Indeed, in the early 2000s, this was the preferred approach to regulating intermediaries. Under US law, liability exemptions are also provided to specific service providers, although vertically. S.230(c) of the Communications Decency Act exempts access providers from liability for any content and hosting providers for information they store (excluding IP rights), while s.512 of the Digital Millennium Copyright Act grants immunity for access providers, caching services, hosting services and linking services arising from copyright infringements. Luciano Floridi, 'The End of an Era: From Self-Regulation to Hard Law for the Digital Industry' (2021) 34 Philosophy & Technology 619–622; Giancarlo Frosio, 'Regulatory Shift in State Intervention: From Intermediary Liability to Responsibility' in Edoardo Celeste, Amélie Heldt and Clara Iglesias Keller (eds), *Constitutionalising Social Media* (Hart Publishing, forthcoming) pt 3.

vidual request of a service receiver'.[7] However, immunity is only granted for certain services of intermediaries. These services are specified as the transmission of information ('mere conduit'), the provision of automatic, intermediate, and temporary storage ('caching'), and storage of information in the capacity of the host ('hosting'). Having immunity granted, however, depends on fulfilling different conditions for different types of intermediaries. For mere conduit and caching intermediaries, not being involved in the transmission of illegal content or information would be sufficient to have immunity granted, as the provision of these services does not necessarily require any intervention or involvement on their side. On the other hand, hosting intermediaries are required to take swift action once they become aware (for claims regarding damages) or have actual knowledge (for criminal law matters) of the infringing nature of the content uploaded on their platform to benefit from immunity. As hosting intermediaries store information on their platforms, which might require involvement from intermediaries in operating, the immunity is grounded on different conditions from mere conduit and caching intermediaries. In this respect, the ECD encourages hosting intermediaries to implement the notice and takedown (NTD) mechanism in their systems to tackle infringing content. But further insight on how the mechanism should work and what principles should be followed is not provided. These matters are left to Member States to deal with under national laws. That being said, Article 15 ECD prohibits Member States from imposing general monitoring obligations on intermediaries in tackling illegal content. In this way, this article confines hosting intermediaries' involvement in acting against illegal content, although the term 'scope of general monitoring' is not clearly defined, as will be demonstrated later.

The immunity rules apply horizontally so that they apply to cases when the uploaded content gives rise to an infringement of any substantive rights, with only the exception of claims relating to data and privacy protection.[8] More importantly, the immunity rules provide additional protection to intermediaries. This means that not fulfilling the conditions for immunity, ie failing to benefit from immunity, does not automatically lead an intermediary to be regarded as liable.[9] The intermediaries' liability question is dealt with by the national laws of Member States. This is compatible with the approach adopted for the ECD, as well as the fact that tort law (which often applies to civil liability cases) is not harmonised

---

7 ECD, recital 17.

8 ECD, Art 5(b).

9 Eifert and others state that the immunity rules should not be considered as rules to provide privileges to intermediaries. The regime instead specifies the general duty of care of intermediaries from illegal content. The DSA's approach of reproducing the immunity regime is thus regarded as appropriate, provided that intermediaries are granted exemption from liability when they are not involved in their users' infringing activity. Martin Eifert, Axel Metzger, Heike Schweitzer and Gerhard Wagner, 'Taming the Giants: The DMA/DSA Package' (2021) 58 Common Market Law Review 987, 1005–1006.

within the EU.[10]

Having said that, the DSA is grounded on a somewhat different approach. It reflects the prevailing idea of acknowledging digital platforms as responsible actors in tackling illegal content.[11] Although the ECD's immunity regime is maintained in the DSA with a small addition, new sets of transparency, accountability and information obligations are imposed on providers of digital services, where some of these obligations appear as ex-ante ones. Considering the evolution of the Internet since the ECD was adopted, acknowledging intermediaries as main actors and imposing duties on them seem more appropriate for establishing a properly functioning digital market. When the Internet was in its infancy, the aim was to foster innovation with the ECD, but now innovative digital services have been taken to a different level. Especially with the advent of Web 2.0,[12] users have become more actively involved in the Internet, while intermediaries' societal, economic and political impact scales up accordingly.[13] This also means that the harm caused by illegal content affects more users.[14] In dealing with this, the ECD, as mentioned, requires hosting intermediaries to act against illegal content and accordingly encourages them to implement NTD mechanisms. It, however, does not determine the scope of the actions or the measures that could be taken. In default of

[10] Helmut Koziol, 'Harmonising Tort Law in the European Union: Advantages and Difficulties' (2013) 1 ELTE Law Journal 73–88; Michael Faure, 'The Harmonisation of EU Tort Law: A Law and Economics Analysis' in Paula Giliker (ed), *Research Handbook on EU Tort Law* (Edward Elgar Publishing 2017). There is also an EU plan to establish a legal framework for AI technologies. One of the legal initiatives proposed as part of that plan is to create civil liability rules for AI. For this action plan, see 'A European Approach to Artificial Intelligence' *(European Commission,* 28 September 2022) <https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence> accessed 10 September 2022. See also Bernhard A Koch and others, 'Response of the European Law Institute to the Public Consultation on Civil Liability: Adapting Liability Rules to the Digital Age and Artificial Intelligence' (2022) 13 Journal of European Tort Law 25; European Commission, Directorate-General for Justice and Consumers, Ernst Karner, Bernhard Koch and Mark Geistfeld, *Comparative Law Study on Civil Liability for Artificial Intelligence* (Publications Office of the European Union 2021); Alberto Galasso and Hong Luo, 'Punishing Robots: Issues in the Economics of Tort Liability and Innovation in Artificial Intelligence' in Ajay Agrawal, Joshua Gans and Avi Goldfarb (eds), *The Economics of Artificial Intelligence: An Agenda* (University of Chicago Press 2019) 493–504.

[11] Frosio (n 6). Floridi asserts that regulating digital platforms through soft law or self-regulation was also the most logical approach to facilitate the dialogue between society and the digital industry, although he now strongly supports regulating the digital market through hard law. See Floridi (n 6) 619 and 622.

[12] Web 2.0 is the technology which allows user interaction online via interactive applications and platforms. For a detailed analysis, see Tim O'Reilly, 'What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software' (2007) 65 International Journal of Digital Economics 17.

[13] Ilaria Buri and Joris van Hoboken, 'The Digital Services Act (DSA) Proposal: A Critical Overview' (2021) Discussion paper, Digital Services Act (DSA) Observatory, Institute for Information Law (IViR), University of Amsterdam.

[14] Alexandre De Streel and Martin Husovec, 'The E-commerce Directive as the Cornerstone of the Internal Market', study for the committee on Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies (European Parliament, Luxembourg 2020) 25.

clearly defined rules and transparency obligations,[15] the intermediaries can be said to become private powers.[16] This is perhaps one of the ECD's greatest challenges in reaching its goal of establishing uniform rules.

The DSA, on the other hand, promisingly sets outs due diligence obligations of transparency, accountability and information for digital services to qualify. More importantly, it takes the technical abilities, sizes and powers of digital services into account in establishing the rules. The obligations are set out depending on their size and roles in the online world. In this respect, the providers of digital services are classified into four categories: intermediaries, hosting intermediaries including online platforms, online platforms (providers of hosting services that also disseminate information),[17] and very large online platforms (VLOPs) and very large online search engines (VLOSEs) (online platforms that have more than 45 million recipients).[18] As will be demonstrated later, each is required to perform duties at different levels. This approach seems effective in creating a uniformly applied legal framework, as it specifies each platform's obligations. Furthermore, the DSA reproduces the immunity regime for digital services. This also appears to be fit for purpose: regulating new means of digital services, especially Big Tech,[19] while benefiting from their 'technical and operational ability to act against specific items of illegal content'[20] in preventing the availability of illegal content and pro-

[15] Indeed, back in 2015, academics from around the world wrote an open letter directed at Google, seeking more transparency from Google, especially on the reasons for denying or granting delisting requests, as the Transparency Report published by Google was considered to lack the required clarity on these points. See Ellen P Goodman 'Open Letter to Google from 80 Internet Scholars: Release RTBF Compliance Data' (*Medium*, 13 May 2015) <https://ellgood.medium.com/open-letter-to-google-from-80-internet-scholars-release-rtbf-compliance-data-cbfc6d59f1bd> accessed 10 September 2022.

[16] De Gregorio and Pollicino also state that '[…] immunizing or exempting these actors – Big Tech's predecessors – from third-party responsibility has contributed to the transformation of economic freedoms into something that resembles the exercise of powers as vested in public authorities' in Giovanni De Gregorio and Oreste Pollicino, 'The European Constitutional Road to Address Platform Power' in Heiko Richter, Marlene Straub and Erik Tuchtfeld (eds), *To Break Up or Regulate Big Tech? Avenues to Constrain Private Power in the DSA/DMA Package* (2021) Max Planck Institute for Innovation and Competition Research Paper No 21-25, 16–21.

[17] DSA, Art 2(h).

[18] ibid.

[19] This is used for describing digital services, which are the major controllers of the digital market and have gained regulatory power over the market. It is associated with Google, Amazon, Facebook, Apple and Microsoft. This is why the Digital Markets Act (Commission Proposal for a Regulation on contestable and fair markets in the digital sector (Digital Markets Act) COM(2020) 842 final) is also proposed by the legislators besides the DSA (as the second legislative initiative of the Digital Services Act package) and is aimed at providing a level playing field for all sizes of platforms and at protecting competition within the digital market by bringing new sets of rules for specific platforms (which are defined as gatekeepers) to comply with.

[20] DSA, recital 26.

tecting fundamental rights.[21]

Although the approach seems promising and effective, whether the framework established by the DSA will iron out the deficits of the ECD calls for discussion. This paper aims to address this question. To do so, it will first try to identify the deficiencies of the ECD. Second, and more importantly, it will seek to scrutinise the DSA to evaluate if it provides the answers for the issues the ECD has failed to address. It should, however, be underlined that the DSA's framework will not be discussed in its entirety; instead, it is to be addressed within the scope of the article's objective.

2 The ECD: where does it fall short?

The ECD establishes a legal framework for Internet intermediaries concerning their liability for illegal content made available on their platform, electronic contracts, or commercial communications. In tackling the liability question, as it is addressed, it sets out harmonised safe harbour rules for intermediaries in Articles 12–15. More precisely, it provides the rules governing the circumstances when an intermediary can be immune from the liability that may arise for third parties' illegal content made available on its platform. If an intermediary does not qualify for immunity, its liability is to be assessed by the courts of Member States as per their corresponding tort or penal liability laws. Hence, the existing regime is more appropriately described as an immunity regime rather than a liability regime.[22] Before addressing the immunity regime, it should be noted that the ECD is adopted as a directive. This means that the ECD was not directly applied in Member States when it came into force. As a directive, the rules should be transposed into their national laws by the Member States. In doing so, the choice of forms and methods is left to the Member States. As will be seen, the choice of a directive affected the purpose of harmonisation in a negative way, especially regarding the NTD mechanism.

Reverting to immunity rules, immunity is provided for certain types of online services, namely the service that merely transmits information ('mere conduit'); that offers automatic, intermediate and temporary storage ('caching'); and that stores information in the capacity of a host ('hosting'). The regime, however, establishes different conditions according to the type of service provided since these services require a different

[21] In contrast, Buri and van Hoboken argue that the imposition of accountability obligations might entrench the dominant position of the intermediaries, although the exact opposite is aimed at. See Ilaria Buri and Joris van Hoboken, 'The DSA Proposal's Impact on Digital Dominance' in Heiko Richter, Marlene Straub and Erik Tuchtfeld (eds), *To Break Up or Regulate Big Tech? Avenues to Constrain Private Power in the DSA/DMA Package* (2021) Max Planck Institute for Innovation and Competition Research Paper No 21-25 10–15.

[22] Patrick Van Eecke and Maarten Truyens, 'EU Study on the Legal Analysis of a Single Market for the Information Society' (2009) EU Study <https://op.europa.eu/en/publication-detail/-/publication/a856513e-ddd9-45e2-b3f1-6c9a0ea6c722> Ch 6.3.2 accessed 10 September 2022.

operating process. These conditions assist in separating an active intermediary from one that remains passive while operating, as the ECD's approach in tackling illegal content is to foster innovation as well as to prevent the availability of infringing content online. Thus, immunity is provided to an intermediary that is regarded as passive. However, what should be understood by an active or passive intermediary is not clearly explained by the ECD. Recital 42 only states that the activity of an intermediary should be 'of a mere technical, automatic and passive nature which implies that the information society service provider has neither knowledge of nor control over the interested parties of deciding freely whether to adhere to the information which is transmitted or stored'.[23]

In the *Google France* case,[24] the Court of Justice of the European Union (ECJ) held that a hosting intermediary should play a neutral role when providing its service in order to benefit from immunity. This case considered third-party trademark infringements committed on Google's platform. One of the questions before the ECJ was whether or not Google (a referencing service provider that also enables advertisers to purchase keywords) qualifies as an information society service under the ECD. If it does, should it benefit from immunity?[25]

In dealing with these questions, the ECJ held, in the light of recital 42, that a hosting provider should be neutral to be exempted from liability. It further established that it is considered to play a neutral role in offering its service when 'its conduct is merely technical, automatic and passive, pointing to a lack of knowledge or control of the data it stores'.[26] However, this test appears problematic as it would not always be straightforward to assess if a hosting intermediary's conduct is passive and purely technical. Hosting intermediaries would often need to have some tools implemented in their system to enable their users to use the services properly.

For example, an online auction site, eBay, optimises the presentation and sales on its platform through its advertisements on search engines,

---

[23] In that regard, recital 42 states the following: 'The exemptions from liability established in this Directive cover only cases where the activity of the information society service provider is limited to the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission more efficient; this activity is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the interested parties of deciding freely whether to adhere to information which is transmitted or stored'.

[24] Joined Cases C-236/08 to C-238/08 *Google France SARL and Google Inc v Louis Vuitton Mallettier SA* and *Google France SARL v Viaticum SA and Luteçial SARL and Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL and Others* ECLI:EU:C:2010:159, paras 114–116.

[25] ibid.

[26] ibid.

and assists users in enhancing their activities on its platform.[27] Such advertising-driven business models help the platforms attract more users and make them spend more time on these platforms.[28] The ECJ in *L'Oréal*[29] decided that eBay's role is passive unless the optimisation of presentation and sales through advertisements gives it knowledge of or control over the content. In this respect, it would not be wrong to conclude that hosting intermediaries would have some degree of involvement in providing their services.[30] Indeed, this was the ground on which the Advocate General (AG) in *L'Oréal*[31] based his opinion when criticising the neutrality test that the ECJ in *Google France* applied. The ECJ, however, approved neutrality as a condition for hosting intermediaries' immunity in *L'Oréal* without discussing the points raised by the AG.[32]

Later, in *YouTube v Cyando*,[33] the ECJ held, concerning the neutrality test, that the hosting provider's implementation of measures aimed at detecting illegal content on its platform should not be considered as giving an active role to the intermediary in conducting its service. This would mean that the hosting intermediary could and should (as per Article 14(1)(b)) implement necessary measures to tackle illegal content, but this ought not lead the intermediary to play an active role in conducting its service. But how should this apply to the extensive content moderation technologies of today? Where should the line be drawn for an intermediary not to be considered active? There is no further insight given on this. Hence, the intermediary will decide on that in light of the general

---

[27] The ECJ also considered this as an element in answering the question of eBay's liability from its users' sale of products that infringed the trademark rights of an owner. See Case C-324/09 *L'Oréal SA and Others v eBay International AG and Others* ECLI:EU:C:2011:474.

[28] Miriam Buiten, 'The Digital Services Act: From Intermediary Liability to Platform Regulation' (2021) <https://ssrn.com/abstract=3876328> 2–4 accessed 10 September 2022.

[29] *L'Oréal* (n 27) paras 114–116.

[30] Van Eecke astutely states that the neutral role of hosting intermediaries should not be understood and construed as them being completely passive in the provision of services. See Patrick Van Eecke, 'Online Service Providers and Liability: A Plea for a Balanced Approach' (2011) 48 Common Market Law Review 1462, 1483. Van Hoboken and others also state '[i]n our view, they are not binary terms to be understood solely with reference to their ordinary meaning. Rather, they should be understood as terms of art that encompass a range of meanings – ascribed by the CJEU (and national courts) – along a potential spectrum of activities performed by intermediaries'. See Van Hoboken and others, 'Hosting Intermediary Services and Illegal Content Online: An Analysis of the Scope of Article 14 ECD in Light of Developments in the Online Service Landscape' European Commission (2018) 31–37 available at <op.europa.eu/nl/publication-detail/-/publication/7779caca-2537-11e9-8d04-01aa75ed71a1> accessed 10 September 2022. See also Miquel Peguera, 'The Platform Neutrality Conundrum and the Digital Services Act' (2022) 53 IIC – International Review of Intellectual Property and Competition Law 681, 682; and De Streel and Husovec (n 14) 20.

[31] Case C-324/09 *L'Oréal SA and Others v eBay International AG and Others*, Opinion of AG Jääskinen ECLI:EU:C:2010:757, para 146.

[32] ibid, para 113.

[33] Joined Cases C-682/18 and C-683/18 *Frank Peterson v Google LLC, YouTube LLC, YouTube Inc, Google Germany GmbH (C-682/18) and Elsevier Inc v Cyando AG* ECLI:EU:C:2021:503, para 109.

monitoring obligation, which will be addressed later.

Furthermore, there is a diligent economic operator test applied by the ECJ, which should also be considered in distinguishing active intermediaries from passive ones. Article 14 grants hosting intermediaries immunity depending on two qualifying conditions: either a hosting provider does not obtain awareness[34] as to the infringing content made available on its platform or acts expeditiously to remove or block access to the infringing content once it obtains awareness. Hence, assessing whether a provider has become aware of the infringing content is also important. Although this assessment is left to domestic courts to address under their national laws, the ECJ established that awareness should be assessed based on a 'diligent economic operator' criterion.[35] It went on to decide that[36] the courts should ask the question if a diligent economic operator 'should have identified the illegality in question and acted in accordance with Article 14(1)(b)' concerning 'every situation in which the provider concerned becomes aware, in one way or another of such facts or circumstances'.[37] This, however, would unlikely assist in setting the standard in practice for intermediaries to follow as the intermediaries' technical capabilities and sizes differ.[38] It is evident that the powers of relatively small or medium-sized intermediaries and their already implemented measures to investigate and prevent the illegality of content could hardly match the facilities of bigger intermediaries. The same applies to distinguishing a passive intermediary from an active one. Besides being of different size, intermediaries have various architectural structures and business models. Hence, setting a standard of diligence without paying attention to such differences and infrastructural advantages hardly assists in establishing a fair framework. In this regard, the DSA's approach of distinguishing digital services according to their sizes and impact on the digital world appears appropriate. How effective this could be will be

[34] As mentioned in the introduction, immunity from criminal liability depends, under Article 14, on obtaining actual knowledge. However, as this paper focuses only on the circumstances which give rise to civil liability, the actual knowledge standard is not discussed here.

[35] *L'Oréal* (n 27) para 120.

[36] ibid, paras 120–121.

[37] This test resembles the reasonable person test stemming from tort law which basically asks what a reasonable person of ordinary prudence would have done under the same or similar circumstances. For a detailed assessment, see Berrak Genç-Gelgeç, *The Law of Contributory Liability on the Internet: A Trademark Analysis* (Cambridge Scholars Publishing 2022) ch 3.

[38] It should also be recalled that, as the matter is left to domestic courts to decide under their applicable tort law, divergent interpretations and applications of the test would not be inevitable. Similarly, Synodinou argues that not having a uniform understanding of the term diligence would most likely bring fragmented applications across the EU. See Tatiana-Eleni Synodinou, 'Intermediaries Liability for Online Copyright Infringement in the EU: Evolutions and Confusions' (2015) 31 Computer Law & Security Review 66. De Streel and Husovec argue that 'the passivity criterion became the most controversial and led to the diverging outcomes on the national level because it allowed national courts to easily sidestep the ECD'. See De Streel and Husovec (n 14) 20.

discussed later.

Reverting to Article 14, it is established that a hosting intermediary may also benefit from immunity even if it obtains awareness of the infringing content uploaded by third parties. Article 14(1)(b) requires a hosting intermediary to act *expeditiously* to remove or block access to the infringing content after obtaining awareness. As it was also clarified by the ECJ later in *L'Oréal*,[39] an intermediary can obtain awareness 'as the result of an investigation undertaken on its own initiative, an illegal activity or illegal information, as well as a situation in which the operator is notified of the existence of such an activity or such information'.

The latter is perhaps the most common way of obtaining awareness. Hence, intermediaries are encouraged to implement a mechanism that enables users to notify the provider regarding illegal content so that they take appropriate action (removal or disablement of the content). This reflects the NTD mechanism, as mentioned above. The ECD, however, does not establish a legal framework concerning the mechanism's procedures and elements, such as the requirements of notice and the timeframe for taking appropriate actions or safeguards for the parties involved.[40] This is left to Member States to regulate through self-regulation within their domestic laws.[41] By virtue of this, some regulatory actions have been undertaken by Member States in their national laws, but their effectiveness has never been tested before the ECJ.[42] Besides, these regulations generally focus on the specific type of illegality, like terrorism-related content or child abuse. More importantly, as a result of self-regulations, the rules and procedures of the NTD mechanism are heavily fragmented amongst the Member States.[43]

Considering the lack of a legal framework, it would not be wrong to say that the applicable rules and procedures have been formed through the application of intermediaries' self-implemented mechanisms. Intermediaries usually implement necessary mechanisms to tackle illegal content and not lose the immunity provided by the ECD. This is the natural outcome of the approach adopted in the ECD, ie not confining intermediaries with hard law and liability rules to incentivise innovation. But it has failed to provide uniformity and strike a balance between the parties' fundamental rights that might be at stake. Article 14 requires the intermediary to take down or block access to the content infringing the rules

[39] *L'Oréal* (n 27) paras 121–125.

[40] Only Art 21(2) explicitly mentions notice and takedown mechanisms and it states that notice and those takedown procedures and the attribution of liability following the taking down of content shall also be analysed and included in the report that is required to be prepared by the Commission every two years after the ECD came into force.

[41] ECD, recital 46.

[42] De Streel and Husovec (n 14) 30.

[43] Commission, Online Services, Including e-Commerce, in the Single Market Accompanying the document Communication on 'A coherent framework to boost confidence in the Digital Single Market of e-commerce and other online services' SEC(2011) 1641 final, 3.4.4.

after receiving a notice. Hence, crucially it is the intermediary who examines the notification and the content and subsequently decides to take it down. This, however, raises serious concern about the protection of the fundamental rights of the parties, which is one of the main objectives of the ECD. When a rightsholder notifies an intermediary about the illegality of certain content, the intermediary's first task is to assess this claim and the content in question. Then, it decides to take down the content or block access to it if it finds the content illegal, as is claimed. Here, in dealing with the claim of illegality, an intermediary, a private company, acts similarly to a judge as it examines the claim and the illegality of the content. Such discretion appears problematic and perhaps detrimental, especially in protecting the content provider's right to freedom of expression and information. Moreover, if the content is mistakenly taken down or access to it is blocked, whether or not the content provider can challenge this decision is left to each Member State's rules if it provides any, or mostly intermediaries' own operation.[44] This would harm the protection of the content provider's right to a fair trial.

Content providers' fundamental rights are not the only concern regarding the application of the NTD mechanism. The mechanism may also affect the fundamental rights of other parties, such as the intermediary's right to conduct business and freedom of expression and the rightsholder's right to protection and access to justice.[45] Protection of these rights is, however, left to intermediaries, as they are the ones who implement and apply the NTD mechanism.

Moreover, the ECD does not set transparency or due diligence obligations for intermediaries to comply with. This strengthens the intermediaries' power in the digital world as they can act almost like lawmakers. These are left to the intermediaries' discretion and control. Although most of the Big Tech companies have transparency rules in their terms and conditions (TCs) and publish transparency reports on their content moderation activities, these are mostly criticised as not including essential and vital information as to their content moderation activities.[46] Hence, the transparency obligations imposed on them appears to have

---

[44] For instance, Facebook has implemented the Oversight Board system where a user can appeal against the takedown decision. However, this is only available for a specific type of content. The fact that Facebook is not obliged to apply the decision to all similar cases is criticised as this might result in controversy, especially concerning politics and democracy. See Elettra Bietti, 'A Genealogy of Digital Platform Regulation' (2022) 7 Georgetown Law and Technology Review (forthcoming) available at <http://dx.doi.org/10.2139/ssrn.385948> accessed 10 September 2022. For detailed information on Facebook's Oversight Board, see <https://www.facebook.com/help/711867306096893>.

[45] The CJEU first pointed out the importance of the application of the balancing test in Case C-275/06 *Productores de Música de España (Promusicae) v Telefónica de España SAU* ECLI:EU:C:2008:54.

[46] Goodman (n 15); Mathew Ingram, 'Facebook "Transparency Report" Turns Out to Be Anything But' (*Columbia Journalism Review*, 26 August 2021) <www.cjr.org/the_media_today/facebook-transparency-report-turns-out-to-be-anything-but.php> accessed 10 September 2022.

been the right step towards protecting fundamental rights and balancing the intermediaries' powers.

The NTD mechanism, apart from putting intermediaries in a judge-like position, can hardly be said to assist in achieving the goal of tackling illegal content effectively. As immunity rules apply horizontally, intermediaries may receive notifications about the illegality of content or information arising from different substantive rights. Examples are defamation, trademark infringement claims, etc. An intermediary is the one who examines those claims. However, such an assessment may require legal knowledge or even expertise unless the content is manifestly illegal. For instance, in *L'Oréal*, eBay was expected to assess whether the content had infringed the trademark of a rightsholder. This assessment required eBay to examine the authenticity of the products bearing L'Oréal trademarks. In another case, an intermediary may be required to assess the legality of a digital copy of a movie in terms of copyright infringement[47] or the nature of the comments left on the platform to see whether this amounts to defamation, hate speech or incitement to violence.[48]

It is evident that intermediaries, especially the Big Tech companies, have implemented automated systems like artificial intelligence (AI) to tackle the availability of illegal or infringing content on their platforms. For instance, YouTube has a Content ID mechanism, an automated content moderation system to identify copyright infringements.[49] Although such automated mechanisms might be time-efficient and practical compared to human moderation, they might not capture all kinds of policy violations or infringements. For example, it would often be difficult for an AI without human intervention to identify and distinguish fair use of copyright-protected content from an infringement. In such cases, an intermediary might be inclined to take down the content to benefit from immunity, as the ECD does not impose any sanction or transparency obligations on intermediaries for a false or unfair takedown. This could also 'damage user experience by over-detection and the generation of

[47] In fact, in terms of copyright infringement, providers might be required to apply the test of 'communication to the public' as per Art 3(1) of the InfoSoc Directive 2001/29 to take further action. This indeed requires additional expertise. On this, see Neville Cordell and Beverley Potts, 'Communication to the Public or Accessory Liability: Is the CJEU Using Communication to the Public to Harmonise Accessory Liability Across the EU?' (2018) 40(5) European Intellectual Property Review 289.

[48] The judgments *Delfi AS v Estonia* App no 64569/09 (ECtHR, 16 June 2015); *Magyar Tartalomszolgáltatók Egyesülete (MTE) and Index.hu Zrt v Hungary* App no 22947/13 (ECtHR, 2 February 2016); and *Pihl v Sweden* App no 74742/14 (ECtHR, 7 February 2017) of the European Court of Human Rights could be illustrative of this. In those cases, the platforms were expected to assess the nature of the comments and take the appropriate action to deal with them, although they were not considered intermediaries.

[49] See <https://support.google.com/youtube/answer/2797370?hl=en> accessed 10 September 2022.

false-positives'.[50] The same concerns were raised about Facebook's own automated mechanisms by Facebook itself in 'Facebook Response to EC Public Consultation on the Digital Services Act (DSA)'.[51] As mentioned above, the intermediaries' transparency reports do not provide sufficient information and figures on these processes. It is submitted that this may pose a severe risk to fundamental rights and raise difficulties in providing uniform rules for the digital world. On the other hand, taking down the content in order to benefit from immunity without explicitly examining the content may not be a much-desired action for intermediaries, given that the contents attract users and cause interaction. Here, the DSA's transparency obligations seem to iron out the risks and difficulties attributed to the procedures of tackling illegal content, as it provides standards for different intermediaries to follow and comply with. However, the conclusion should be made after evaluating the rules.

Along with the immunity regime, injunction orders should also be addressed. The application of an injunction order by the courts against intermediaries is made possible in Articles 12(3), 13(3) and 14(3) ECD. As clearly stated in these articles, applying an injunction order is not bound to the immunity question. This means that qualifying or not qualifying for immunity does not affect the imposition of such orders. However, they are still germane to the immunity regime and have been assisting in defining the framework. Injunction orders serve to tackle infringements by imposing ex-post obligations on intermediaries. These measures are grounded on the principle of best cost avoider, meaning that the measures should be applied by 'the party that has or can develop measures to avoid the harm most cheaply'.[52] In this sense, injunction orders also seem to serve the DSA's purpose of balancing the power given to intermediaries, as they are the best cost avoiders considering their infrastructural advantages and self-implemented measures. Such orders have also proven to be popular among rightsholders, especially owners of intellectual property rights, to combat online infringements. However, the implementation of injunctions has not been straightforward in practice. It is mainly because these orders are left to each national court to apply under their national laws. Moreover, the ECD only sets out a rule on the prohibition of the general monitoring obligation in Article 15, which applies to injunction orders.

---

[50] This was the statement by one of the online providers in the EU Study on 'Online Platforms' Moderation of Illegal Content Online'. See the detailed analysis in Alexandre De Streel and others, 'Online Platforms' Moderation of Illegal Content Online', Study for the committee on Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies (European Parliament, Luxembourg 2020).

[51] 'Facebook Response to EC Public Consultation on the Digital Services Act (DSA)' (*Facebook*, 2020) <https://about.fb.com/de/wp-content/uploads/sites/10/2020/09/FINAL-FB-Response-to-DSA-Consultations.pdf> accessed 10 September 2022.

[52] Martin Husovec, 'Accountable, Not Liable: Injunctions Against Intermediaries' (2016) TILEC Discussion Paper No 2016-012 (Draft) 25 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2773768/> accessed 10 September 2022.

Complementing the ECD on injunction orders, there is also the Enforcement Directive 2004/48,[53] which enables rightsholders to apply for an injunction against an intermediary for infringements of intellectual property rights specifically excluding copyright (as another directive[54] directly applies to copyright cases). It sets out the principles for an injunction measure in Article 3.[55] Under this, an injunction measure shall be effective in reaching its aim while not being costly or unfair or open for abuse.[56] These are the minimum standards that Member States' courts should consider in assessing injunction requests made against an intermediary to prevent unreasonable and disproportionate burdens on intermediaries.

In addition, the ECJ's case law provides further insight but limited to the issues brought before it. In those cases, the ECJ was challenged to address whether an injunction could be ordered for future infringements of the same kind or for an unlimited time and how to balance the fundamental rights that might be at stake in granting an injunction order.[57] In dealing with these, the ECJ first and foremost underlined the significance of protecting the fundamental rights of the parties affected by an injunction order. As for NTD mechanisms, an injunction order involves three parties: intermediaries, content providers, and rightsholders. The fundamental rights of these parties would also be affected. The rights that would be at stake were identified by the ECJ as follows: the content provider's right to freedom of expression and information; the right to the protection of personal data and privacy or the right to a fair trial; the intermediary's right to conduct business and the right to freedom of expression; and the rightsholder's right to protection and access to justice.[58] Accordingly, the Court's appraisals focused on striking a balance between the fundamental rights at stake.

---

[53] Directive (EC) 2004/48 of 29 April 2004 on the enforcement of intellectual property rights [2004] OJ L195/16.

[54] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC [2019] OJ L130/92.

[55] Art 3(1) of Enforcement Directive 2004/48 states that an injunction measure 'shall be fair and equitable and shall not be unnecessarily complicated or costly or entail unreasonable time-limits or unwarranted delay' and Art 3(2) states that it 'shall also be effective, proportionate and dissuasive and shall be applied in such a manner as to avoid the criterion of barrier to legitimate trade and to provide for safeguards as against their abuse'.

[56] For proportionality in injunction cases, see Tobby Headdon, 'Beyond Liability: On the Availability and the Scope of Injunctions Against Online Intermediaries After L'Oréal v eBay' (2012) 34(3) European Intellectual Property Review 137, 139–141; Pekka Savola, 'Proportionality of Website Blocking: Internet Connectivity Providers as Copyright Enforcers' (2014) 5 Journal of Intellectual Property, Information, Technology and E-Commerce Law 116.

[57] *L'Oréal* (n 27).

[58] Case C-70/10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* ECLI:EU:C:2011:771; Case C-314/12 *UPC Telekabel Wien GmbH v Constantin Film Verleigh GmbH, Wega Filmproduktionsgesellschaft GmbH* ECLI:EU:C:2014:192.

The outcomes of these cases can be summarised as follows. An injunction order requiring an intermediary to implement a filtering system as applicable to all its users and for an unlimited time should not be granted, as such measures would amount to general monitoring[59] and would harm the balance between the fundamental rights of the parties. However, in another case, the imposition of a generic order was considered in compliance with EU law as long as the chosen measure strikes a balance between the parties' fundamental rights.[60] A generic order means that an injunction order is granted against an intermediary without determining the type of the injunction. Here, the intermediary chooses the appropriate mechanism to prevent the availability of illegal content and applies it. Requiring an intermediary to select a measure that respects the fundamental rights of the parties was undoubtedly in accordance with the law concerned in that case,[61] but leaving the duty to take care of the fundamental rights of the parties would give rise to the very same concern that is pointed out for the NTD mechanism. In this case, the intermediary was given judge-like discretion without specifying the borders in assessing and choosing the most appropriate measure that also protects fundamental rights. This could hardly strike a balance between the parties.

Lately, the Member States were also given the green light to extend the scope of the previously ordered injunction to be effective worldwide for content that is identical or equivalent to the content regarded as illegal before.[62] This case concerned an injunction order requiring the hosting intermediary to remove the defamatory content. The ECJ held that this intermediary might also be required to monitor and search for information – which is identical or has equivalent meaning to the content regarded as defamatory before – by such a measure. The act of monitoring is limited to 'information conveying a message the content of which remains essentially unchanged'.[63] The Court found that such a measure would not amount to a general monitoring obligation prohibited by Article 15. Unfortunately, the decision did not clarify the application of Article 15 and injunction orders. First, here an injunction order was given an extraterritorial effect 'within the framework of relevant international law'.[64] However, the application of such an injunction within other legal systems

[59] Case C-360/10 *Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) v Netlog* ECLI:EU:C:2011:771. This case concerned an injunction requested against a social networking platform for the content infringed copyrights of the rightsholders.

[60] Case C-314/12 *UPC Telekabel Wien GmbH v Constantin Film Verleigh GmbH, Wega Filmproduktionsgesellschaft GmbH* ECLI:EU:C:2014:192. Here, the injunction order was requested against an ISP for the availability of unauthorised copies of the movies protected by copyright.

[61] It was a referral from an Austrian court, and it was possible to grant a generic order under Austrian national law. Hence, the impact of the case might remain limited.

[62] Case C-18/18 *Eva Glawischnig-Piesczek v Facebook Ireland Limited* ECLI:EU:C:2019:821.

[63] ibid, para 53.

[64] ibid.

might raise concern over the protection of fundamental rights, given that a balance between fundamental rights might be struck differently under different jurisdictions.[65] Second, the ECJ did not clearly determine the borders of the concerned injunction. Although it was held that a search could be done for information that is identical or has equivalent meaning, assessing if the information has equivalent meaning is open to interpretation. In this respect, it is hard to conclude that the injunction ordered can be classified as specific. Determining the borders of the 'specific' monitoring obligation is, however, important, as a monitoring obligation can only be imposed on the intermediaries for specific cases under Article 15. As no insight is provided by the ECD or the ECJ,[66] what should be considered a 'specific' monitoring obligation remains a challenging task for the national courts. This should be decided under their national laws.

Against this background, it can be concluded that the current regime of intermediaries' liability does not seem to achieve the goals of the ECD thoroughly. The ECD's main objective is to establish a properly functioning single market for digital services by providing uniform rules and focusing on the protection of the fundamental rights of the parties. As far as the immunity regime is concerned, it establishes the general principles, but the application of these rules hardly provides uniformity. As demonstrated, fragmentation mainly arises out of the application of the NTD mechanism. The ECD does not establish any framework for this. This is left to the Member States and their national laws. In a similar sense, the ECJ does not provide a clear understanding of what should be understood as a passive/active intermediary for courts to follow in assessing hosting intermediaries' immunity. It does not take the intermediaries' differences into account, either. More importantly, the application of the current law seems to point out that the biggest obstacle in ensuring harmonisation is the discretion given to the intermediaries regarding the matters relevant to the immunity regime and tackling illegal content. This, as shown, raises serious concerns over the protection of fundamental rights. It is submitted that this appears to be due to the approach adopted, the lack of further guidance, and the lack of transparency obligations. Indeed, the European Commission's Impact Assessment[67] on the ECD similarly emphasises these matters. The DSA accordingly and plausibly focuses on them while reproducing the immunity regime almost

---

[65] Federico Fabbrini and Edoardo Celeste, 'The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders' (2020) 21 German Law Journal 55, 64.

[66] In *Loreal*, the ECJ was asked whether an intermediary would be under a duty to apply the same measure for future infringements of a same or similar kind, but the question was left unanswered. See *L'Oréal* (n 27). The Advocate General in his opinion stated that an intermediary could apply the measure to prevent the same or similar infringements committed by the same person in the future as this would not amount to general monitoring. See Opinion of AG Jääskinen in *L'Oréal* (n 31) para 181.

[67] Commission, 'Impact Assessment Accompanying the Document Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC' (Staff Working Document) SWD (2020) 348 final, Part 1 (Impact Assessment Part 1).

verbatim. Whether it does provide the necessary answers will now be examined.

3 Regulating digital platforms: the DSA

As the two main legislative initiatives of the Commission's digital strategy, the DSA and the Digital Markets Act (DMA) aim to regulate digital services, especially those that have become dominant players on the Internet, economically and socially. The fact that the DSA applies to all digital services which provide services to users who are established or residents of the EU (regardless of the intermediaries' place of establishment) demonstrates that these companies, ie Big Tech, are the main focus as most of them are established outside the EU.[68] The DSA's main objective is to update the rules governing digital services, namely the ECD,[69] while the DMA's is to provide a competitive and fair digital market for digital services. To this end, both Acts are adopted as a regulation. This means that once the DSA comes into force, it is to be binding 'in its entirety and directly applicable'[70] in all Member States. This could be considered the right step toward uniformity, as the rules will be expected to apply uniformly.[71]

Besides the choice of instrument, the legislators' approach to regulating digital services should also be referred to before discussing the proposed rules. Like the ECD, the DSA provides the rules for information society services.[72] However, unlike the ECD, the DSA does not consider only the providers of Internet intermediaries. Along with certain intermediary services, namely mere conduit, caching, and hosting, the DSA acknowledges new digital services, such as online platforms and search engines. An online platform is a hosting service provider that stores and dissemi-

[68] DSA, Art 1(a)(1). Art 11 obliges such intermediaries to appoint a legal representative.

[69] However, it complements existing sector-specific legislation (such as Directive 2010/13/EU on Audiovisual Media Services) and existing EU laws regulating certain aspects of intermediaries (such as Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services). These are applicable as *leges speciales*. See Explanatory Memorandum to the DSA proposal, Commission Proposal for a Regulation on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, 15 December 2020, COM(2020)825 final.

[70] Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union [2012] OJ C326/47, Art 288(2).

[71] Having said that, making relevant national laws in line with the DSA and complying with the rules (especially for digital services) would take time, as was experienced with the application of the GDPR. See EU Commission press release, 'General Data Protection Regulation Shows Results, But Work Needs to Continue' (*EU Commission*, 24 July 2019) <https://ec.europa.eu/commission/presscorner/detail/en/IP_19_4449> accessed 10 September 2022.

[72] Information society services are defined as 'any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient' in Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services [2015] OJ L241/1.

nates information to the public.[73] So, an online platform is differentiated from a hosting service provider as the latter only stores information but does not disseminate it. Dissemination is making information available to an unlimited number of third parties at the request of the provider of that information.[74] An online search engine, on the other hand, is defined 'as a digital service that allows users to input queries to perform searches of, in principle, all websites, or all websites in a particular language, on the basis of a query on any subject in the form of a keyword, voice request, phrase or other input, and returns results in any format in which information related to the requested content can be found'.[75] As digital services are distinguished according to the services provided, the DSA establishes a legal framework that takes account of these differences. The creation of asymmetric due diligence and transparency obligations is a part of this approach.

The rules established by the DSA can be categorised under three main categories: immunity rules, due diligence obligations, and enforcement. These will be addressed now, but not as a whole. They will be addressed within the relevance of the article's aim.

3.1 Immunity rules

Starting with the immunity regime, the DSA reproduces the ECD's immunity regime in Articles 3–9, as they are still considered instrumental in creating the digital single market, despite the present fragmentation over the implementation of some principles.[76] Articles 12–14 of the ECD, are incorporated within Articles 3–5 of the DSA with a small addition. The addition is made to Article 5, which concerns hosting intermediaries. According to Article 5(3), providers of an online platform that intermediate between traders and customers cannot benefit from immunity from liability arising from customer protection law when a provider 'lead[s] an average consumer to believe that the information […] is provided either by the online platform itself or by a recipient of the service who is acting under its authority or control'. This article applies to online marketplaces and excludes them from immunity if their liability from customer protection law arises when they act in a certain way.[77]

---

[73] DSA, Art 2(h).

[74] DSA, Art 2(ha). However, this definition is criticised as its application to providers who do not directly face customers in a contractual relationship, such as cloud services, may be challenging. See European Parliament, Committee on the Internal Market and Consumer Protection (IMCO), Background Paper for the workshop 'The Digital Services Act and the Digital Markets Act: A Forward-looking and Consumer-centred Perspective' (*European Parliament,* 26 May 2021) 5 <www.europarl.europa.eu/cmsdata/234761/21-05- 19%20Background%20note%20REV%20final.pdf> accessed 10 September 2022.

[75] DSA, Art 2(ha)(i).

[76] DSA, recital 16.

[77] The European Consumer Organisation (BEUC), the Digital Services Act – BEUC position paper (*BEUC,* 9 April 2021) 9 <www.beuc.eu/publications/beuc-x-2021-032_the_digital_services_act_proposal.pdf> accessed 10 September 2022.

In addition to this new addition to the article, some matters are dealt with within the recitals. In the light of the ECJ's case law, it is now clearly stated that only the specific service of an intermediary in which an alleged infringement is committed should be considered in assessing whether an intermediary will benefit from immunity.[78] Taking Google as an example, it should be regarded as a caching service concerning its referencing service, whilst it might qualify as a hosting service regarding its keywords service since it enables its users to purchase keywords and display them as advertisements.[79] More crucially, the ECJ's ruling on the neutrality standard in *L'Oréal*[80] is included in recital 18 for clarity. The recital accordingly prescribes that an intermediary should not be considered to be providing its service neutrally when it 'plays an active role of such a kind as to give it knowledge of, or control over, those data'.[81]

Further, it is established that if an intermediary deliberately collaborates with its users to make illegal content available, it should not be deemed as providing its service neutrally. [82] In this regard, the DSA, unfortunately, does not give any answer to the criticism raised about the implementation of the neutrality test. It seems the legislator misses an opportunity to provide clarification or even review the applicability of the test to extensive content moderation technologies. Moreover, setting a standard of deliberate collaboration indicates the prospects of more ambiguity. The assessment of 'deliberate' is open to interpretation. How this is to be applied with the already problematic neutrality test under the DSA is therefore doubted.

Along with these relatively unaltered articles, the subsequent articles bring new principles relevant to the immunity regime. Article 6 prescribes that solely carrying out their voluntary own-initiative investigations will not be considered a factor in making intermediaries ineligible

[78] DSA, recital 27(a).

[79] This was actually one of the questions referred to the CJEU in Joined Cases C-236/08 to C-238/08 *Google France* ECLI:EU:C:2010:159. Although the CJEU did not address the question, the AG's opinion was that the immunity of an intermediary should be assessed according to the specific activity of the service at stake, as Recital 27(a) DSA establishes. See Joined Cases C-236/08 to C-238/08 *Google France* ECLI:EU:C:2009:569, Opinion of Advocate General Poiares Maduro, para 140.

[80] Joined Cases C-236/08 to C-238/08 *Google France* ECLI:EU:C:2010:159, para 110; *L'Oréal* (n 27) para 113.

[81] The DSA, recital 18 further establishes 'the mere ranking or displaying in an order, or the use of a recommender system should not, however, be deemed as having control over an information'.

[82] DSA, recital 20.

for immunity.[83] The implementation of voluntary mechanisms by intermediaries is not something new. Intermediaries have already been implemented in such mechanisms, especially automated ones. It is also implicitly encouraged by the ECD since the ECD requires them to act against illegal content to benefit from immunity. Even the ECJ held in *YouTube v Cyando* that the hosting provider's implementation of measures aimed at detecting illegal content on its platform should not be considered as giving an active role to the intermediary in conducting its service.[84] Now, the DSA explicitly encourages intermediaries to implement voluntary mechanisms and carry out their investigation to tackle illegal content. But the question is, does the DSA provide the solution for the issues arising from the application of voluntary obligations that were addressed before?

Article 6 limits the scope of voluntary actions that may be taken. It states that voluntary mechanisms cannot be considered as giving an active role to the intermediary only when voluntary investigations and measures are taken in good faith and in a diligent manner. Recital 25 explains that such acting 'should include acting in an objective, non-discriminatory and proportionate manner, with due regard to the rights and legitimate interests of all parties involved and providing the necessary safeguards against unjustified removal of legal content, in accordance with the objective and requirements of this Regulation'. However, this does not assist the interpretation of good faith and diligent manner. For instance, it is difficult to answer whether an intermediary is regarded as diligent when it applies the measure, but fails to detect the illegality.[85] Crucially, intermediaries will be the judge of whether they act in good faith or diligently. This might be a challenging and undesirable task for them, as they would not want to trigger the awareness or knowledge threshold that would mean a loss of immunity. Thus, there is doubt about how these standards would be implemented effectively and uniformly in practice. Hence, the framework on voluntary mechanisms should not be considered complete. On the other hand, the DSA imposes transparency obligations on digital services, which will be examined below. These might assist in establishing more concrete standards in applying voluntary measures.

Article 7 is another threshold that applies to voluntary mechanisms. Article 7 reproduces the ECD's general monitoring obligation. It prohibits

---

[83] DSA, recital 25. This article is called the 'Good Samaritan Clause' after the US's Communications Decency Act S.230. However, Article 6 appears different from the US' Good Samaritan Clause. Moreover, Savin argues that this article has no reforming effect, although it is a new addition to the immunity regime. See Andrej Savin, 'The EU Digital Services Act: Towards a More Responsible Internet' (2021) Copenhagen Business School Law Research Paper No 21-04, Journal of Internet Law 6 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3786792> accessed 10 September 2022. See also Eifert and others (n 9); Buiten (n 28) 2–4; Alexandra Kuczerawy, 'The Good Samaritan That Wasn't: Voluntary Monitoring Under the (draft) Digital Services Act' (*Verfassungsblog*, 12 January 2021) <https://verfassungsblog.de/good-samaritan-dsa/> accessed 10 September 2022.

[84] Peguera states that this was the ECJ's anticipation that such a 'Good Samaritan clause' was to be included in the DSA. See Peguera (n 30) 682–683.

[85] Kuczerawy (n 83).

the imposition of a general monitoring obligation and an obligation that would require intermediaries to seek facts or circumstances actively. As a general monitoring obligation is an important tool for confining the application of content moderation, it is crucial for the DSA to include this prohibition. However, it would not be realistic to expect that the existing fragmentation on the interpretation of general monitoring would fade, as the assessment of the scope of specific or general monitoring is for Member State courts in light of the ECJ's case law. Moreover, in terms of voluntary actions, intermediaries assess whether the implemented action qualifies as general or specific monitoring. This again raises questions over the protection of fundamental rights addressed above.

Following on, Article 8 sets out the framework for orders issued by national courts or administrative authorities against an intermediary which applies against a specific item of illegal content, ie injunction orders. In that regard, Member States are required to issue orders that clearly define the scope of a measure and that indicate the illegal content with information on its exact location, why it is considered illegal and its legal basis, as well as the redress mechanisms available under national or EU law. On the other hand, intermediaries must inform the issuing authority about the actions taken, such as the specific type of action and its effects. Similar conditions are also established for issuing an order requiring an intermediary to provide information on a specific user or users under Article 9. For both cases, intermediaries must also inform the recipient, whom the order concerns, about the order applied and the available redress possibilities.

Taking all these into account, it would not be wrong to conclude that Articles 8–9 are essential steps towards establishing more balanced enforcement mechanisms and a regulatory framework. As addressed, ensuring the protection of fundamental rights and a balance between the parties' powers and positions have proven challenging under the ECD. However, establishing the conditions and requirements for both the imposition and application of these orders, and giving parties the right to have an effective remedy, would undoubtedly assist in ironing out such concerns.

3.2 Due diligence obligations

The DSA establishes due diligence obligations for digital services in Articles 10–37. These obligations are perhaps the most significant aspect of the DSA. Digital services are classified into four categories: intermediaries (Articles 10–13), hosting intermediaries including online platforms (Articles 14–15), online platforms (Articles 16–24), and VLOPs and VLOSEs (Articles 25–33). As stated, the legislator's aim was to regulate new means of digital services (especially Big Tech) while benefiting from their technical and operational ability in preventing the availability of illegal content and protecting fundamental rights. Hence, considering digital

services according to their sizes and role within the online world appears to be fit for purpose. As a result of this approach, first, hosting intermediaries are distinguished from other intermediaries (namely, mere conduit, caching intermediaries), on whom more duties are imposed. Second, hosting intermediaries are differentiated depending on their service and their sizes. Hosting platforms which store and disseminate information are required to do more. Finally, online platforms and online search engines with more than 45 million recipients, VLOPs and the VLOSEs, have more formal and administrative duties.[86] This is sensible considering that these have technical and operational abilities and, perhaps more importantly, social and economic influence over the Internet. As the previous part shows, the impact exerted by these platforms should be balanced to create a fairer online environment. In this respect, the DSA imposes due diligence obligations regarding transparency, accountability and information. However, only the obligations relevant to the paper's main objective will be addressed here.

Starting with the transparency obligations, all intermediaries are required by Article 13 to publish a detailed report every year on the operation of their content moderation. The article also expressly stipulates what information should be included in the report. Briefly, information that would provide transparency regarding the intermediaries' way of tackling infringing content must be included in the report. For instance, the type of measures undertaken and the reasons, the timeframes for taking action against complaints received through the internal complaint-handling system, decisions undertaken against these complaints, etc. Article 13(1)(e) also requires the inclusion of information on 'any use made of automated means for the purpose of content moderation, including a qualitative description, a specification of the precise purposes, indicators of the accuracy and the possible rate of error of the automated means used in fulfilling those purposes, and any safeguards applied'. Importantly, this obligation is applicable for the measures undertaken as a result of injunction orders issued under Articles 8 and 9, as well as for actions undertaken as a result of intermediaries' initiatives. This is significant, especially for the concern arising from the lack of transparency in applying the voluntarily implemented measures. Such transparency reporting obligations should assist in balancing the distribution of power through the Internet since companies need to be more transparent about their content moderation technologies.

Further, these hosting intermediaries, including online platforms, are given more transparency duties concerning the application of notice and action mechanisms that they are obliged to implement within their system.[87] In addition to these, providers of online platforms are required

[86] Here, it should be underlined that fewer due diligence obligations are imposed on VLOSEs than on VLOPs. These obligations concern crisis response mechanism (Art 27a) and supervisory fees (Art 33a-b).

[87] DSA, Art 23.

to give more information since they are obliged to implement an internal complaint-handling system for their notice and action mechanisms and to make available out-of-court dispute settlement possibilities for their users.[88] Briefly, online platforms must include information on these in their reports, such as the number of disputes referred to an out-of-court dispute settlement body, which disputes are referred to the body, and the average time needed to complete the proceedings.[89] With regard to the notice and action and internal compliant-handling systems implemented, the decisions must be published and a statement of reasons given for the action taken without undue delay, and the information must be provided in a way that is user-friendly and easily accessible to the users.[90] A very similar obligation is also set for online advertisements.[91] Online platforms must display online advertisements clearly and unambiguously and inform users about the parameters to determine the target users for the advertisements. Finally, online platforms are required to publish a report demonstrating their average monthly active recipients of the service.[92] This is necessary to keep track of the number of their users as this is a standard set to distinguish an online platform from the VLOP.

VLOPs have more duties imposed on them. In terms of transparency obligations, further to the obligations stated above, they are required to create a repository for the advertisements presented on their online interfaces. This must be made available to the public and be presented until one year after the last time the advertisement was shown.[93] It is stated that this repository must consist of the relevant information concerning advertisements, such as the advertisement's content, the period of its display, and the natural or legal person on whose behalf the advertisement is displayed. Finally, additional transparency reporting obligations are imposed on VLOPs for the measures undertaken in dealing with illegal content. In addition to the duty – of every intermediary – to publish a report on the content moderation and measures applied, VLOPs are required to publish this report every six months. More importantly, they must include additional information on the human resources used in content moderation in the report.[94]

---

[88] DSA, Arts 17–18.

[89] DSA, Art 23(1).

[90] DSA, Art 23(2a).

[91] DSA, Art 24. The same transparency obligation is established for the recommender systems used by online platforms in Art 24(a).

[92] DSA, Art 23(2)-(3).

[93] DSA, Art 30.

[94] DSA, Art 33(1)(1): '(b) the human resources that the provider of very large online platforms dedicates to content moderation in respect of the service offered in the Union, for each official language of the Union as applicable, including for compliance with the obligations set out in Articles 14 and 19, as well as for compliance with the obligations set out in Article 17; (c) the qualifications and linguistic expertise of the persons carrying out the activities referred to in point (a), as well as the training and support given to such staff; (d) the indicators of accuracy and related information referred to in Article 13(1), point (e), per official languages of the Union, as applicable'.

Concerning the general framework on transparency obligations of the DSA, the first thing to say is that detailed and tiered rules on transparency should be welcomed. As shown, lack of transparency has been one of the obstacles in establishing a uniform and fair framework under the ECD. Intermediaries have had their own transparency reports on their content moderation activities, but these are mostly criticised for not containing crucial information. The DSA, however, sets out the standards for this. Information that must be included in these reports is clearly established. More significantly, the formality and stringency of these obligations are increased for online platforms and VLOPs, which are required to publish transparency reports on their content moderation technologies every six months. The obligations concerning online advertisements appear to be an effective tool in establishing a fairer digital environment. Advertisements are potent tools for big intermediaries to attract users and promote their content without their users' knowledge. This is done through the parameters used. Establishing transparency obligations on the advertisements presented in their online interface and the parameters used should provide more transparency and lead to fair use of the parameters. This could also assist in limiting the acquired impact and power of online intermediaries, especially VLOPs, over their users' choices and the way they disseminate information. Such transparency obligations might also indirectly have an impact on tackling illegal content, given that advertisement systems risk disseminating illegal content or financially incentivising harmful or illegal content. This appears to target where the ECD fell short regarding transparency. But the rules may still benefit from further insight. For instance, additional rules may be provided on the structure and content of the transparency reports to prevent platforms from publishing strategically structured reports.[95]

The notice and action mechanism established by the DSA should also be addressed with transparency obligations. The detailed reporting and transparency obligations set out for the notice and action mechanism appear assistive in determining the framework of the mechanism and providing more uniformly applied measures. However, whether the rules established by the DSA could deliver its promise as to the notice and action mechanism should be addressed.

In contrast to the ECD, the DSA explicitly requires hosting intermediaries, including online platforms, to implement notice and action mechanisms in their systems, and establishes the mechanism's elements to a certain extent. Articles 14–15 set the framework of the notice and action mechanism, then Articles 16–23 bring further obligations for online plat-

[95] BEUC position paper (n 77).

forms (excluding micro and small enterprises)[96] to ensure the protection of the fundamental rights of the parties affected by the application of the measures. The established system works in the following way: the hosting intermediary implements a mechanism that enables users to issue notifications electronically for the item claimed to be illegal. This notification, however, should include certain information on the claim to be regarded as valid and taken into account by a hosting intermediary.[97] In this regard, the issuer of the notification is first required to provide sufficient information, such as the exact URL(s) of the content, to a hosting intermediary for it to be able to identify the concerned content successfully. It is then required to substantiate its claim by providing the reasons why the concerned content is considered illegal, with evidence, if any. A statement of good faith confirming the accuracy of the claim and the completeness of information are other elements of a valid notification.

The issuance of a valid notice (ie a notice which comprises all the elements mentioned above) is vital for both the issuer and the hosting intermediary. First, the hosting intermediary can only take into account the notice and then act if it is valid. Second, being served a valid notice would give rise to actual knowledge or awareness if it allows 'a diligent provider of hosting services to identify the illegality of the relevant activity or information without a detailed legal examination'.[98] Here, again, the evaluation of diligence comes to the fore as a standard. As shown, the diligence assessment depends on the specifics of the case. The hosting intermediary should assess if the concerned notice would allow any other diligent provider to identify the illegality of the content before taking action. This assessment may result in the hosting intermediary triggering the knowledge/awareness threshold.[99] Hence, there is still a chance of the intermediary acting without properly examining the content. This might result in over-removals.

Reverting to the working principle of the mechanisms, the hosting intermediary must act against content claimed to be illegal or infringing once it has been served with a valid notification. It is also explained in recital 41(a) that identification of the illegality of content without a detailed legal examination means that the illegality of the content is clear. Against such content, a hosting intermediary may decide 'the removal of, the disabling of access to, the demotion of, the restriction of the visibility of the information or the suspension or termination of monetary payments

[96] DSA, Art 16. Micro and small enterprises are specified in Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises. According to Articles 2–3, 'a small enterprise is defined as an enterprise which employs fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million'; whereas 'a microenterprise is defined as an enterprise which employs fewer than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 2 million'.

[97] DSA, Art 14(2).

[98] DSA, Art 14(3).

[99] DSA, Art 14(3).

related to that information or [to] impose[s] other measures with regard to the information'.[100] The decision process should be carried out in a diligent, timely, objective and non-arbitrary manner.[101] The decision must be supported by a statement of reasons which includes information on the territorial scope and the duration of the decision; the legal grounds[102] proving why the specific action is taken; the facts and circumstances relied on; and whether the decision is made in light of information obtained as a result of the notification submitted or an injunction order or through its voluntary own-initiative investigations. More significantly, the issuer of the notice should be provided with clear and understandable information on the redress possibilities that might be pursued.

As far as the mechanism is concerned, it is evident that the DSA establishes a framework for the mechanism by setting out the minimum standards for hosting intermediaries to follow in tackling illegal content. More importantly, these rules set the standards for actions undertaken as a result of injunction orders as well as voluntary own-initiative investigations. As discussed above, as an enforcement mechanism, the application of the notice and action mechanisms[103] is directly related to protecting the parties' fundamental rights. However, the NTD mechanism stipulated by the ECD has failed to ensure this for all the parties concerned since crucial discretion to take down the content is left to intermediaries without providing any safeguards. Having set the minimum elements and having clarified what a valid notification should be composed of and what the hosting intermediary should do in assessing the claim, and what it should do after deciding on the action, the DSA provides significant insight and necessary attention to matters that the ECD has so far failed to consider. It is also substantial that transparency obligations support the rules on notice and action mechanisms. Besides, because the DSA is a regulation, the established framework would be expected to become more uniformly applied since the rules would be directly applicable and binding in all Member States. These can all be said to be the right steps to fulfil the regulation's main objectives: the protection of fundamental rights and harmonisation.

[100] DSA, Art 15(2)(a).

[101] DSA, Art 14 (6).

[102] DSA, Arts 15(2d)–15(2e). If the decision concerns a claim of illegality, the legal ground relied on making the decision should be provided with sufficient explanations. If, however, it concerns the content's incompatibility with TCs, the contractual ground relied on should be provided with sufficient explanations.

[103] The notice and action is an umbrella term comprising different variants of notice mechanisms categorised according to the type of action taken after receiving the notice, such as notice and takedown, notice and stay down, or notice and notice. For an examination of these different mechanisms from the fundamental rights aspect, see Christina Angelopoulos and Stijn Smet, 'Notice-and-fair-balance: How to Reach a Compromise Between Fundamental Rights in European Intermediary Liability' (2016) 8(2) Journal of Media Law 274; Alexandra Kuczerawy, 'From "Notice and Take Down" to "Notice and Stay Down": Risks and Safeguards for Freedom of Expression' (2019) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3305153>. For trademarks and the copyright aspect, see Genç-Gelgeç (n 37).

That said, the established system cannot be considered complete, as some significant elements require further attention. Perhaps the most important one is that the established system does not entitle users to the right to defend their case before the hosting provider takes action. This might be done by enabling the user to issue a counter-notice that consists of all the elements required by an individual who claims the illegality of the content. This notice would be contained in the information of why the user claims that the concerned content is not illegal, and it should be substantiated with legal or contractual grounds as well as evidence if there is any. Granting such a right would undeniably reinforce the protection of users' fundamental rights that might be affected, such as the right to be heard and the right to receive appropriate information about the status of proceedings.[104] However, the DSA obliges hosting intermediaries to inform users and make available the redress possibilities to them only after the decision is taken.[105] From this it follows that users are granted the right to an effective remedy under the DSA but not the right to be heard before the decision is taken.

Regarding remedial possibilities, users are given the right to lodge their complaint against the decision taken by online platforms through internal complaint-handling systems that online platforms (excluding micro and small enterprises) are obliged to put in place. As stated above, further obligations are imposed on online platforms on the ground that they not only store information – as hosting intermediaries do – but also disseminate that information to the public. The obligation to put an internal complaint-handling system in place is one of these additional obligations. Some hosting intermediaries have already implemented such procedures,[106] although not as a legal obligation. These are implemented within their TCs. Therefore, there were no general standards to follow.

The DSA establishes the minimum requirements that online platforms fulfil in the operation of the mechanism under Article 17. Under that article, users, including individuals or entities that have submitted a notice, should be provided with an internal-complaint handling mechanism to lodge their complaints electronically. The mechanism would be available for them at least for six months after the decision is referred to them.[107] The article further establishes the same general standards as set for the notice and action mechanism, ie complaints must be dealt with in a non-discriminatory, timely, and non-arbitrary manner. If the complaint is based on sufficient information and evidence proving that the decision should be reversed, then the online platform must reverse its decision

[104] Giancarlo Frosio and Christophe Geiger, 'Taking Fundamental Rights Seriously in the Digital Services Act's Platform Liability Regime' (2022) European Law Journal (forthcoming), s III-3.

[105] Eifert and others claim that these procedural remedies hardly provide protection of the fundamental rights enshrined by the EU Charter. See Eifert and others (n 9) 1012.

[106] Such as Facebook's Oversight Board. See n 44.

[107] DSA, Art 17(1).

and inform the complainant accordingly without delay. In fact, including reversal decisions, online platforms are obliged to inform complainants about every decision taken concerning their complaint and the possibilities of redress, including out-of-court dispute resolution.

Notably, online platforms are required to ensure that qualified staff are included in the decision process so that the decision is not taken solely based on automated means. This appears reasonable since qualified human intervention in the decision process would likely eliminate wrong decisions. For example, a qualified person could differentiate a copyright infringement from fair use with the provided evidence. On the other hand, it would be challenging for online platforms to employ such qualified staff. Illegality may arise from the infringement of different substantive rights, ranging from defamation to trademarks. Online platforms should then employ suitable human resources to tackle various infringements. It is also evident from the aforementioned report provided by Facebook that full automation in content moderation technologies has not been as effective as hoped.[108] They should also benefit from human intervention in their content moderation and the mechanism related to tackling illegal content. Nevertheless, to what extent online platforms would comply with this requirement remains to be seen.

Even though users are only given the right to lodge their complaints after the decision is taken, these are still essential safeguards to protect users' fundamental rights. Moreover, users may still pursue out-of-court dispute settlement or other available redress possibilities regarding the decision taken, including complaints that could not be settled through the internal complaint-handling system of online platforms. Out-of-court dispute settlement bodies are determined and certified by the Digital Service Coordinators (DSCs),[109] whom each Member State appoints as an authority responsible for the supervision of intermediaries in each Member State. The DSA also sets out the conditions to be certified as an out-of-court dispute settlement body in Article 18. Although this is not directly within the scope of this paper, one of the conditions is worth mentioning. Article 18(2b) requires the settlement body to have 'the necessary expertise in relation to the issues arising in one or more particular areas of illegal content, or in relation to the application and enforcement of terms and conditions of one or more types of online platforms'. Although it remains to be seen how this is to be applied in practice by each Member State and concerning the different substantive rights at stake, this should ensure the effectiveness of the process and the remedy in principle. Besides, as out-of-court dispute settlement bodies are certified by the DSCs, having standardised bodies would have a positive impact

[108] See n 51. See also Antonio A Casilli and Julián Posada Gutiérrez, 'The Platformization of Labor and Society' in M Graham and WH Dutton (eds), *Society and the Internet. How Networks of Information and Communication are Changing Our Lives* (2nd edn, OUP 2019) 12 <https://halshs.archives-ouvertes.fr/halshs-01895137/document> accessed 10 September 2022.

[109] DSA, Art 38.

on making the process uniform. On the other hand, the decisions held by these bodies are not binding, meaning that out-of-court dispute resolution is not the final remedy for users to apply. The dispute may always be brought to the court for judicial examination.[110]

Then, Article 18 sets out a rule on the costs of the process. If the decision is given in favour of the user,[111] the online platform bears the fees and reimburses the user. Otherwise, the user is not required to reimburse the fees or related expenses paid by an online platform unless it is held that it acted manifestly in bad faith. This rule incentivises users to apply for the remedy whilst making them refrain from lodging ungrounded and false claims before the body. In addition, online platforms are obliged to take measures to ensure notices submitted by trusted flaggers[112] are given priority by Article 19 and also obliged to apply certain measures set out in Article 20 to prevent misuse of the mechanisms, such as notice and action or internal complaint-handling systems. These articles reinforce the application and the framework of the mechanism.

Finally, Article 15(2)(a) should be mentioned with regard to the deficiencies of the established mechanism. This article permits hosting intermediaries to apply other measures to the illegal content. However, interpretation of the extent of different actions may give rise to fragmented applications. Hence, further guidance or safeguards should be provided on this.[113] Similarly, the precise scope of some of the standards set in the DSA, such as diligence, should be determined as far as possible so as not to result in ambiguous implementation. Article 14 also requires intermediaries to conduct their decision process in a timely manner, but

[110] DSA, Art 17(1)(1a).

[111] This includes the individual or entity that has submitted a notice.

[112] Trusted flaggers are private entities with special expertise in certain illegal content or activities; accordingly, they can issue notices regarding infringing activities relating to their expertise once their trusted flaggers status is confirmed. For a detailed assessment, see Savin (n 83) 9; Frosio and Geiger (n 104) s VI-1.

[113] In fact, Member States implement different variants of notice mechanisms within their domestic laws in order to tackle illegal content online, although the ECD stipulates NTD mechanisms. For instance, one of the variants of a notice and action mechanism, the so-called notice and disconnection or the graduated response scheme, was implemented in France by the (repealed) HADOPI law for copyright infringements. This mechanism requires intermediaries or authorised administrative agencies to apply sanctions gradually – and the last one usually being the suspension of Internet access – after receiving a certain number of notifications. For a detailed examination, see Maria Frabboni, 'File Sharing and the Role of Intermediaries in the Marketplace: National, European Union and International Developments' in Irini A Stamatoudi (ed), *Copyright Enforcement and the Internet* (Kluwer Law International 2010) 119, 136–137; Andres Guadamuz, 'Developments in Intermediary Liability' in Andrej Savin and Jan Trzaskowski (eds), *Research Handbook on EU Internet Law* (Edward Elgar 2014) 312, 333–336.

there is nothing to assist intermediaries in determining what should be considered timely.[114]

3.3 Enforcement

Last but not least, the enforcement rules of the DSA should be considered. As will be shown, the DSA sets out a framework for enforcing the rules. This is important and needed, given that the DSA imposes obligations on digital platforms. So far, the paper has demonstrated that the above rules are promising in providing answers to the issues raised by the ECD. However, their desired effect can only be ensured with effective enforcement. The ECD does not provide enforcement rules, as this is left to the cooperation of the Member States and the codes of conduct at the EU level.[115] Although this is compatible with the ECD's approach, it is difficult to conclude that it has impacted uniformity positively and hugely. The EU-level enforcement authority that would work with the Member States in implementing or enforcing the rules would have been assistive for effective enforcement.[116]

Fortunately, the DSA sets out enforcement rules and sanctions to urge providers to comply with the rules and obligations. The enforcement powers are distributed among different actors, mainly the DSCs and the European Commission. There is also the European Board of Digital Services (the Board), composed of the DSCs. However, the Board works as an advisory to the main enforcement actors: the DSCs and the Commission. The DSCs are appointed[117] by each Member States as a competent authority. Their primary duty is to ensure coordination at the national level. Hence, they are responsible for supervision, intermediaries' compliance with the rules, and the consistency and effectiveness of the application of the rules.[118] As the DSCs are considered responsible authorities of the Member States for matters related to the DSA and are required to carry out several tasks, Member States are required to appoint a DSC with sufficient technical, financial and human resources. To carry out their tasks, the DSCs are entitled to have both investigation and enforcement powers such as requiring information from providers, even making on-

[114] There are two studies pointing out the existence of such fragmentation in the application of these standards. For example, one study concluded that the time frame for intermediaries to take action after receiving a notice ranges from three hours to ten days. See Sjoera Nas, 'The Multatuli Project ISP Notice & Take Down' (*SANE*, 1 October 2004) <https://www-old.bof.nl/docs/researchpaperSANE.pdf>. See also Christian Ahlert, Chris Marsden and Chester Yung, 'How 'Liberty' Disappeared from Cyberspace: The Mystery Shopper Tests Internet Content Self-Regulation' (2004) <https://www.academia.edu/686683/How_Liberty_Disappeared_from_Cyberspace_The_Mystery_Shopper_Tests_Internet_Content_Self_Regulation/>. For a detailed examination, see Genç-Gelgeç (n 37) 170–174.

[115] ECD, Arts 16–20.

[116] De Streel and Husovec (n 14) 18; De Streel and others (n 50) 81–82.

[117] 'Within two months from the date of entry into force of this Regulation' according to the DSA Art 38(3).

[118] DSA, Art 41.

site inspections of the premises in assessing their compliance with the rules or dealing with specific infringement and perhaps, more importantly, imposing fines when an intermediary fails to comply with the rules.[119] The DSA puts a cap on the amount of penalties[120] to be imposed on intermediaries and leaves the Member States to set the standards for the fines and penalties.

On the other hand, regarding VLOPs and VLOSEs, the Commission is responsible for supervising and enforcing the rules concerning them. Hence, the Commission is vested with both investigation and enforcement powers.[121] Some of the Commission's powers in this respect are as follows: conducting an assessment on the compliance of the due diligence obligations, including transparency obligations that are imposed on VLOPs and VLOSEs; taking necessary actions against the non-compliance[122] and other matters found in the independent audits;[123] investigating suspected infringements[124] or requesting relevant information as to such infringements[125] or non-compliance and imposing fines and penalties.[126] However, VLOPs and VLOSEs must be given the right to be heard and to access the file before the Commission decides on non-compliance, fines and penalties.[127] It is also made clear that the Court of Justice has unlimited jurisdiction to review the Commission's decision on penalties and fines.[128]

As briefly shown, the DSA establishes an enforcement regime that the ECD lacks. This is aimed to operate at the EU level. This should be welcomed as the enforcement rules appear to support the obligations. The distribution of powers and the encouragement of cooperation amongst them appear an important tool to avoid potential setbacks of centralised enforcement, such as long-delayed enforcement.[129] On the

[119] DSA, Art 41.

[120] DSA, Art 42(3) establishes 'the maximum amount of penalties imposed for a failure to comply with the obligations laid down in this Regulation shall not exceed 6% of the annual worldwide turnover of the provider of intermediary services concerned. Penalties for the supply of incorrect, incomplete or misleading information, failure to reply or rectify incorrect, incomplete or misleading information and to submit to an on-site inspection shall not exceed 1% of the annual worldwide turnover of the provider concerned'. Then, Art 42(4) states 'the maximum amount of a periodic penalty payment shall be 5% of the average daily worldwide turnover or income of the provider of intermediary services concerned in the preceding financial year per day, calculated from the date specified in the decision concerned'.

[121] DSA, Art 50.

[122] DSA, Art 58.

[123] DSA, Art 28.

[124] DSA, Art 51.

[125] DSA, Arts 52–54.

[126] DSA, Art 59.

[127] DSA, Art 63.

[128] DSA, Art 64(a).

[129] With regard to the GDPR, see European Commission, 'Data protection as a pilar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation' (Communication) COM(2020) 264 final.

other hand, the established system should be criticised for its potential ineffectiveness. The DSA prescribes that the DSCs must be technically and financially sufficient. Given that the DSCs' powers include carrying out investigations, identification of infringements and imposition of fines, they indeed should be capable of performing these tasks. However, this is easier said than done. This would require Member States to allocate human and financial resources. Concerning the GDPR, one report shows that the Member States hardly provided such resources and the Data Protection Authorities (DPAs)[130] are barely equipped with sufficient technical staff.[131] One of them is the Irish DPA, responsible as lead authority for the compliance of some Big Tech companies (such as Google and Facebook) with the GDPR, although it receives more complaints than any other DPA. Unsurprisingly, it receives criticism for the lack of effective enforcement of the GDPR and data protection in general.[132] This indicates the importance of providing resources for effective enforcement.

Given that this report was published two years after the GDPR came into effect, it offers illustrative facts for the DSA. The DSA requires Member States to establish their DSCs within fifteen months from its entry into force.[133] However, this would not necessarily mean that the supervision and enforcement of the rules will effectively take place accordingly. This would not happen unless the DSCs were provided with sufficient resources to perform their tasks. It is also possible that uneven resourcing might result in different levels of enforcement among the Member States. Moreover, the DSA requires the DSCs to cooperate and the Member States to make their technical staff available to the Commission for matters related to VLOPs and VLOSEs. This makes resourcing even more critical for fulfilling the objective of effective enforcement. It is hence vital to ensure effectiveness in the designation of the DSCs and to take lessons from the GDPR.

The power vested in the Commission concerning VLOPs and VLOSEs may also be criticised. Given that the non-compliance of VLOPs and VLOSEs might have a potential cross-border effect in the EU, this cen-

---

[130] Which are the responsible authorities of the compliance and supervision of the GDPR at national level.

[131] Johnny Ryan and Alan Toner, 'Europe's Governments Are Failing the GDPR Brave's 2020 Report on the Enforcement Capacity of Data Protection Authorities' (*Brave,* April 2020) <https://brave.com/static-assets/files/Brave-2020-DPA-Report.pdf> accessed 10 September 2022. For example, the report reveals that 'only 6 national DPAs have more than 10 specialist tech investigation staff'; 'data protection authorities have 2 tech specialists or less'; 'half of all national DPAs receive small (€5 million or less) annual budgets from their governments'.

[132] Madhumita Murgia and Javier Espinoza, 'Ireland Fails to Enforce EU Law against Big Tech' *Financial Times* (London, 13 September 2021) <www.ft.com/content/5b986586-0f85-47d5-8edb-3b49398e2b08> accessed 10 September 2022; Samuel Stolton, 'MEPs Rue Lack of GDPR Sanctions Issued by Irish Data Authority' (*Euractiv*, 26 March 2021) <www.euractiv.com/section/data-protection/news/meps-rue-lack-of-gdpr-sanctions- issued-by-irish-data-authority> accessed 10 September 2022.

[133] DSA, Art 38(3).

tralised-like approach might assist in more effective enforcement. That being said, the exclusive powers given to the Commission may put this body in a position different from the one it was originally assigned. As an executive arm of the EU, its principal role is to propose new laws and monitor their implementation. However, the DSA gives a central role to the Commission in enforcing the rules. This might create a conflict of interests as the Commission is the body that proposes the law and then imposes fines for non-compliance, which might indicate the deficiencies of the DSA that it itself proposed. This might also negatively impact the separation of EU powers.[134]

Finally, it ought to be mentioned that the Commission's exclusive powers should be without prejudice to certain administrative tasks assigned to the DCSs.[135] Cooperation between the Commission, the Board, the DSCs and the Member States' competent authorities is encouraged by the DSA. These are assistive in ironing out the potential setbacks of enforcement and in ensuring effectiveness and unity in enforcement. That being said, how smoothly this could be applied in practice remains to be seen.

4 Conclusion

The task of this paper was to scrutinise the DSA to address whether it could iron out the deficits of the ECD. To do so, first the ECD's deficiencies were identified. Second, the rules established by the DSA were examined to answer the paper's question.

The ECD has been the law applicable to Internet intermediaries related to their liability for third-party content on their platform, electronic contracts and e-commerce activities for over twenty years. It was based on the objectives of facilitating the free movement of digital services within the EU and fostering innovation and e-commerce activities. To fulfil these objectives, a harmonised immunity regime was established for certain services of intermediaries, ie mere conduit, caching, and hosting. This means that the providers of these services might be granted immunity from liability arising from the infringing content made available by their users on their platform, provided that the conditions set out by the ECD in Articles 12–14 are met. These conditions are set out to assess the intermediaries' involvement in the availability of illegal content uploaded by their users. This is because the immunity is granted to an intermediary whose operation remains technical and passive as to the infringing content made available on its platform. This being the general framework of the ECD's immunity regime, most of the matters associated with this regime, such as procedures and conditions of the NTD mechanism, are

[134] Suzanne Vergnolle, 'Enforcement of the DSA and the DMA: What Did We Learn from the GDPR?' in Heiko Richter, Marlene Straub and Erik Tuchtfeld (eds), *To Break Up or Regulate Big Tech? Avenues to Constrain Private Power in the DSA/DMA Package* (2021) Max Planck Institute for Innovation and Competition Research Paper No 21-25, 103, 107.

[135] DSA, Art 84(b).

left for the Member States to deal with under their national law. The Member States are provided with further insight into applying the rules either when the matters were referred to the ECJ or when the EU Commission publishes the codes of conduct or additional communications.

The above appraisal indicates that the most challenging issues of the ECD are the lack of harmonisation and the discretion given to the intermediaries. Concerning the lack of harmonisation, the fragmentation primarily arises from the interpretation of the rules concerning hosting intermediaries, the implementation and the application of the NTD mechanism, and the prohibition of the general monitoring obligation. Regarding the conditions established for hosting intermediaries, the ECJ sets out a neutrality test for courts to apply in distinguishing active intermediaries from passive ones. However, the application of this test has not been straightforward in practice. Hence, it has led to divergent applications.[136] Moreover, the test was not assessed by the ECJ concerning today's extensive content moderation technologies, so the application of the test to these remains open to divergent applications. Besides, the application of the NTD mechanism has proven to be challenging in providing harmonisation, as each Member State establishes the standards and elements of the NTD systems within their corresponding national law. The rules on this have been heavily fragmented.[137] In the same vein, the interpretation of the prohibition of the general monitoring obligation has been divergent among the EU Member States.

Another setback of the ECD's framework is the discretion given to hosting intermediaries. As demonstrated, hosting intermediaries are provided with powers similar to a judge in dealing with illegal content. As the ECD requires the hosting intermediary to act against illegal content made available on its platform, it puts the hosting intermediary in the position of a judge. When the notice is received as to the illegality of content, the intermediary assesses the notice and claim and then decides whether or not to take down the content. The ECD does not establish rules, standards or safeguards for intermediaries to follow in this respect. Hence, the rules and procedures have been formed by intermediaries' TCs and through the application of their self-implemented mechanisms. In default of any transparency rules, matters related to the moderation procedures, such as how they act against the illegal content and how they apply their mechanisms, are left under their control and discretion. This strengthens the intermediaries' position within the digital world as they may act almost like a lawmaker. More crucially, the protection of fundamental rights is also left to intermediaries. As shown, the application of NTD directly impacts on the parties' fundamental rights. The ECD leaves the task of protecting and balancing the rights at stake to intermediaries

[136] De Streel and Husovec (n 14) 42.

[137] Commission, Online Services, Including e-Commerce, in the Single Market Accompanying the document Communication on 'A coherent framework to boost confidence in the Digital Single Market of e-commerce and other online services' SEC(2011) 1641 final 3.4.4.

– which are private parties – without providing any safeguards.

After identifying these as the deficiencies of the ECD's framework, this paper examined the DSA. In light of this, the very first thing to conclude is that the DSA appears to target matters related to which the ECD fell short. Therefore, it should be welcomed.

First, the DSA's adopted approach to regulating intermediaries appears appropriate to fulfil its objectives. Its main aim is to ensure the adequate functioning of digital services within the EU by striking a balance between the powers and responsibilities of intermediaries of different sizes and by protecting the fundamental rights of all parties. To fulfil these tasks, attention is placed on digital services, especially on Big Tech companies and their infrastructural advantages. Therefore, new sets of due diligence obligations are imposed on them. These rules are established depending on the size and roles of the intermediaries within the online world. Accordingly, the providers of digital services are classified into four categories: intermediaries, hosting intermediaries including online platforms, online platforms, and VLOPs and VLOSEs. This is an important change in the legal framework, and it is promising one to strike a balance between the different sizes of digital services.

Second, the DSA establishes much-needed rules for notice and action mechanisms. Hosting intermediaries must implement notice and action mechanisms in their systems by the DSA. In line with this, they are provided with minimum standards for the mechanism, such as the system's specifications or what constitutes a valid notice. They are obliged to support their decision regarding the claim with a statement of reasons, including the legal grounds, of why the specific decision is taken, the duration and territorial scope of the decision, etc. The notice issuer should also be provided with information on the possibilities of redress. Furthermore, online platforms are required to implement internal-complaint handling systems and make available out-of-court dispute resolution mechanisms. The standards related to these are also established to some extent. Furthermore, hosting intermediaries, online platforms and VLOPs are required to comply with different levels of transparency and information obligations concerning the notice and action mechanism. These obligations play a significant role in setting the standards in the application of the rules, eliminating intermediaries' discretion in applying enforcement mechanisms, and striking a balance between the parties' fundamental rights.

Third, the DSA establishes detailed and tiered reporting and transparency obligations. This is significant as the lack of transparency is identified as one of the deficiencies of the ECD that leads to fragmentation and unfair applications. The DSA requires all digital platforms to have transparency reports and sets the standards for them. The level of obligations is increased for online platforms and VLOPs. They are also obliged to ensure transparency in their advertisements. These moves ap-

pear promising in establishing a more uniform and fairer framework and limiting intermediaries' discretion on the application of content moderation.

Last but not least, the DSA creates an enforcement regime that the ECD lacks. This means that the obligations are supported by enforcement rules, although their effectiveness can be criticised. The decentralised approach of the enforcement mechanism distributes enforcement and investigation powers through the DSCs and the European Commission. There is also the Board which works as an advisory to them. The DSCs are appointed by the Member States and are made responsible for coordination at the national level, while the Commission is vested with enforcement powers as to the VLOPs and VLOSEs. As shown, both are empowered to impose fines and penalties in the case of non-compliance.

As a concluding remark, it should be underlined that the DSA cannot be considered complete, although its framework appears full of promise. As indicated, some issues require further attention. Although these are not discussed in detail here, they should be recalled. Starting with the established notice and action mechanism, the DSA misses an opportunity to entitle the user to issue a counter-notice which would ensure the protection of and balance between the fundamental rights of the parties. As addressed, users are given the right to lodge their claim only after an intermediary takes the decision. As far as the immunity rules are concerned, the DSA also appears to fail to clarify the application of the neutrality standard. The DSA, like its predecessor, does not take account of new technologies and the content moderation activities of intermediaries in relation to the immunity regime. Despite the evident interrelation between the application of the immunity rules and the obligations imposed, the opportunity to come up with a more complete and straightforward immunity regime appears not to have been seized. Clarification on the interpretation of standards, such as general monitoring and diligence, may also be needed for uniformity. As for the due diligence obligations, it is doubted how many of them will be embraced by digital platforms. The enforcement regime is established, but questions about its effectiveness are also raised. How effectively this will work and if the DSA can deliver the promise of a new regime may only be seen after the rules come into force and are applied in practice.

This work is licensed under the *Creative Commons Attribution – Non-Commercial – No Derivatives 4.0 International License*.

Suggested citation: B Genç-Gelgeç, 'Regulating Digital Platforms: Will the DSA Correct Its Predecessor's Deficiencies?' (2022) 18 CYELP 25.