jipitec

5 | 2021

Volume 12 (2021)
Issue 5 ISSN 2190-3387

Journal of
Intellectual Property,
Information Technology,
and Electronic Commerce
Law

www.jipitec.eu

jipitec

Journal of Intellectual Property, Information Technology and Electronic Commerce Law

Volume 12 Issue 5
www.jipitec.eu
contact@jipitec.eu

A joint publication of:

Prof. Dr. Thomas Dreier, M. C. J. (NYU)
KIT - Karlsruher Institut für Technologie, Zentrum für Angewandte Rechtswissenschaft (ZAR), Vincenz-Prießnitz-Str. 3, 76131 Karlsruhe Germany

Prof. Dr. Axel Metzger, LL. M. (Harvard)
Humboldt-Universität zu Berlin, Unter den Linden 6, 10099 Berlin

Prof. Dr. Gerald Spindler
Dipl.-Ökonom, Georg-August-Universität Göttingen, Platz der Göttinger Sieben 6, 37073 Göttingen

Karlsruhe Institute of Technology, Humboldt-Universität zu Berlin and Georg-August-Universität Göttingen are corporations under public law, and represented by their respective presidents.

ISSN 2190-3387

Funded by

DGRI Deutsche Gesellschaft für Recht und Informatik e.V.

Table Of Contents

Editorial

Articles

Book Reviews

Editorial

by **Gerald Spindler**

Recommended citation: Gerald Spindler, Editorial, 12 (2021) JIPITEC 360 para 1.

1 The new issue of JIPITEC provides a good example for the wide range of issues that are prominent today in legal discussions around the globe. One accent lies upon intellectual property rights problems such as the highly debated intermediary liability of internet platforms that the recently proposed Digital Services Act of the EU attempts to tackle and which is discussed by the article of Miriam C. Buiten. Also dealing with the Digital Services Act, but with a focus on the out of court dispute settlement mechanisms, is Jörg Wimmers. Moreover, new phenomena are arising already like Non-Fungible Tokens in copyright transactions, where Adarsh Vijayakumuran gives us an insight to global perspectives on these blockchain based new forms of integrating tokenization and copyright. More dedicated to a specific limitation in copyright, the article of Gabriele Spina Ali deals with the parody exception as provided by Article 17 (7) of the DSM-Directive and its missing implementation in Italy. Also related to copyright law, Maurice Schellekens' article covers the recent discussion on framing links as it has been accentuated by the CJEU recently.

2 While the bulk of articles concerns more or less new developments in copyright law, IT-security is also a hot topic debated at the EU level. Within this realm, the article of Sandra Schmitz and Stefan Schiffner deepens current questions about responsible vulnerability disclosure under the NIS 2.0-proposal—an issue which is central for the time span between detecting security flaws and their disclosure.

3 Finally, a special article is dedicated to developments in transnational data transfer of personal data under the Turkish personal data protection law by Sevde Pelen. Whereas the legal landscape regarding the GDPR provisions is well known little can be found concerning other (neighbouring) countries.

4 Last but not least, the issue is completed with two book reviews: one on the responsibility of online intermediaries, a front-runner of the EU-Digital services act, written by Folkert Wilman, and the other one covering the impact of artificial intelligence on competition regulation in the Data Economy by Gintarė Surblytė-Namavičienė.

5 This short overview reflects the balance of issues to which JIPITEC is dedicated, as well as its European and global orientation. May the reader enjoy this new issue!

Prof. Dr. Gerald Spindler

The Digital Services Act From Intermediary Liability to Platform Regulation

by **Miriam C. Buiten***

Abstract: The proposed Digital Services Act (DSA) aims to reconcile the responsibilities of online platforms with their position as key intermediaries and essential sources and shapers of information. The DSA proposes new, asymmetric obligations while maintaining the liability exemption for hosting providers. This article aims to provide an overview of the tiered obligations and to critically evaluate the regulatory approach of the DSA. The article calls into question whether the liability exemption based on playing a passive, neutral role reflects the extensive moderation that online platforms undertake as part of their business model. It considers the consequences of taking the responsibility of online platforms out of the domain of liability and into the domain of regulation and suggests alternative approaches to the liability regime.

Keywords: Digital Service Act; Liability; Online Platforms; Platform Regulation

Recommended citation: Miriam C. Buiten, The Digital Services Act: From Intermediary Liability to Platform Regulation, 12 (2021) JIPITEC 361 para 1.

A. Introduction

1 On 15 December 2020, the European Commission presented drafts for both a Digital Services Act (DSA) and a Digital Markets Act (DMA).[1] The DSA aims to reconcile the responsibilities of online platforms with their increased importance. Since the adoption of the e-commerce Directive two decades ago, online platforms have evolved into key intermediaries in the digital economy, as well as essential sources and shapers of information. They have developed from passive, neutral intermediaries to active co-creators of the digital sphere. In the attention economy, digital services and content are optimised to benefit online platforms' advertising-driven business models. A central component of this business model is the moderation of content in order to encourage users to spend more time on the platform and share more personal data. Today's search engines, social media networks and e-commerce platforms determine not only which users can participate in the ecosystem or the way transactions are to be carried out via the platform but also what information corresponding users will receive.

* Assistant Professor at the University of St. Gallen. This article builds on Miriam C. Buiten, 'Der Digital Services Act (DSA): Vertrautes Haftungsregime, neue Verpflichtungen' [2021] Zeitschrift für Europarecht (EuZ) 102.

1 On the DMA, see eg Matthias Leistner, 'The Commission's vision for Europe's digital future: proposals for the Data Governance Act, the Digital Markets Act and the Digital Services Act—a critical primer' [2021] Journal of Intellectual Property Law & Practice (JIPLP) <https://doi.org/10.1093/jiplp/jpab054> accessed 31 May 2021; Damien Geradin, 'The DMA proposal: Where do things stand?' (*The Platform Law Blog*, 27 May 2021) <https://theplatformlaw.blog/2021/05/27/the-dma-proposal-where-do-things-stand/> accessed 31 May 2021; Andreas Heinemann and Giulia Mara Meier, 'Der Digital Markets Act (DMA): Neues "Plattformrecht" für mehr Wettbewerb in der digitalen Wirtschaft' [2021] Zeitschrift für Europarecht (EuZ) 86.

2 Online platforms' business models have proven vulnerable to new risks, both for society at large and for individual users.[2] Specifically, platforms have demonstrated to be a fertile breeding ground for illegal activities, such as the unlawful distribution of copyrighted works on video-sharing platforms, the sale of counterfeit goods on e-commerce platforms or the dissemination of hate speech and content glorifying violence on social media platforms.[3] The increasing spread of disinformation via such platforms is met with ever-growing concern.[4] Concurrently, the first legislative attempt at EU level to make platforms directly liable for illegal content under the Copyright Directive[5] triggered public protests[6] and criticism from academics,[7] as it was feared that this would result in online censorship.

3 Amidst the apprehension concerning disinformation on the one hand, and censorship on the other, online platforms have come under pressure to do both less and more to monitor their platforms.[8] In 2018, Facebook was accused of failing to adequately address calls for violence against Muslim minorities in Myanmar.[9] Recently, Facebook and Twitter were criticized after permanently suspending Donald Trump's account following his comments about violence at the US Capitol in 2021.[10] These examples illustrate that the debate revolving around platform responsibility reaches beyond the question of platforms' liability in curbing illegal content. It is about the role of platforms in removing harmful content and the disadvantages of platforms having too much power in deciding what content to show.

4 In December 2020, the Commission proposed new horizontal rules for platforms in the DSA, intending to modernise the e-commerce Directive. The Commission has chosen to leave the liability regime of the e-commerce Directive untouched, and instead to regulate how online platforms are to remove il-

2 European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC' COM (2020) 825 final (DSA), recital 56 preamble: "*The way they design their services is generally optimised to benefit their often advertising-driven business models and can cause societal concerns*".

3 See on the infringement of copyrights, trademarks, design rights and patents, eg OECD and European Union Intellectual Property Office, 'Trends in Trade in Counterfeit and Pirated Goods' (Illicit Trade, OECD Publishing 2019) <https://doi.org/10.1787/g2g9f533-en> accessed 5 May 2021.

4 See European Commission, 'Flash Eurobarometer 464 Report on Fake News and Online Disinformation' (12 March 2018) <https://ec.europa.eu/digital-single-market/en/news/final-results-eurobarometer-fake-news-and-online-disinformation> accessed 5 May 2021.

5 Parliament and Council Directive 2019/790/EU 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 L 130/92.

6 Elisabeth Schulze, 'Thousands Protest Against Controversial EU Internet Law Claiming It Will Enable Online Censorship' (*CNBC*, 19 March 2019) <www.cnbc.com/2019/03/25/protesters-in-germany-say-new-eu-law-will-enable-online-censorship.html> accessed 28 April 2021; Morgan Meaker, 'Inside the Giant German Protest Trying to Bring Down Article 13' (*Wired*, 26 March 2019) <https://www.wired.co.uk/article/article-13-protests> accessed 28 April 2021.

7 Christina Angelopoulos, 'Harmonising Intermediary Copyright Liability in the EU: A Summary' in Giancarlo Frosio (ed), *The Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020).

8 See eg Miriam C. Buiten, Alexandre De Streel and Martin Peitz, 'Rethinking Liability Rules for Online Hosting Platforms Rethinking Liability Rules for Online Hosting Platforms' (2019) 27 International Journal of Law And Information Technology (IJLIT) 139; Natali Helberger and others, 'The Information Society An International Journal Governing Online Platforms: From Contested to Cooperative Responsibility' (2018) 34 The Information Society 1.

9 Steve Stecklow, 'Hatebook' <https://www.reuters.com/investigates/special-report/myanmar-facebook-hate/> accessed 28 April 2021; Alexandra Stevenson, 'Facebook Admits It Was Used to Incite Violence in Myanmar' *The New York Times* (New York, 6 November 2018) <www.nytimes.com/2018/11/06/technology/myanmar-facebook.html> accessed 28 April 2021; Olivia Solon, 'Facebook Struggling to End Hate Speech in Myanmar Investigation Finds' *The Guardian* (London, 16 August 2018) <www.theguardian.com/technology/2018/aug/15/facebook-myanmar-rohingya-hate-speech-investigation> accessed 28 April 2021; 'Facebooks halbherziger Kampf gegen den Hass' *Der Spiegel* (Hamburg, 16 August 2018) <www.spiegel.de/netzwelt/web/facebook-in-myanmar-halbherziger-kampf-gegen-den-hass-a-1223480.html> accessed 28 April 2021.

10 Kate Conger and others, 'Twitter and Facebook Lock Trump's Accounts After Violence on Capitol Hill' *The New York Times* (New York, 6 January 2021) <www.nytimes.com/2021/01/06/technology/capitol-twitter-facebook-trump.html> accessed 28 April 2021; Charlie Savage, 'Trump Can't Block Critiques From His Twitter Account, Appeals Court Rules' *The New York Times* (New York, 9 July 2019) <www.nytimes.com/2019/07/09/us/politics/trump-twitter-first-amendment.html> accessed 28 April 2021; Ryan Browne, 'Germany's Merkel Hits Out a Twitter Over Problematic Trump Ban' (*CNBC*, 11 January 2021) <www.cnbc.com/2021/01/11/germanys-merkel-hits-out-at-twitter-over-problematic-trump-ban.html> accessed 28 April 2021.

legal content. The DSA provides for a tiered regulation differentiating between intermediaries, hosting providers, online platforms and very large online platforms ("VLOPs").[11] The new obligations for these digital service providers include measures to combat illegal online content under the notice and takedown procedure, the introduction of an internal complaints management system enabling users to challenge decisions made by platforms to block or remove content, as well as far-reaching duties for VLOPs.

5 This article aims to provide an overview of the tiered obligations and to critically evaluate the regulatory approach of the DSA. The article questions the choice of maintaining the passive/active distinction from the e-commerce Directive in relation to the liability of hosting providers, especially when considering the extensive moderation that online platforms undertake as part of their business model. It argues that a more significant leap in the liability framework for online platforms would have been to work towards better, more precise and, above all, more accountable and transparent content moderation, rather than maintaining a focus on notice and takedown. It proposes sanctioning non-compliance with DSA obligations with losing the liability exemption, turning the DSA obligations into a standard of liability for platforms. The article finds that, by opting for fines and periodic penalty payments, the DSA pulls the responsibility of intermediaries out of the realm of liability, and into the area of regulation.

6 The article is structured as follows. Section B summarises the aims and approach of the DSA proposal. Section C discusses the liability regime of the e-commerce Directive, as adopted in the DSA proposal. Section D lays out the due diligence obligations imposed by the DSA, as well as the additional obligations for hosting providers, online platforms and VLOPs. Section E considers the sanction regime of the DSA proposal, followed by a conclusion in Section F.

B. Aims and approach

I. Background: Recent sector-specific reforms

7 Since the adoption of the e-commerce Directive in 2000, sectoral rules as well as co- and self-regulatory measures have been adopted to supplement the basic horizontal regime.[12] Self- and co-regulation was promoted inter alia with the adoption of a "Memorandum of understanding on the sale of counterfeit goods on the internet"[13] in 2011, with the establishment of an Alliance to Better Protect Minors Online[14] in 2017, with a Multi-Stakeholders Forum on Terrorist Content[15] in 2015, with the adoption of an EU Code of Conduct on Countering Illegal Hate Speech Online[16] in 2016 as well as a Code of Practice on Disinformation[17] in 2018.[18]

8 In the meantime, service providers developed tools aside from notice and takedown systems to fight illegal content on their platforms. In 2017, Amazon started cooperating with brands to detect counterfeits by tagging each product with a unique barcode.[19] YouTube uses an identification database

11 The remainder of this article follows the terminology used in the DSA, which assigns a specific meaning to the term "online platform". On the Typology of Online Platforms see further Jaani Riordan, *The liability of internet intermediaries* (Oxford University Press 2016).

12 For an overview, see Buiten, De Streel and Peitz (n 8) 139; Alexandre De Streel and Martin Husovec, 'The e-commerce Directive as the cornerstone of the Internal Market: Assessment and options for reform' (Study for the European Parliament, May 2020) <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648797/IPOL_STU(2020)648797_EN.pdf> accessed 19 May 2021.

13 European Commission, 'Memorandum of understanding on the sale of counterfeit goods on the internet' <https://ec.europa.eu/growth/industry/policy/intellectual-property/enforcement/memorandum-understanding-sale-counterfeit-goods-internet_en> accessed 12 May 2021.

14 European Commission, 'Alliance to better protect minors online' <https://ec.europa.eu/digital-single-market/en/alliance-better-protect-minors-online> accessed 12 May 2021.

15 European Commission, 'EU Internet Forum: Bringing together governments, Europol and technology companies to counter terrorist content and hate speech online' (Press release IP/15/6243, 3 December 2015) <https://ec.europa.eu/commission/presscorner/detail/en/IP_15_6243> accessed 12 May 2021.

16 European Commission, 'The EU Code of conduct on countering illegal hate speech online' <https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en> accessed 18 May 2021.

17 European Commission, 'Code of Practice on Disinformation' <https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation> accessed 12 May 2021.

18 See further De Streel and Husovec (n 12) 27.

19 Amazon, 'Transparency' <https://brandservices.amazon.com/transparency> accessed 28 April 2021.

in cooperation with rightsholders to identify illegal uploads of copyrighted videos.[20] WhatsApp had to restrict message forwarding after the rapid spread of dangerous misinformation led to deaths in India in 2019.[21]

9 Two soft law instruments, the 2017 Communication on illegal content online[22], followed by a 2018 Recommendation on illegal content online[23], aimed at improving the effectiveness and transparency of the notice and takedown procedure between users and platforms, to encourage preventive measures by online platforms, and to improve cooperation between hosting service providers, trusted flaggers and authorities.

10 Sector-specific rules have been adopted for particularly harmful types of content. The Child Sexual Abuse Directive (2011) requires member states to ensure that intermediaries promptly remove websites that contain or distribute child pornography;[24] the Counter-Terrorism Directive (2017) requires member states to ensure the prompt removal of online content that constitutes a public solicitation to commit a terrorist offence;[25] and the revised Audiovisual Media Services Directive (AVMSD) 2018 requires video platforms that host content for which they have no editorial responsibility, such as videos posted by users, to take measures with regards to harmful content in the areas of terrorist and racist subject matters, child pornography and hate speech to the general public.[26]

11 The DSM Copyright Directive (2019) requires that online content-sharing service providers use their best efforts to obtain licences for content posted by their users and holds them liable for copyright or related rights infringement if they do not remove the material after notification and prevent its reappearance.[27] A 2019 regulation moreover promotes fairness and transparency of online platforms towards business users and requires platforms to provide terms and conditions that are easily understandable to an average business user.[28]

12 As part of the Digital Single Market Strategy adopted in 2015, the European Commission identified the promotion of fairness and responsibility of online platforms as an area in which further action is needed to ensure a fair, open and safe digital environment.[29] After the Von der Leyen Commission announced[30] that it would propose a new law to mod-

20 Google, 'How Content ID Works' <https://support.google.com/youtube/answer/2797370?hl=en> accessed 28 April 2021.

21 Zeba Siddiqui and others, 'He Looked Like a Terrorist! How a Drive in Rural India ended in a Mob Attack and a Lynching' (*Reuters*, 29 July 2018) <www.reuters.com/article/us-india-killings/he-looked-like-a-terrorist-how-a-drive-in-rural-india-ended-in-a-mob-attack-and-a-lynching-idUSKBN1KJ09R> accessed 28 April 2021; Donna Lu, 'WhatsApp Restrictions Slow the Spread of Fake News, But Don't Stop It' (*NewScientist*, 27 September 2019) <www.newscientist.com/article/2217937-whatsapp-restrictions-slow-the-spread-of-fake-news-but-dont-stop-it/> accessed 28 April 2021.

22 European Commission, Parliament, Council, Economic and Social Committee and Committee of the Regions, 'Tackling illegal Content Online. Towards an enhanced responsibility of online platforms' (Communication) COM (2017) 555 final.

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

24 Parliament and Council Directive 2011/93/EU of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA [2011] OJ L 335/1, art 25.

25 Parliament and Council Directive 2017/541/EU of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA [2017] OJ L 88/6, art 21.

26 Parliament and Council Directive 2018/1808/EU of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities [2018] OJ L 303/69.

27 Parliament and Council Directive 2019/790/EU 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 L 130/92.

28 Parliament and Council Regulation (EU) 2019/1150 of June 20 2019 on promoting fairness and transparency for business users of online intermediation services [2019] OJ L 186/57.

29 European Commission, 'Accompanying the Document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Mid-Term Review on the implementation of the Digital Single Market Strategy A Connected Digital Single Market for All' (Staff Working Document) SWD (2017) 155 final.

30 European Commission, 'A Union that strives for more: the first 100 days' (Press release IP/20/403, 6 March 2020) <https://ec.europa.eu/commission/presscorner/detail/en/ip_20_403> accessed 12 May 2021.

ernise the liability rules for online platforms, the European Parliament considered that exemptions should continue to apply to digital platforms that have no actual knowledge of illegal activities or information on their platforms.[31] The European Parliament maintained that the key principles of the liability regime are still justified, but at the same time called for more fairness, transparency and accountability in relation to the moderation of digital content, ensuring respect for fundamental rights and guaranteeing independent redress. To this end, the Parliament proposed a detailed notice and takedown procedure to combat illegal content, as well as comprehensive rules for online advertising and enabling the development and use of smart contracts.[32] The European Council stressed that harmonised rules on responsibilities and accountability for digital services should guarantee an adequate level of legal certainty for internet intermediaries.[33]

II. Policy objectives

13 With the DSA, the Commission aims to improve the protection of consumers and their fundamental rights in the online area as well as to create a uniform legal framework regarding the liability of online platforms for illegal content including requirements for more algorithmic transparency and transparent online advertising.[34] Relying on Article 114 TFEU as a legal basis for the DSA, the Commission wants to prevent a fragmented legal landscape, because "(...) several Member States have legislated or intend to legislate on issues such as the removal of illegal content online, diligence, notice and action procedures and transparency".[35] The objective of ensuring uniform protection of rights and uniform obligations for businesses and consumers throughout the internal market poses the main reason for implementing the DSA as a regulation,[36] which minimises the possibilities of Member States amending the provisions.

14 At the same time, the Commission remains limited by the objective of harmonising rules for the benefit of the internal market, as liability rules are predominantly national.[37] This partially explains why the Commission has retained the liability exception, which operates above national liability rules, rather than specifying new obligations in the form of a standard of care for online platforms.[38] The DSA only contains EU rules on the liability exemption for intermediary service providers—the conditions under which intermediary service providers incur liability con-

31 European Parliament, 'Report on the Digital Services Act and fundamental rights issues posed 2020/2022(INI)' (A9-,172/2020, 1 October 2020) <https://www.europarl.europa.eu/doceo/document/A-9-2020-0172_EN.html> accessed 19 May 2021, para 24; European Parliament, 'European Parliament, Resolution of 20 October 2020 with recommendations to the Commission on the Digital Services Act: Improving the functioning of the Single Market (2020/2018(INL))' (P9_TA(2020)0272, 20 October 2020) <https://www.europarl.europa.eu/doceo/document/TA-9-2020-0272_EN.html> accessed 19 May 2021, para 57.

32 See further DSA, recital 2 preamble; European Parliament, Resolution (2020/2018(INL); European Parliament, 'Resolution of 20 October 2020 with recommendations to the Commission on a Digital Services Act: adapting commercial and civil law rules for commercial entities operating online (2020/2019(INL))' (P9_TA(2020)0273, 20 October 2020) <https://www.europarl.europa.eu/doceo/document/TA-9-2020-0273_EN.html> accessed 20 May 2021; European Parliament, 'Resolution of 20 October 2020 on the Digital Services Act and fundamental rights issues posed (2020/2022(INI))' (P9_TA(2020)0274, 20 October 2020) <https://www.europarl.europa.eu/doceo/document/TA-9-2020-0274_EN.html> accessed 19 May 2021.

33 European Council, 'Conclusions on shaping Europe's digital future 8711/20' (9 June 2020) <www.consilium.europa.eu/media/44389/st08711-en20.pdf> accessed 19 May 2021; European Council, 'Special Meeting of the European Council (1 and 2 October 2021)' (2 October 2020) <www.consilium.europa.eu/media/45910/021020-euco-final-conclusions.pdf> accessed 19 May 2021.

34 DSA, 3 and 6.

35 DSA, 5-6, see also recital 2 preamble.

36 DSA, 8.

37 The impact assessment points out that Art. 114 TFEU would probably not be appropriate as the internal market legal basis for harmonising the rules on tort law. European 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 2 (Impact Assessment Part 2) 163.

38 DSA, recital 17 preamble: The draft clarifies that the new rules should only specify "when the provider of intermediary services concerned cannot be held liable in relation to illegal content provided by the recipients of the service. Those rules should not be understood to provide a positive basis for establishing when a provider can be held liable, which is for the applicable rules of Union or national law to determine.".

tinue to be determined by Member States' rules.[39]

15 The impact assessment considered three alternatives for modernising the liability rules for hosting providers. The first option was to codify the 2018 Recommendation on illegal content, establishing a set of procedural obligations for online platforms to address illegal activities by their users. The obligations would also include safeguards to protect fundamental rights and improve cooperation mechanisms for authorities.[40] The second option was full harmonisation, promoting transparency of recommendation systems and including a "Good Samaritan" clause to encourage service providers to take voluntary measures to combat illegal activities (see further Section C.IV below).[41] The third option would clarify the liability regime for intermediary service providers, provide for an EU governance system for supervision and enforcement, and impose stricter obligations on VLOPs.[42] The Commission opted for a combination of these options that maintains the core liability rules of the e-commerce Directive and introduces additional obligations for large platforms.

III. Scope

16 Overall, the DSA package results in the following set of rules: an ex-ante regulation in the DMA; ex-post liability rules from the e-commerce Directive implemented in Chapter II DSA; new obligations in Chapters III-IV DSA; and sector-specific regulations mentioned in DSA Article 1(5).

17 Chapter I of the DSA lays down general provisions regarding subject matter and scope. The DSA is set to have extraterritorial effect, meaning the regulation will apply whenever a recipient of intermediary services is located in the EU, regardless of the place of establishment or residence of the service provider.[43] Additionally, a "substantial connection" of the service provider with the EU is required, which is to be considered when the intermediary service has a significant number of users within the EU or where the provider targets its activities towards one or more Member States.[44]

18 In terms of its material scope, the DSA contains new obligations for digital service providers with respect to illegal content. The definition of illegal content is comprehensive, including "information relating to illegal content, products, services and activities".[45] It could therefore be information that in itself is illegal, such as illegal hate speech or terrorist content and unlawful discriminatory content, or information that relates to illegal activities, such as the sharing of images showing the sexual abuse of children, the unlawful sharing of private images without consent, cyber-stalking, the sale of non-compliant or counterfeit products, the unauthorised use of copyrighted material or activities that violate consumer protection law.[46] Otherwise, illegal content continues to be defined according to the member states' national laws.[47] The DSA does not distinguish between different types of infringement with respect to any of the obligations. This means that criminal offences, intellectual property rights violations and infringements of personal rights all face uniform compliance rules.[48]

19 Harmful but not necessarily illegal content, such as disinformation, is not defined in the DSA and is not subject to mandatory removal, as this is a sensitive area with serious implications for the protection of

39 See also Caroline Cauffman and Catalina Goanta, 'A New Order: The Digital Services Act and Consumer Protection' [2021] European Journal of Risk Regulation 1, 9. Rössel points out that the DSA hardly concretizes the liability rules, despite the Commission having identified the need for harmonization over the past years, because of the legal fragmentation of national bases for removal and cease-and-desist orders. See Markus Rössel, 'Digital Services Act' (2021) 52 Archiv für Presserecht (AfP) 93, 98 referring to European Commission, 'Public Consultation on Procedures for Notifying and Acting on Illegal Content hosted by Online Intermediaries – Summary of Responses' 3 Question 6 <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=42071> accessed 30 August 2021.

40 DSA, 12.

41 European 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) 43, para 159.

42 DSA, 12.

43 DSA, recital 7 preamble.

44 DSA, recitals 7-8 preamble.

45 DSA, recital 12 preamble.

46 DSA, recital 12 preamble.

47 See further DSA, art 2(g).

48 In this regard, Härting and Adamek question if each type of law violation warrants the obligations set out in the DSA. See Niko Härting and Max Valentin Adamek, 'Digital Services Act – Ein Überblick. Neue Kompetenzen der EU-Kommission und hoher Umsetzungsaufwand für Unternehmen' (2021) 37 Computer und Recht (CR) 165, 170.

freedom of expression.[49] To tackle disinformation and harmful content, the Commission wants to focus on how this content is disseminated and shown to people rather than pushing for its removal.[50]

20 The proposed DSA imposes transparency and due diligence obligations on providers of "intermediary services"[51]—the latter includes the services of "mere conduit"[52], "caching"[53], and "hosting"[54].[55] The material scope of the DSA coincides with that of the "information society services" in the InfoSoc Directive,[56] which encompasses services normally provided (i) for remuneration, (ii) at a distance, (iii) electronically and (iv) at the individual request of a user.[57]

This material scope and definition also applies to the e-commerce Directive.[58]

21 The DSA, however, extends the scope of the e-commerce Directive in several ways. One of the more notable alterations lies with the differentiation within the category of intermediary services. In addition to the provisions applying to all providers of intermediary services, the DSA proposes increased obligations for hosting providers and online platforms.[59] The DSA implements a pyramidal structure (see Figure 1 below), with general "due diligence obligations" applying to a broad group of providers of intermediary services and additional obligations only affecting certain providers of an increasingly limited category of intermediary services. The proposed obligations apply cumulatively, meaning online platforms will also need to comply with due diligence obligations that apply to intermediary services in general as well as with obligations hosting providers are subject to. Therefore, a VLOP will not only have to comply with the obligations that relate specifically to its category but also with those for "ordinary" online platforms.[60] The classification of the different

49 DSA, 10.

50 Vice President of the European Commission Věra Jourová in September 2020, see Samuel Stolton, 'Content removal unlikely to the part of the EU regulation on digital services, Jourova says' (*Euractiv*, 23 September 2020) <www.euractiv.com/section/digital/news/content-removal-unlikely-to-be-part-of-eu-regulation-on-digital-services-jourova-says/> accessed 5 May 2021.

51 DSA, art 1(1).

52 DSA, art 3: Mere conduit consists of the transmission in a communication network of information provided by a recipient of the service. *The information is only stored* automatically, intermediately and transiently *for the sole purpose of carrying out the transmission*. As Polčák points out mere conduit providers essentially are defined as provider of communication links. See Radim Polčák, 'The Legal Classification of ISPs. The Czech Perspective' (2010) 1 Journal of Intellectual Property, Information Technology and Electronic Commerce Law (JIPITEC) 172, 174. A typical example would be traditional internet access providers.

53 DSA, art 4: Caching also consists of the transmission in a communication network of information provided by a recipient of the service. However, *the information is stored* automatically, intermediately and temporarily *with the sole purpose of increasing efficiency*. An example would be a "proxy server".

54 DSA, art 5: Hosting services include *the unlimited storage of information* provided by a recipient of the service. An example hereof are providers of webhosting.

55 DSA, art 2(f); See further Gregor Schmid and Max Grewe, 'Digital Services Act: Neues "Grundgesetz für Onlinedienste"? Auswirkungen des Kommissionsentwurfs für die Digitalwirtschaft' (2021) 24 MultiMedia und Recht (MMR) 279; Leistner (n 1). On the implications of the DSA for non-hosting intermediaries, see Sebastian Felix Schwemer, Tobias Mahler and Håkon Styri, 'Liability exemptions of non-hosting intermediaries: Sideshow in the Digital Services Act?' (2021) 8 Oslo Law Review 4.

56 DSA, recital 5 preamble and art 2(a) referring to Parliament and Council Directive (EU) of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification) [2015] OJ L 241/1.

57 Parliament and Council Directive 2015/1535/EU of 9 September laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society service (codification) [2015] OJ L 241/1, art 1-1(b).

58 Parliament and Council Directive 2000/31/EC 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 L 178/1 (e-commerce Directive), art 1 and 2(a).

59 Dessislava Savova, Andrei Mikes and Kelly Cannon, 'The Proposal for an EU Digital Services Act: A closer look from a European and three national perspectives: France, UK and Germany' (2021) 2 Computer Law Review International (Cri) 38, 40; Jorge Morais Carvalho, Francisco Arga e Lima and Martim Farinha, 'Introduction to the Digital Services Act, Content Moderation and Consumer Protection' (2021) 3 Revista de Direito e Tecnologia (RDTec) 71, 76.

60 See also Folkert Wilman, 'Het voorstel voor de Digital Services Act: Op zoek naar nieuw evenwicht in regulering van onlinediensten met betrekking tot informatie van gebruikers' [2021] Nederlands tijdschrift voor Europees recht (NtEr) 28.

intermediary services under the DSA could however still lead to uncertainties. For example, cloud infrastructures seem to fall under the category of online platform (or possibly VLOP), although they are technically not able to monitor or moderate the content they store on behalf of customers.[61]

22 Specifically, the draft proposes a classification that distinguishes in: (a) very large online platforms (VLOPs)[62]; (b) online platforms[63]; (c) hosting providers[64]; and (d) intermediary services.[65] Qualification

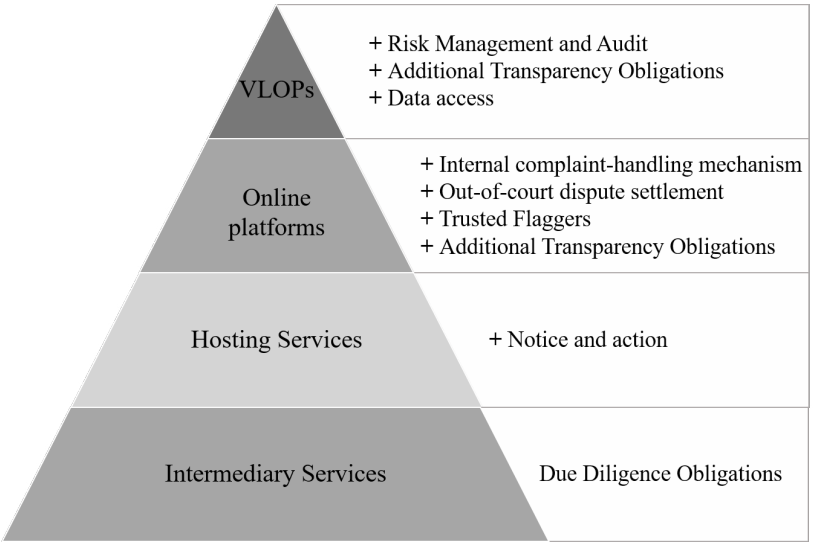

Figure 1: Cumulative obligations for intermediary services (simplified).

is made bases on relevant activities, not on the basis of the relevant service provider as a whole. This means that a service provider may qualify as an online platform with respect to certain activities and as a "mere conduit" for others.[66]

23 The principal innovative feature of the DSA is that it foresees separate, additional obligations for the subcategory of online platforms. The main difference between hosting services and online platforms lies in the dissemination of stored information to the public. While hosting services only store information, *online platforms also make information available to the public*.[67] General due diligence obligations for all intermediary services include establishing a single point of contact[68], incorporating certain information in the provider's terms and conditions[69] as well as complying with transparency reporting duties[70] (see Section D.I below). In addition to these obligations, hosting services are required to implement an easily accessible, user-friendly notice and action procedure to allow third parties to notify the provider of illegal content on the service (see Section D.II below).[71]

24 With respect to the subcategory of online platforms, the draft aims at tightening complaint management and reporting obligations to supervisory authorities. Also, the establishment of out-of-court dispute resolution mechanisms, including the introduction of trusted flaggers and precautions against the abuse of complaints, is proposed (see Section D.III).[72] However, there is a carve-out exception for micro

61 Computer & Communications Industry Association, 'Feedback Digital Services Act' <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12417-Digital-Services-Act-deepening-the-internal-market-and-clarifying-responsibilities-for-digital-services/F1965307> accessed 12 May 2021.

62 DSA, art 25: To qualify as a VLOP the online platform needs to provide services to more than 10% of the 450 million consumers within the EU. The methodology of calculation will be set out in delegated acts.

63 DSA, art 2(h) and (i): Online platforms are provider of hosting services that not only store information provided by the recipients, *but also disseminate that information to the public* upon request of the recipient, meaning that they make information available to a potentially unlimited number of people; see also DSA, recitals 13-14 preamble.

64 For an explanation, see DSA, art 5 and fn 55 of this article.

65 DSA, art 2(f): As previously explained, intermediary services mean either the service of "mere conduit", "caching" or "hosting"; for an explanation see fn 52 ff of this article.

66 DSA, recital 15 preamble; see also Wilman (n 60) fn 11.

67 DSA, art 2(h) and (i).

68 DSA, art 10.

69 DSA, art 12.

70 DSA, art 13.

71 DSA, art 14 and art 15: Hosting services will also have to issue a statement of reasons.

72 DSA, art 17 ff; Härting and Adamek (n 48) 165 ff; Gerald Spindler, 'Der Vorschlag für ein neues Haftungsregime für Internetprovider – der EU-Digital Services Act, Teil 2: Große und besonders große Plattformen' [2021] Gewerblicher Rechtsschutz und Urheberrecht (GRUR) 653.

and small enterprises who will not be required to comply with these additional obligations.[73]

25 For the limited subcategory of VLOPs, the proposal further foresees obligations with regard to risk management, data access, compliance, and transparency, as well as the implementation of an independent audit (see Section D.IV. below).[74]

26 In a broader perspective, the proposal raises the question on the DSA's relationship with other frameworks that contain *lex specialis* rules.[75] In context with the e-commerce Directive, rather than repealing the Directive the DSA only amends certain provisions.[76] Generally, the DSA is intended to complement the e-commerce Directive and other more recent sector- or subject-specific instruments already put in place.[77] It ,therefore, aims to coexist with current legislation rather than replace it.

C. Liability regime

I. Liability exemption

27 Chapter II of the DSA largely adopts the liability rules of the e-commerce Directive, making it clear that the Commission wished to leave the principles underlying the liability regime for hosting providers unchanged. This means that online platforms continue to be fundamentally not responsible for third-party content.

28 The e-commerce Directive created a harmonised exception to the national liability regime applicable to online platforms for unlawful material uploaded by users. According to Article 14 e-commerce Directive, service providers are exempted from liability for third-party illegal content, provided that they are unaware of or fail to remove the illegal content after becoming aware of it. In practice, this has resulted in notice and takedown procedures enabling users to notify service providers of illegal content. As will be discussed further below, the DSA lays down new requirements for the notice and takedown procedure for hosting providers, extending it to a notice and action procedure (section D.I.).

29 Article 5 DSA adopts Article 14 e-commerce Directive. For mere conduits and caching services, Articles 3 and 4 DSA respectively exclude liability, while Article 5 exempts hosting services from liability as long as they remove illegal content expeditiously upon obtaining knowledge of it. The DSA only contains EU rules on the liability exemption for intermediary service providers—the conditions under which intermediary service providers incur liability continue to be determined by Member States' rules.

30 What is new is that the DSA, in Articles 8 and 9, introduces rules regarding the orders that national judicial or administrative authorities can address to intermediaries. These orders can oblige intermediaries to cooperate with member states' judicial or administrative authorities when acting against concrete instances of illegal content. Orders need to include a statement of reasons and information on possibilities of appeal. Articles 8 and 9 do not grant new powers but instead establish a harmonized framework for existing powers to be exercised in an efficient and effective manner.[78]

31 A reason provided in the DSA for maintaining the liability regime of the e-commerce Directive is that the European Court of Justice ("ECJ") provided clarification and guidance for the existing rules.[79] The proposal notes that the legal certainty created has helped many new types of services emerge and expand throughout the internal market.[80] According to the impact assessment, departing from the liability exemption by imposing more legal risks on intermediaries could have a severe impact on citizens' freedom of expression on the internet. It is argued changing the liability regime would be prohibitively expensive for new businesses while lowering the standard for hosting providers to qualify for liability exemptions would affect security and trust in the online environment.[81] Further, alternative liability regimes were simply considered inappropriate. Creating a positive basis at EU level for determining in which cases a service provider should be held liable was rejected as this would not comply with the

73 DSA, art 16.

74 DSA, art 26 ff.

75 In detail concerning the CDSM Directive: João Pedro Quintais and Sebastian Felix Schwemer, 'The Interplay between the Digital Services Act and Sector Regulation: How Special is Copyright?' (2021) Working Paper <https://privpapers.ssrn.com/sol3/papers.cfm?abstract_id=3841606> accessed 31 May 2021.

76 DSA, art 71; see namely e-commerce Directive, art 12-15.

77 Carvalho, Arga e Lima and Farinha (n 59) 73; Wilman (n 60) 27.

78 DSA, recital 29 preamble; see also Wilman (n 60) 30; Leistner (n 1) 9.

79 DSA, 3.

80 DSA, recital 16 preamble.

81 Impact Assessment Part 2, 48 para 170.

principle of subsidiarity.[82] The possibility of including online marketplaces in the liability regime and requiring them to obtain accurate and up-to-date information on the identity of third-party service providers offering products or activities through the platforms was considered a separate issue from the review of the horizontal liability regime set out in the e-commerce Directive.[83] The impact assessment also rejected the option of making the liability exemption conditional on compliance with due diligence obligations. Instead, it advocated for requiring compliance with these obligations separately from the liability exemption. According to the impact assessment, this would impose a disproportionate burden on public authorities and create further legal uncertainty for service providers.[84] With a view to individuals' rights, the possibility of linking due diligence obligations to the liability exemption may have been discarded too quickly (see Section E.II. below).

32 In addition to the liability exemption, two further pillars make up the e-commerce Directive liability regime.[85] First, the country-of-origin principle states that an online platform is only subject to the liability regime of the EU Member State in which it is established.[86] The DSA holds on to this principle, although it reduces its practical meaning by harmonising a number of significant issues at Union level.[87] Second, the e-commerce Directive prohibits EU Member States from imposing a general obligation on hosting platforms to monitor material.[88] The ECJ has drawn a blurred line between general monitoring measures, which are prohibited,[89] and permitted specific monitoring measures, in particular in the case of suspected infringement of intellectual property rights.[90] Article 7 DSA takes over the prohibition on member states stated in Article 15 e-commerce Directive imposing a general duty of supervision on intermediary services.[91] With regard to the difficulty mentioned above in distinguishing between general and specific monitoring obligations, the draft DSA now clarifies that authorities and courts may issue orders to stop infringements by specific illegal content.[92]

33 The impact assessment prepared for the DSA identified three main shortcomings of the existing liability regime:[93] i) the e-commerce Directive could discourage voluntary actions taken to fight illegal content online; ii) the concept of playing an "active" role is uncertain,[94] and iii) the e-commerce Directive does not clarify when a platform is deemed to have acquired "actual knowledge" of an infringement which triggers the obligation to remove the content.[95]

II. "Active"

34 The ECJ distinguishes between, on the one hand, services that assume a purely technical, automatic and passive role, which can benefit from the exemption from liability, and on the other hand, services that assume a more active role, such as optimising the ranking of offers for an e-commerce platform, which cannot benefit from the exemption.[96]

82 Impact Assessment Part 2, 163.

83 Impact Assessment Part 2, 163 ff.

84 Impact Assessment Part 2, 165-66.

85 See further Buiten, De Streel and Peitz (n 8) 144-45.

86 E-commerce Directive, art 3; see also Daniel Holznagel, 'Platform Liability for Hate Speech & the Country of Origin Principle: Too Much Internal Market?' [2021] Computer Law Review international (CRi) 103.

87 Wilman (n 60) at 28.

88 E-commerce Directive, art 15.

89 Case C-360/10 *SABAM v Netlog* EU:C:2012:85

90 Case C-314/12 *UPC Telekabel Wien v Constantin Film Verleih and others* EU:C:2014:192.

91 DSA, art 7 and recital 28 preamble; on the ambiguous wording of art 7 DSA, see Daniel Holznagel, 'Chapter II des Vorschlags der EU-Kommission für einen Digital Services Act. Versteckte Weichenstellungen und ausstehende Reparaturen bei den Regelungen zu Privilegierungen, Haftung & Herkunftslandprinzip für Provider und Online-Plattformen' (2021) 2 CR 123, 128.

92 DSA, art 3(3), 4(2), 5(4) and recitals 29 ff preamble; Matthias Berberich and Fabian Seip, 'Der Entwurf des Digital Services Act' (2021) 1 Gewerblicher Rechtsschutz und Urheberrecht, Praxis im Immaterialgüter- und Wettbewerbsrecht (GRUR-Prax) 4.

93 Impact Assessment Part 2, 157 ff.

94 Impact Assessment Part 2, 159 f.

95 Impact Assessment Part 2, 161.

96 Case C-360/10 *SABAM v Netlog* EU:C:2012:85; EuGH, Case C-70/10 *Scarlet Extended v SABAM* ECLI:EU:C:2011:771, [2011] ECR I-11959; Case C-314/12 *UPC Telekabel Wien v Constantin Film Verleih and others* EU:C:2014:192; joined Cases C-236/08 to C-238/08 *Google France v Louis Vuitton* ECLI:EU:C:2010:159, [2010] ECR I-02417, para 113; Case C-324/09 *L'Oréal and others v eBay* ECLI:EU:C:2011:474, [2011] ECR I-06011, para 116; EuGH, Case C-484/14 *Tobias Mc Fadden v Sony Music Entertainment Germany* EU:C:2016:689, para 62; see further Patrick Van Eecke, 'Online Service Providers and Liability: A Plea for a Balanced Approach' (2011) 48 Common Market Law

35 The Impact Assessment notes that, "(...) there is still an important uncertainty as to when it is considered that an intermediary, and in particular, a hosting service provider, has played an active role of such a kind as to lead to knowledge or control over the data that it hosts."[97] The Impact Assessment states: "Many automatic activities, such as tagging, indexing, providing search functionalities, or selecting content are today's necessary features to provide user-friendly services with the desired look-and-feel, and are absolutely necessary to navigate among an endless amount of content, and should not be considered as 'smoking gun' for such an 'active role'."[98]

36 In order to benefit from the liability exemptions, the distinction between a passive, neutral role and an active role remains relevant for service providers.[99] Thus, as before, the liability exemptions require that the role of the intermediary of a service is purely technical, automatic and passive, having neither knowledge of nor control over the information stored.[100] The DSA does not significantly develop this concept[101] but clarifies some aspects. First, the DSA includes a "Good Samaritan" clause[102] (see Section C.IV below). Secondly, the DSA excludes intermediary service providers from the liability exemptions if they knowingly cooperate with a user to engage in illegal activities. In that case, the platform does not provide the service in a neutral manner.[103] Thirdly, an online marketplace operator is excluded from the liability exemption if third party offers misleadingly look like the platform operator's own offers.[104] In such a case, however, it is less relevant who controlled the offer or stored information, but much more whether service providers created the impression that the offer or information originated from them. This criterion is objectified, because the impression of an average, reasonably well-informed consumer is decisive.[105] This e-commerce liability aims to distinguish the responsibility of different types of e-commerce platforms: those who have a limited role in the transactions between users and those who play a central role in promoting of the product, the conclusion of the contract and its execution.[106]

37 Given the extensive moderation that online platforms undertake as part of their business model, maintaining the passive/active distinction as a criterion for the liability of service providers seems questionable. Filtering, sorting and optimising content for profit is still seen as an activity of a purely technical, passive nature and does not lead to knowledge of illegal content on the platform. Whether this reflects the AI-moderated world of today's online platforms may rightfully be doubted.

38 In their early days, service providers were often seen as mere intermediaries bringing together different user or customer groups by reducing transaction costs.[107] Today, online platforms active on two-sided

Review (CMLR) 1455; Martin Husovec, *Injunctions Against Intermediaries in the European Union: Accountable But Not Liable?* (Cambridge University Press 2017); Jan Nordemann, 'Liability of Online Service Providers for Copyrighted Content – Regulatory Action Needed?' (In-Depth Analysis for the IMCO Committee, January 2018) <https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/614207/IPOL_IDA(2017)614207_EN.pdf> accessed 20 May 2021; Joris Van Hoboken and others, 'Hosting Intermediary Services and Illegal Content Online' (Study for the European Commission, 2018) <https://op.europa.eu/en/publication-detail/-/publication/7779caca-2537-11e9-8d04-01aa75ed71a1/language-en> accessed 20 May 2021.

97 Impact Assessment Part 2, 159.

98 Impact Assessment Part 2, 159.

99 DSA, recitals 18 ff preamble. However, as Cauffman and Goanta (n 39), referring to the cases C-238/08 *Google France v Louis Vuitton* EU:C:2010:159, [2010] ECR I-02417 and C-324/09 *L'Oréal and others v eBay* EU:C:2011:474, [2011] ECR I-06011, point out: "It is not entirely clear [...] whether the neutrality requirement is intended to remain applicable in exactly the same way under the DSA as it was understood in the case law of the Court of Justice."

100 Joined Cases C-236/08 to C-238/08 *Google France v Louis Vuitton* EU:C:2010:159, [2010] ECR I-02417.

101 Berberich and Seip (n 92) 4.

102 DSA, art 6 and recital 25 preamble.

103 DSA, recital 20 preamble.

104 DSA, recital 23 preamble and art 5(3). On the protection of individual consumers in the DSA, see further Christoph Busch and Vanessa Mak, 'Putting the Digital Services Act in Context: Bridging the Gap Between EU Consumer Law and Platform Regulation' (2021) 10 Journal of European Consumer and Market Law (EuCML) 109.

105 DSA, recital 23 preamble; see also Wilman (n 60) 29.

106 See further Bram Duivenvoorde, 'De aansprakelijkheid van ecommerceplatforms' (*Blog van het Utrecht Centre for Accountability and Liability Law*, 20 April 2021) <http://blog.ucall.nl/index.php/2021/04/de-aansprakelijkheid-van-e-commerceplatforms/> accessed 31 May 2021.

107 For fundamentals see Jean-Charles Rochet and Jean Tirole, 'Platform Competition In Two-Sided Markets' (2003) 1 Journal of the European Economic Association (JEEA) 990; Jean-Charles Rochet and Jean Tirol 'Two-Sided Markets: A Progress Report' (2006) 35 The RAND Journal of Economics (RJE) 645; see eg Richard Schmalensee, 'An Instant Classic:

markets attract users by offering them free services or content, generating revenues by charging users on the other side of the market and through advertising. To maximise their revenues, ad-supported platforms design services to hold users' attention to show them more advertising and encourage users to disclose more personal data in order to serve up more lucrative personalised ads.[108] In this attention economy, the design of digital services is usually optimised in favour of these advertising-driven business models.

39 While some service providers may still take up a passive, neutral role, online platforms have evolved into active co-creators of the digital sphere.[109] A central component of the advertising-driven business model lies in the moderation of content to encourage users to spend more time on the platform and share more personal data. Today's search engines, social media networks and e-commerce platforms determine not only which users can participate in the ecosystem or the way transactions are to be carried out via the platform but also what information corresponding users will receive.

40 With this in mind, it is difficult to maintain that online platforms offer a service of a purely neutral, technical nature. It is also difficult to discern what type of moderating is allowed, and at what point it turns into an "active" role for the purpose of liability. An alternative solution would be to let go of the passive/active distinction and instead link the liability exemption to complying with the due diligence obligations in the DSA. This would effectively set a Union-wide standard of care for hosting providers and online platforms (see further Section E.II. below).

III. "Knowledge"

41 The e-commerce Directive does not clarify at which point a platform is deemed to have acquired "actual knowledge" of an infringement that triggers the obligation to remove the content. It is unclear what information is required for a notification to trigger such knowledge.[110]

42 The draft DSA clarifies that providers can obtain this knowledge through sufficiently precise and sufficiently substantiated notifications. It remains to be seen to what extent platforms will be able to hide behind an imprecise or incomplete notification in order to circumvent takedown obligations. [111]

IV. Good Samaritan clause

43 According to the impact assessment, the ECJ's interpretation of the e-commerce Directive left a paradox of incentives for service providers: proactive measures taken to detect illegal activities (through automatic means) could be used as an argument that the service provider is an "active" service controlling the content uploaded by its users and therefore cannot be considered as falling within the scope of the conditional exemption from liability.[112] As a result, the e-commerce Directive could discourage voluntary "Good Samaritan" measures to remove or detect unlawful content.[113] The 2018 Recommendation on Illegal Content Online already included a "Good Samaritan" clause but was merely a non-binding instrument.[114]

44 The proposal to include a "Good Samaritan" clause in hard law had been proposed by several academics and will be met with approval.[115] It is consistent with the policy goal of getting service providers to better monitor their platforms without violating the prohibition on general monitoring obligations in the DSA.[116]

Rochet & Tirole, Platform Competition in Two-Sided Markets' (2014) 10 Competition Policy International (CPI Journal) 174.

108 See further David Evans, 'Attention Platforms, the Value of Content, and Public Policy' (2019) 54 Review of Industrial Organisation 775.

109 See also Teresa Rodríguez de las Heras Ballell, 'The background of the Digital Services Act: looking towards a platform economy' (2021) 22 Europäische Rechtsakademie (ERA) Forum 75, 83.

110 Impact Assessment Part 2, 161.

111 See Joan Barata, 'The Digital Services Act and the Reproduction of Old Confusions' (*Verfassungsblog*, 2 March 2021) <https://verfassungsblog.de/dsa-confusions/> accessed 32 May 2021; European Commission, 'Shaping Europe's digital future' <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package> accessed 31 May 2021.

112 Impact Assessment Part 2, 158-59.

113 Impact Assessment Part 2, 158-59.

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

115 See e.g. Buiten, Peitz and De Streel (n 8), Leistner (n 1).

116 See Aleksandra Kuczerawy, 'The Good Samaritan that wasn't: voluntary monitoring under the (draft) Digital Services Act' (*Verfassungsblog,* 12 January 2021) <https://

45 Article 6 DSA includes a "Good Samaritan" clause, which clarifies that liability privileges do not cease merely because online intermediaries voluntarily take measures to remove or detect unlawful content, as long as these activities are undertaken in good faith and in a diligent manner.[117] The provision seeks to create incentives for service providers to take more initiative against illegal content without any immediate risk of being labelled "active" and losing immunity. The rule does not apply to activities of service providers involving user information that is not illegal, so service providers need to be sure that the content in question is illegal. The clause also applies when service providers take such measures to comply with requirements of other Union law instruments, for instance, under Article 17 of the DSM Copyright Directive or the Regulation on Combating Terrorist Content Online.[118]

46 The wording of Article 6, however, leaves much to be desired. The provision only states that voluntary measures taken by intermediaries on their own initiative should not be the *sole reason* for losing the liability exemption.[119] Article 6 does not protect intermediaries against the fact that voluntary actions could lead intermediaries to have "actual knowledge" of illegal content in the meaning of Article 5(1) DSA, which would require them to remove the content in order to avoid liability.[120] Kuczerawy names the example of a moderator trained to review for one type of illegality, who fails to recognize that a particular video is illegal on another ground. Not removing that content that was reviewed "could still result in liability because the host 'knew' or 'should have known' about the illegality".[121]

47 Neither does the provision guarantee that the intermediary is considered passive and neutral. Thus, it remains open to interpretation if, for instance, unsuccessful voluntary actions might not be considered "diligent", resulting in intermediaries losing their exemption from liability.[122] The provision, moreover, leaves open the possibility of liability exemptions being revoked due to service providers having an active role with respect to other aspects, such as in presenting the information or the offer.[123]

48 Overall, the provision protects an intermediary only from being considered "active"solely on the basis of actions taken to remove illegal content voluntarily. The "Good Samaritan" clause illustrates the difficulties of trying to hold on to the legal distinction between passive and active service providers in the moderated online world.

D. Obligations

I. Due diligence obligations

49 Chapter III of the DSA lays down due diligence obligations. Section 1 covers obligations applicable to all intermediary service providers.

50 Looking only at the exemption from liability, the DSA does not significantly change the status quo.[124] The DSA does not raise the standard for hosting provider liability in civil proceedings before national courts. However, the proposal provides for a number of information and due diligence obligations for platforms in Chapters III and IV, which impose new administrative duties on online platforms.

51 According to Article 10, hosting providers will have to set up a one-stop shop for authorities.[125] The focal point will be required to cooperate and communicate with supervisory authorities, the EU Commission and the European Committee on Digital Services (created under the DSA) in relation to their obligations under the DSA. Online intermediaries based outside the EU (e.g., in the UK) but operating in the EU will have to appoint an EU legal representative for this purpose.[126]

52 In addition, Article 12 provides for an obligation for service providers to include in their general terms and conditions information on "any policies, procedures, measures and tools used for the purpose of content moderation, including algorithmic deci-

verfassungsblog.de/good-samaritan-dsa/> accessed 12 May 2021.

117 DSA, art 6 and recital 25 preamble.

118 See also Wilman (n 60) 30.

119 Kuczerawy (n 116).

120 Holznagel (n 86) 128.

121 Kuczerawy (n 116).

122 Kuczerawy (n 116).

123 Vanessa Mak and Femke Schemkes, '"With great power comes great responsibility": De Digital Services Act en de Digital Markets Act mogen wel wat strenger zijn voor Big Tech' [2021] Nederlands Juristenblad (NJB) 749.

124 See also Andrej Savin, 'The EU Digital Services Act: Towards a More Responsible Internet' (2021) 24 Journal of Internet Law 1, 6.

125 DSA, art 10 and recital 36 preamble.

126 DSA, art 11 and recital 37 preamble.

sion-making and human review".[127] Finally, according to Article 13, providers are obliged to publish annual reports on the content moderation they carry out.[128] Separate transparency obligations apply to platforms under Article 23 (see 5). Furthermore, Articles 8 and 9 introduce procedural measures and oblige providers to inform the competent authorities of the measures they have taken to combat infringements (Article 8) and harmonise which elements this information must contain (Article 9).

II. Hosting providers: Notice and action mechanism

53 Chapter III, Section 2 of the DSA introduces additional obligations for hosting services, primarily with regard to their notice and takedown systems.

54 With reference to illegal content, the draft DSA clarifies the obligations of platforms to benefit from the liability exemption. The proposal no longer refers to a notice and takedown procedure, but to a notice and action mechanism. However, it does not envisage any dramatic changes, but rather harmonises some procedural aspects for these mechanisms[129] that were already laid down in the laws of many member states.[130]

55 According to Article 14 DSA, hosting service providers must implement a user-friendly and easily accessible notice and action procedure that allows users to report illegal content.[131] It requires a timely, thorough and objective handling of notices based on uniform, transparent and clear rules that provide for robust safeguards to protect the rights and legitimate interests of all data subjects, in particular their fundamental rights.[132]

56 While the proposal provides for specific rules in the case of repeated infringements, it does not go so far as to impose a "notice and stay down" obligation, which would require hosting providers to ensure that illegal content does not reappear.[133] The ECJ has already explicitly pointed out that a platform must effectively contribute to preventing repeated infringements.[134] The new obligations to temporarily block accounts of repeat offenders are therefore, a rather conservative codification of this case law. It remains to be seen how platforms will deal with tactics by repeat offenders to avoid measures, such as switching back and forth between different accounts.[135]

57 Article 14 specifies what information hosting service providers must request in order to be aware of the illegality of the content in question.[136] Article 14 requires that notifications must contain, in addition to the reason for the request, a clear indication of the location of the information, in particular the precise URL address, as well as the name and details of the requesting party and a statement of good faith. The requirement of precise information codifies ECJ case law which states that injunctions targeting specific content are admissible, while general injunctions are not.[137] Article 14 also clarifies that notices containing the elements mentioned above are presumed to be actual knowledge of illegal content, in which case the provider loses the exemption from liability under Article 5.[138] In this way, the DSA aims to remove the uncertainty regarding "knowledge" discussed above.[139]

127 DSA, art 12.

128 DSA, art 13.

129 See further DSA, recital 41 preamble.

130 See Alexandre De Streel and others, 'Online Platforms' Moderation of Illegal Content Online: Law, Practices and Options for Reform' (Study requested by the IMCO Committee, 23 June 2020) <www.europarl.europa.eu/RegData/etudes/STUD/2020/652718/IPOL_STU(2020)652718_EN.pdf> accessed 12 May 2021; see further Savin (n 124) 8.

131 DSA, art 14(1).

132 DSA, recital 41 preamble.

133 On "notice and stay down" see eg Giancarlo Frosio, 'Reforming intermediary liability in the platform economy: A European digital single market strategy' (2017) 112 Northwestern University Law Review Online (NULR Online) 19; Martin Husovec, 'The Promises of Algorithmic Copyright Enforcement: Takedown or Staydown: Which Is Superior: And Why' (2019) 42 Columbia Journal of Law and the Arts (Colum JL & Arts) 53.

134 Case C-324/09 *L'Oréal and others v eBay* EU:C:2011:474, [2011] ECR I-06011.

135 See Markenverband, 'Feedback Digital Services Act' <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12417-Digital-Services-Act-deepening-the-internal-market-and-clarifying-responsibilities-for-digital-services/F1966164> accessed 12 May 2021.

136 DSA, art 14(2).

137 Case C-360/10 *SABAM v Netlog* EU:C:2012:85; Case C-70/10 *Scarlet Extended v SABAM* EU:C:2011:771, [2011] ECR I-11959; see further Savin (n 124) 8.

138 Holznagel (n 91) 126.

139 DSA, art 14(2).

58 Hosting service providers must notify users of the decision in a timely manner, inform them of possible remedies as well as of the use of any automated systems.[140] If the hosting service provider decides to remove or block access to the reported content, it must notify the user in accordance with Article 15 no later than the time of removal or blocking of access with a clear and specific justification. This is independent of the means used to trace, identify, remove or block access to this information.[141] The justification must contain certain information and be easily understandable given the circumstances.[142]

III. Online Platforms: Procedural and transparency obligations

59 Chapter III, Section 3 of the DSA contains further provisions for online platforms, excluding micro or small enterprises.[143] An "online platform" is a "hosting service which, at the request of a recipient of the service, stores and disseminates to the public information, unless that activity is a minor and purely ancillary feature of another service and, for objective and technical reasons cannot be used without that other service, and the integration of the feature into the other service is not a means to circumvent the applicability of this Regulation".[144] As previously mentioned, the distinguishing element of an online platform is, therefore, the dissemination of users' information to the public.

60 Article 17 obliges online platforms to set up an easily accessible and free electronic complaints management system. The complaints system must enable users to appeal against decisions made by the platform that user information is illegal or violates the general terms and conditions. This applies to decisions to remove content, to suspend services to users or to terminate a user's account altogether.[145] It is noted that platforms must not make such decisions solely by automated means.[146] This effectively creates a human oversight obligation that can prove costly for platforms. For decisions arising from the preceding mechanism, users must have the possibility to resort to out-of-court dispute resolution mechanisms (Article 18). This mechanism neither replaces other legal or contractual means of dispute resolution (courts or arbitration)[147] nor does the DSA create its own substantive user rights.[148]

61 Article 19 codifies the role of "trusted flaggers": specific entities (not individuals) that are given priority the handling complaints, thus streamlining the procedure and increasing accuracy. Member States can grant trusted flagger status to entities such as NGOs or rightholders' organisations, provided they have the necessary expertise, represent collective interests and are independent of any online platform and submit their reports in a timely, diligent and objective manner.[149] Priority in the processing of their notifications, however, seems to be the only advantage associated with the trusted flagger status.[150]

62 Article 20 regulates the conditions under which services are temporarily blocked for users who frequently provide "manifestly illegal content".[151] Users who frequently submit obviously unfounded reports or complaints should also be blocked after prior warning.[152] The criteria for abuse must be clearly stated in the general terms and conditions[153] and must take into account the absolute and relative number of obviously illegal content or obviously unfounded reports or complaints, as well as the severity of the abuses and their consequences, and the intentions pursued.[154] According to Article 21, the law enforcement authorities must be notified immediately if "(...) a serious criminal offence involving a threat to the life or safety of persons (...)" is suspected.[155]

140 DSA, art 14(4-6).

141 DSA, art 15(1).

142 See further DSA, art 15(2).

143 Micro or small enterprises as defined in the Annex to Commission Recommendation 2003/361/EC of May 2003 concerning the definition of micro, small and medium-sized enterprises [2003] OJ L 124/36, the criteria for which are number of employees, turnover and balance sheet.

144 DSA, art 2(h).

145 DSA, art 17(1)(a-c).

146 Savin (n 124) 9.

147 Savin (n 124) 9.

148 Berberich and Seip (n 92) 5.

149 DSA, art 19(2).

150 See further Savin (n 124) 9.

151 DSA, art 20(1).

152 DSA, art 20(2).

153 DSA, art 20(4).

154 DSA, art 20 (3)(a-d).

155 DSA, art 21.

63 In addition to the general transparency obligations listed above, Article 23 requires online platforms to publish information on out-of-court disputes, on blocking under Article 20 and on the use of automated means for the purpose of content moderation.[156] It remains to be seen how this relates to Article 17's prohibition on relying exclusively on automated content moderation.

64 Article 22 DSA also provides for a "know your customer" obligation, according to which online marketplaces, where traders offer products or services, must collect detailed information on the identity of traders.[157] Platforms must make reasonable efforts to ensure that the information provided is accurate and complete. The duty to identify traders means a new, potentially costly layer of administration for platforms.[158] However, it should be noted that micro or small businesses are exempt from these obligations. The "know your customer" obligation should help detect rogue traders and protect online shoppers from counterfeit or dangerous products.

65 Finally, advertising-financed online platforms must provide transparency to users about personalised advertising. Article 24 obliges online platforms to provide their users with real-time information about the fact that the information displayed is advertising, why they are seeing a particular advertisement and who has paid for it. The platforms must also ensure that sponsored content is clearly marked as such.[159] However, a ban on personalised advertising, as proposed in a parliamentary report, is not suggested.[160]

156 DSA, art 23.

157 DSA, art 22.

158 Savin (n 124) 10.

159 DSA, art 24.

160 European Parliament, 'Report with recommendations to the Commission on a Digital Services Act: adapting commercial and civil law rules for commercial entities operating online (2020/2019(INL))' (A9-0177/2020, 5 October 2021) <https://www.europarl.europa.eu/doceo/document/A-9-2020-0177_EN.html> accessed 19 May 2021; see further European Parliament, 'Resolution of 20 October 2020 with recommendations to the Commission on a Digital Services Act: adapting commercial and civil law rules for commercial entities operating online (2020/2019(INL))' (P9_TA(2020)0273, 20 October 2021) <https://www.europarl.europa.eu/doceo/document/TA-9-2020-0273_EN.html> accessed 19 May 2021.

IV. VLOPs: Additional risk management and transparency obligations

66 Finally, Chapter III, Section 4 DSA introduces the strictest compliance, accountability and risk management requirements to systemically important platforms. According to Article 25, these are platforms that provide their services to active users in the Union whose average monthly number is at least 45 million people or 10% of the Union population.[161] Systemically important platforms are thus defined quantitatively and not, as under the DMA, via their gatekeeping function and their impact on the internal market. The calculation method explicitly takes into account the number of active users. The platform is not subject to the special regime until the digital services coordinator has decided to that effect.[162]

67 For these VLOPs, the Commission considers further obligations necessary due to their reach in terms of the number of users and "(...) in facilitating public debate, economic transactions and the dissemination of information, opinions and ideas and in influencing how recipients obtain and communicate information online (...)".[163] The systemic relevance is that the way VLOPs are used "(...) strongly influences safety online, the shaping of public opinion and discourse, as well as on online trade".[164]

68 In addition to the obligations imposed on gatekeepers under the DMA proposal, the DSA primarily addresses risk mitigation in content moderation situations for the largest platforms. Under Article 26, VLOPs will be required to conduct an annual risk analysis addressing "(...) any significant systemic risks stemming from the functioning and use made of their services in the Union".[165] The risks to be assessed relate to the dissemination of illegal content through their services; to the adverse effects on the exercise of fundamental rights, such as freedom of expression and information and the prohibition of discrimination; as well as to the intentional manipulation of the service with adverse effects on the protection of public health, minors, social debate, electoral processes and public safety. This includes manipulation through inauthentic use or automated exploitation of the service. These risk assessments

161 DSA, art 25.

162 DSA, art 25(4).

163 DSA, recital 53 preamble.

164 DSA, recital [56] preamble.

165 DSA, art 26.

should particularly focus on the impact of the platform's moderation and recommendation systems.[166]

69 These risks should be mitigated by appropriate, proportionate and effective risk mitigation measures (Article 27). As examples of such measures, the DSA mentions adapting content moderation and recommendation systems, limiting advertising, strengthening internal supervision, adapting cooperation with trusted flaggers and initiating cooperation with other platforms through codes of conduct and crisis protocols.[167] Section 5 of Chapter III introduces codes of conduct (Articles 35-36) and crisis protocols (Article 37) as forms of self-regulation promoted by the Commission.

70 Per Article 28, VLOPs are also subject to an independent audit at their own expense at least once a year, which assesses compliance with the due diligence obligations in Chapter II and as well as the commitments in accordance with codes of conduct.[168]

71 Further transparency obligations are imposed in relation to the use of recommendation systems (Article 29) and online advertising (Article 30). For recommendation systems, VLOPs must set out the main parameters used in their recommendation systems in an understandable way and elaborate any options they provide for users to influence the main parameters. Also, users must have at least one option to use without profiling.[169] The added transparency of online advertising forces ad-driven platforms to compile and provide information about the ads and the advertiser. It is to be expected that an obligation to disclose such sensitive information will be subject to intense discussions in the legislative process.[170]

72 Finally, VLOPs must ensure the digital services coordinator access to data (Article 31) and appoint a compliance officer (Article 32) who is responsible for monitoring compliance with the regulation and preparing reports (Article 33).

73 The asymmetric structure of obligations in the DSA offers advantages in that it reflects the central role that the largest platforms play in curbing illegal and problematic content. As such, the DSA represents a significant change in the regulatory oversight exercised over large hosting providers. Nevertheless, to prevent harmful activities from being shifted from VLOPs to smaller players, it could be considered to impose obligations to assess and mitigate systemic risks on all or more online platforms on a pro-rata basis and not only to VLOPs.

E. Enforcement and penalties

I. Competences

74 Chapter IV of the DSA introduces a number of detailed and far-reaching enforcement measures and mechanisms. Unlike the e-commerce Directive, the DSA specifically regulates the national authorities responsible for applying the regulation.[171] In this respect, the DSA follows the example of the General Data Protection Regulation ("GDPR").[172] The supervisory authority is determined by the location of the service's main establishment (Article 40).

75 In order to speed up enforcement by national authorities,[173] each Member State must appoint a digital services coordinator: an independent and transparent authority (Article 39) responsible for supervising intermediary services established in the respective Member State and for coordination with specialised authorities (Article 38). The basic idea seems to be to designate a primary contact in cases in which Member States have several competent authorities. Article 41 gives considerable powers to the digital service coordinators. They can request cooperation from anyone with relevant information about infringements, conduct on-site inspections of premises used by intermediaries, including the right to seize information related to a suspected infringement, as well as the power to question any employee. Although the measures are mainly aimed at intermediaries, the coordinators may also impose fines or periodic penalty payments on other entities or persons who fail to comply with the rules. Similar to the GDPR, the DSA provides for a European coordinator—the "European Board for Digital Services"—in Articles 47-49.

76 VLOPs are subject to a separate and detailed enforcement regime. If a digital services coordinator finds that such a platform is in breach of any of the obligations for VLOPs, it will be subject to enhanced supervision under Article 50 and required to draw up an action plan (and possibly a code of conduct). If

166 DSA, art 26(2).

167 DSA, art 27(1).

168 DSA, art 28.

169 DSA, art 29(1).

170 Berberich and Seip (n 92) 6.

171 DSA, recitals 78 ff preamble.

172 Savin (n 124) 12; see also Savova, Mikes and Cannon (n 59) 38.

173 See Berberich and Seip (n 92) 6.

the action plan is not satisfactory, further independent audits may be ordered, and Commission intervention is possible.

77 The Commission is to be given very wide powers in relation to VLOPs. Similar to the Commission's role in the field of EU competition law,[174] Article 51 ff. allows for investigations, interim measures, undertakings and a special sanctions regime that includes fines (Article 59) and periodic penalty payments (Article 60). In the event of persistent non-compliance, the Commission may request the national coordinators to act according to Article 41(3) and request the national judicial authorities to temporarily suspend services or access.

78 With respect to VLOPs, the DSA thus envisages a highly centralised regulatory model with the Commission as the sole regulator. This choice appears to be a response to the difficulties that arose in enforcing the GDPR; experience with the GDPR has shown that the Irish data protection authority was overwhelmed and, therefore, slow to respond to complaints. Integrating the national digital services coordinator into the European Board for Digital Services allows the Commission to circumvent the country-of-origin principle and avoid that all complaints about big tech platforms end up with one national authority. The solution in the DSA maintains the country-of-origin principle while ensuring that it can enforce the DSA swiftly.[175] At the same time, the Commission is no impartial, independent regulator, which is the norm in media and data protection law.[176] Creating an impartial, independent DSA-regulator at the Union level could help ensure a unified approach to content moderation requirements for VLOPs, even if creating a new regulator may be difficult to achieve.[177]

79 Appointing the Commission or a newly to be created entity as DSA-regulator also means that service providers will be supervised by two regulators: a data protection authority for data protection issues and a digital services coordinator for DSA issues. It has been proposed that an interaction between these authorities will be essential as service providers will need to process a large amount of personal data when fulfilling the complaint management obligations.[178]

II. Sanctions: Losing the liability exemption?

80 Failure to comply with the rules of the DSA may, in the most serious cases, result in fines of up to 6% of the annual turnover of the service provider concerned. Providing false, incomplete or misleading information or failing to submit to an on-site inspection may result in a fine of up to 1% of annual turnover (Article 42).

81 Under the DSA approach, it may appear that the obligations essentially set a standard of liability for platforms, but given their sanction regime, this is ultimately not the case. The sanctions for non-compliance with DSA obligations are fines as well as periodic penalty payments. It is not the loss of exemption from liability. Linking the exemption from liability to compliance with the obligations could have been an alternative, possibly more deterrent, solution to fines. While the fines for VLOPs are potentially huge, they may end up being significantly lower than the maximum, as experience from competition law shows.[179] Wagner and Janssen note that antitrust fines have not pushed platforms into compliance, similarly to GDPR fines.[180] At the same time, the detailed obligations foreseen in the DSA could be more burdensome for service providers than a liability approach where platforms can choose how best to achieve remediation.[181]

82 The goal of preventing over-blocking by platforms appears to be the first reason why a regulatory approach was preferred, as it is meant to ensure some control over *how* platforms decide on removing illegal content. Yet, this outcome may also have been achievable by requiring compliance with due diligence obligations in order to enjoy the liability exemption. This would have effectively set a Union-wide standard of care for hosting providers and online platforms that reflects their role in moderating content. This option would simultaneously have allowed moving away from the passive/active distinction, which no longer fits today's online platforms.

174 Berberich and Seip (n 92).

175 Ben Wagner and Heleen Janssen, 'A First Impression of Regulatory Powers in the Digital Services Act' (*Verfassungsblog*, 4 January 2021) <https://verfassungsblog.de/regulatory-powers-dsa/> accessed 28 April 2021.

176 Wagner and Janssen (n 175) 1.

177 Wagner and Janssen (n 175) 3.

178 Härting and Adamek (n 48) 170.

179 Wagner and Janssen (n 175) 3.

180 Wagner and Janssen (n 175) 3.

181 Garry A. Gabison and Miriam C. Buiten, 'Platform Liability in Copyright Enforcement' (2020) 21 Science and Technology Law Review (STLR) 237.

83 A second reason why the liability route was not chosen can be found in the limits of harmonisation due to the principle of subsidiarity. The legal basis for the internal market allows the Commission to adopt rules that affect the liability rules of the Member States, but only to the extent necessary for the internal market. Establishing a positive liability standard at the EU level may, therefore, have been difficult to achieve on the basis of Article 114 TFEU. However, not only do the current rules already considerably affect liability under national rules, but the EU has also adopted liability rules in other contexts, such as antitrust damages actions.[182]

84 The choice to sanction violations of the DSA by a fine rather than by loss of exemption from liability impacts not only service providers but also individuals' rights and remedies. Private individual remedies such as claims for damages or injunctive relief do not follow the duties set out in the DSA. Injured parties continue to rely on national tort law provisions when seeking redress, which is not helped by the liability exemption. Vis-à-vis VLOPs, their extensive moderation policies bear the question of whether this approach is still valid today and in the foreseeable future.[183]

85 Finally, linking the obligations in the DSA to the liability exemption may have encouraged the use, development and improvement of automated detection tools of hosting platforms. Machine learning technologies already enable platforms to rely on automated tools both to perfect their business models and (often relatedly) to detect illegal activity online. While problems with over-blocking in relation to censorship must certainly be avoided, automated detection tools may well improve into (the most) effective means of detecting and removing illegal content online.[184] In this regard, a more significant leap in the liability framework for online platforms would have been to work towards a better, more precise, and above all, more accountable and transparent content moderation, rather than maintaining a focus on notice and takedown.

182 Parliament and Council Directive 2014/104/EU of 17 April 2014 on certain rules governing actions for damages under national law for infringements of the competition law provisions of the Member States and of the European Union, OJ L 349/1.

183 See also Leistner (n 1) 10, who notes: "The problem of private individual remedies should be addressed and considered when further discussing this arguably overextended regulatory framework for very large online platforms."

184 Buiten, De Streel and Peitz (n 8) 163.

F. Conclusion

86 The DSA is an ambitious proposal seeking to reconcile the responsibility of service providers, hosting providers and online platforms with their changed role in optimising and moderating content on their platforms. This goal, however, is not reflected in the liability regime of the DSA in itself, which adopts the liability rules of the e-commerce Directive essentially unchanged. Maintaining the passive/active distinction as a criterion for liability of service providers seems questionable given the extensive moderation that takes place on their platforms. Filtering, sorting and optimising content for profit is still seen as an activity of a purely technical, passive nature and does not result in "actual knowledge" of illegal content on the platform. Whether this reflects the AI-moderated world of today's online platforms may rightfully be doubted.

87 Nevertheless, the DSA brings significant changes to the regulatory framework for service providers. The new obligations and procedural requirements, particularly in relation to the notice and action regime, create a new regulatory approach, part of which is specifically targeted at those providers most likely to engage in problematic practices. While the core exemption from liability remains, service providers will be required to have mechanisms in place to monitor violations.

88 In conjunction with the draft DMA, the asymmetric rules reflect the central role that the largest platforms play in the digital economy today. The additional transparency and due diligence obligations on online platforms and VLOPs recognise the critical role they can play in curbing illegal and problematic content. As such, the DSA represents a significant change in the regulatory oversight exercised over large hosting providers.

89 Overall, the DSA moves the responsibility of intermediaries away from the area of liability and deeper into the realm of regulation. Under the DSA approach, it may appear that the obligations essentially set a standard of liability for platforms. But given the sanction regime, this is ultimately not the case. The sanctions for non-compliance with DSA obligations are fines and periodic penalty payments, not the loss of exemption from liability.

90 The goal of preventing over-blocking by platforms might explain why a regulatory approach was preferred, as it is meant to ensure some control over *how* platforms decide on removing illegal content. Yet, this outcome may have also been achieved by requiring compliance with the due diligence obligations for platforms to enjoy the liability exemption. In light of the changed role of service providers, particularly online platforms, the liability

framework could have been developed further by linking the due diligence obligations to the liability exemption. This would have allowed for a move away from the passive/active distinction and would set a Union-wide liability standard for online platforms.

91 The new framework could also have focused more on achieving better, more precise and above all, more accountable and transparent automated tools for content moderation, rather than aiming to perfect notice and takedown systems.[185] Advances in machine learning technologies enable platforms to increasingly rely on automated tools to detect illegal activity online. The use of automated detection tools by hosting platforms should be encouraged, provided that important safeguards are in place.[186] Hopefully, online platforms will continue to advance machine learning technologies to reduce problems of over-blocking and allow illegal content to be removed swiftly and precisely.

92 The texts of the DSA and DMA have already been subject to extensive public consultation but still need to be approved by the European Parliament and the European Council. The importance of a liability regime for platforms and users suggests that these issues will still be the subject of thorough attention and lengthy debate at various stages of the adoption of the regulation.

185 As Rössel points out, the use of machine filtering technology should help prevent over-blocking, but it is not regulated by the DSA. It is instead left to voluntary agreements between the parties involved (Rössel n 39, 98 and the references therein).

186 Buiten, De Streel and Peitz (n 8) 163.

The Out-of-court dispute settlement mechanism in the Digital Services Act

A disservice to its own goals

by **Jörg Wimmers***

Abstract: The Digital Services Act (DSA), proposed by the EU Commission, introduces extensive content moderation rules for online platforms. Under Article 18 DSA, users whose content has been blocked or removed or whose account has been suspended by the platform are entitled to select a certified out-of-court dispute settlement body to resolve their disputes with the service provider. The author describes context and parties of online speech, examines conditions and consequences of this redress mechanism, and concludes that the proposed provision is flawed in several ways: it does not approximate different regulation, but promotes fragmentation and creates legal uncertainty; it does not provide criteria or standards for the complex factual and legal determinations and balancing of rights in the area of online speech; and with the incentives set by this regulation, it opens the field for a race to the bottom. While out-of-court dispute settlement mechanisms usually aim at a consensual solution, placing emphasis on interests, rather than on the legal positions of the parties or on the rights asserted, free speech disputes are strictly normative and do not lend themselves to a settlement by private bodies, but are reserved for the judiciary. Moreover, most platforms have established appeals mechanisms for their users already allowing for a second review. By further extending this redress mechanism to decisions based on the platforms' community standards, the DSA frustrates existing 'flagging'-systems established by the platform providers, and thereby doing a disservice to its own goals. In the outlook the author proposes to modernize and build on the existing infrastructure of the judiciary to address needs of private persons to pursue their rights and to ensure the quality of process and decision, rather than duplicating the existing court system by adding a redress system of private alternative dispute resolution (ADR) bodies.

Keywords: Digital Services Act; Social Networks; Hosting Privilege; ADR; Community Standards; Free Speech

Recommended citation: Jörg Wimmers, The Out-of-court dispute settlement mechanism in the Digital Services Act - A disservice to its own goals, 12 (2021) JIPITEC 381 para 1

A. Introduction

1 With the out-of-court dispute settlement mechanism in Article 18 of the draft Digital Services Act[1] (in the following "DSA"), the "settlement euphoria"[2] of the European legislature has reached the field of free speech. Directive 2013/11/EU on alternative dispute resolution (ADR)[3] for consumer disputes and Regulation 524/2013 on online dispute resolution for

* Jörg Wimmers, LL.M. (NYU), partner in the Hamburg office of international law firm Taylor Wessing.

1 Commission, 'Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC' COM(2020) 825 final.

2 The term along with its critical undertone is borrowed from Horst Eidenmüller/Martin Engel, 'Against False Settlement: Designing Efficient Consumer Rights Enforcement Systems in Europe' [2014] 29:2 Ohio State Journal on Dispute Resolution 261.

3 Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Directive on consumer ADR).

consumer disputes (ODR)[4] laid the groundwork for an easily accessible framework within which consumers can pursue their rights quickly and effectively. While doubts persist as to whether these legislations have accomplished their goals[5], Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services[6] translated the out-of-court redress into the sphere of internet intermediary services and search engines. While these legislative acts all concerned the role of ADR and ODR in online commerce, Directive 2019/790 on copyright and related rights in the Digital Single Market[7] took a view on the effects of "steps taken by online content-sharing service providers in cooperation with rightholders" on the freedom of expression of those users of the platforms who upload their content and calls on Member States to ensure that these users have access to out-of-court redress mechanisms. Similarly, Directive 2018/1808 amending the Audiovisual Media Services Directive[8] provides for such out-of-court redress for the settlement of disputes between users and video-sharing platform providers.

2 The European Commission's proposal for a Digital Services Act follows suit and prescribes in Article 18 an out-of-court dispute settlement mechanism that uploaders may select when their content is blocked or removed by the platform operator, or when their account or the provision of the service is suspended or terminated. With its predecessors this proposal appears to be on safe ground. This paper will argue the opposite. Doubts are already appropriate because of the apparent lack of empirical data. The Commission itself admits in its Impact Assessment that with regard to out-of-court ADR systems "there is a level of uncertainty, as no reliable data or precedent allows to estimate what volumes of complaints would be escalated"[9]; the availability of ADR in all Member States "would however facilitate access to such mechanisms and likely append negligible costs compared to the current system." The dispute settlement mechanism of Article 18 DSA is flawed in several ways, as will be laid out in more detail below:

- Article 18 DSA is against its intention not approximating different regulation, but promotes fragmentation and creates legal uncertainty. The provision adds to a cacophony of different rules for redress mechanisms[10] that apply to the same service and creates a patchwork of overlapping regulation.[11]

- The DSA does not harmonize regulation "on the merits", but subjects online platforms to the laws of all 27 Member States. There is also no procedural approximation:[12] By providing no standards or criteria for the complex factual and legal determinations and balancing of rights in the area of online speech, the quality of the decision-making process will vary as will the decisions; Article 18 DSA opens the field for a classic race to the bottom.

- With its sweeping reference to Article 11 of the Charter, the Commission fails to recognize that the rights of the Charter are addressed to the institutions and bodies of the Union and do not apply directly to the horizontal relationship between private parties. Therefore, one cannot simply transpose the standard of free speech to which the Union and Member States authorities are bound to private online platforms.

4 Regulation (EU) No 524/2013 of the European Parliament and of the Council of 21 May 2013 on online dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Regulation on consumer ODR).

5 Alexandre Biard, 'Impact of Directive 2013/11/EU on Consumer ADR Quality: Evidence from France and the UK' [2019] 42 Journal of Consumer Policy 109.

6 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.

7 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.

8 Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities.

9 Commission, 'Commission Staff Working Document, 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' SWD(2020) 348 final, Part 1/2, para 193.

10 cf e.g. Article 17(9) of the EU Copyright Directive (n 7), Article 28b of the Audiovisual Media Services Directive (n 8), or Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services (n 6).

11 See infra IV.1.

12 See infra IV.1.

These platforms must have room to direct their network towards specific target groups,

- create respectful interactions within their platform community, or minimise liability risks with regard to possible illegal content.[13]

- Out-of-court dispute settlement mechanisms usually aim at a consensual solution, placing emphasis on interests, rather than on the legal positions of the parties or on the rights asserted. Free speech disputes on the other hand are strictly rights based; there is no room for give and take. With ADR and its online-sibling ODR, even in the field of commercial disputes being far from a silver bullet solution, free speech disputes do not lend themselves to settlement by private bodies. Free speech is a classic field reserved for the judiciary, subject to extensive and nuanced case law, and we should refrain from creating a parallel layer of ADR providers next to the competent court system.[14]

- Article 18 DSA also operates against its own goals. By subjecting decisions by platform operators to remove or block content based on their community standards to the redress mechanism, the DSA frustrates the pre-existing and efficient "flagging"-systems established by all major social networks. These systems are effective, because they are easy and quick to use; the amount of content removed on this basis alone shows that the significant procedural requirements established by Article 18 DSA will likely render these systems unfeasible. Article 6 DSA intends to reward such "voluntary own-initiative investigations", whereas Article 18 DSA does the opposite.[15]

3 To stake out the field, this paper will first take a look at the background for the Commission's votum for an out-of-court dispute settlement mechanism (B.). This will be followed by a description of the relevant provisions of the draft DSA, their scope of application as well as relevant carve-outs (C.), a discussion of the out-of-court redress mechanism (D.) and an outlook and proposal (E.).

13 See infra IV.2.a).

14 See infra IV.3.b).

15 See infra IV.4.

B. The background: The influence of operators on the content available on their online platforms

4 There is a heated debate in Europe about the "censoring" of free speech by private entities. It is claimed that internet-based platforms have grown to become powerful intermediaries, organising, curating and "increasingly controlling" communications in the virtual world[16], and it is argued that it should not be left to private and profit-oriented businesses to decide what content is available on the Internet and what content not.

5 This debate is a revenant of the sometimes sharply conducted upload-filter discussion in the context of the EU Copyright Directive.[17] There is no doubt that freedom of expression constitutes one of the essential foundations of a democratic society and one of the basic conditions for its progress and for each individual's self-fulfilment.[18] However, the debate on

16 Gerhard Wagner, 'Haftung von Plattformen für Rechtsverletzungen (Teil 1)' [2019] GRUR 329; Julia Reda, 'Der Digital Services Act steht für einen Sinneswandel in Brüssel' (netzpolitik.org, 5 January 2021) <https://netzpolitik.org/2021/edit-policy-der-digital-services-act-steht-fuer-einen-sinneswandel-in-bruessel/> accessed 20 August 2021; cf. also recital 3 DSA.

17 cf e.g. Markus Reuter, 'Protests against Copyright Directive: All Cities, Dates and Numbers of Participants across Europe' (netzpolitik.org 25 March 2019) <https://netzpolitik.org/2019/protests-against-copyright-directive-all-cities-dates-and-numbers-of-participants-across-europe/> accessed 20 August 2021; Michael Hanfeld, 'Protest gegen EU-Urheberrecht: „Seid ihr Bots? Seid ihr ein Mob?"' Frankfurter Allgemeine Zeitung (Frankfurt, 23 March 2019) <https://www.faz.net/aktuell/feuilleton/debatten/proteste-gegen-und-eintreten-fuer-das-eu-urheberrecht-16104780.html> accessed 20 August 2021; Julia Reda, ‚Upload Filters' (juliareda.eu, no date) <https://juliareda.eu/eu-copyright-reform/censorship-machines/> accessed 20 August 2021; Julia Reda, Joschka Selinger, Michael Servatius, 'Article 17 of the Directive on Copyright in the Digital Single Market: a Fundamental Rights Assessment' (freiheitsrechte.org, 16 November 2020) <https://freiheitsrechte.org/home/wp-content/uploads/2020/11/GFF_Article17_Fundamental_Rights.pdf> accessed 20 August 2021.

18 *Handyside v The United Kingdom* App no 5493/72 (ECtHR, 7 December 1976), para 49; *Hasan Yazici v Turkey* App no 40877/07 (ECtHR, 15 July 2014), para 48; see regarding this discussion now the instructive statements by Advocate General Saugmandsgaard-Øe in his Opinion in Case C-401/19 *Republic of Poland v European Parliament, Council of the European Union* (Opinion of AG Saugmandsgaard-Øe, 15 July 2021).

the role of internet intermediaries for the process of public communication is often fuelled by political beliefs; on the other hand, it sometimes takes too little consideration of the different actors in online communication and their roles, "responsibilities, powers and capabilities."[19] It is often overlooked in these discussions that the multipolarity of different participants to a communication with different and sometimes conflicting rights and interests is the special feature of online communication over platforms such as Twitter, Facebook, Reddit, or YouTube. There is (i) the person making an online statement, i.e. the uploader of content, there may or may not be (ii) an infringed person, there are (iii) other recipients of the service, viewing the uploaded content[20], and there is (iv) the online platform, defined by Article 2(h) DSA as a provider of hosting services which, at the request of a recipient of the service, stores and disseminates to the public information.[21]

I. Online platforms are hosting services that have neither knowledge of nor control over the content on their platforms

6 Online platforms are hosting providers subject to the (conditional) liability exemption in Article 14 of the e-Commerce Directive if their "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 information which is transmitted or stored."[22] A platform operator can no longer rely on this privilege, where it plays an 'active role' giving it 'knowledge of, or control over' the data which it stores at the request of its users.[23] While it is a truism that any service provider storing information provided by its users necessarily has control over that information as it has the technical capacity to remove or to disable access to it[24], "control" in the sense of an active role requires more, i.e. that the online platform, by the nature of its activity, acquires the intellectual control of that content by selecting the content or otherwise being involved in the content or its presentation.[25] In general, therefore, the online platforms which are at the core of the current discussion—Twitter, Facebook, Reddit, YouTube, etc.—do not "control" the content on their platforms within this meaning. They are intermediaries protected with their content-neutral activity under the liability privilege of Art. 14(1) of the e-Commerce Directive.[26]

7 In his opinion in the joined cases C-682/18 and C-683/18, Advocate General *Saugmandsgaard-Øe* explained that "the logic of 'notice and take down' underlying Article 14(1) seeks to strike a balance between the different interests at stake, and, in particular, to safeguard the freedom of expression of users."[27] The notification is intended to give the op-

19 This is – with the qualification of "special responsibilities" – the formulation used by the Court of Justice of the European Union (CJEU) to define the role of search engines: Case C-136/17 *GC and Others v Commission nationale de l'informatique et des libertés (CNIL)* (CJEU, 24 September 2019), para 49.

20 Regarding their fundamental rights and necessary safeguards cf Case C-314/12 *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH, Munich (Germany), Wega Filmproduktionsgesellschaft mbH* (CJEU, 27 March 2014).

21 Wagner (n 16) 329.

22 Recital 42 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').

23 C-324/09 *L'Oréal SA and Others v eBay International AG and Others* (CJEU, 12 July 2011), para 113; 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 (C-683/18)* (CJEU, 22 June 2021), para 106.

24 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 (C-683/18)* (Opinion of Advocate General Saugmandsgaard-Øe, 16 July 2020), para 151.

25 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 (C-683/18)* (Opinion of Advocate General Saugmandsgaard-Øe, 16 July 2020), para 152.

26 CJEU, judgment dated 3 October 2019 - case C-18/18, para. 22 – Glawishnig-Piesczek/Facebook; 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 (C-683/18)* (Opinion of Advocate General Saugmandsgaard-Øe, 16 July 2020), para 151.

27 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 (C-683/18)* (Opinion of Advocate General Saugmandsgaard-Øe, 16 July 2020), para 186; 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 (C-683/18)* (CJEU, 22 June 2021), para 113; see also C-401/19 *Republic of Poland v European Parliament, Council of the European Union* (Opinion of AG Saugmandsgaard-Øe, 15 July 2021), para 126 et seq,

erator of the service sufficient evidence to verify the illegal nature of the information, as a provider must remove such information only "where its illegal nature is 'apparent', that is to say manifest. That requirement seeks [...] to avoid forcing a provider itself to come to decisions on legally complex questions and, in doing so, turn itself into a judge of online legality."[28]

8 What is true in this copyright case, where the assessment of the infringing character of an uploaded file requires a number of contextual elements and a thorough legal analysis[29], is all the more true for free speech. The determination whether speech is unlawful requires the examination of a statement within its context and the balancing of conflicting fundamental rights, including possible effects and consequences of measures for parties playing an intermediary role on the Internet.[30] An intermediary is generally unable to make this determination. He does not have any own knowledge about the statement and its accuracy, he is in no position to prove whether the incriminated statement is truthful, and therefore cannot make its own assessment of the material justification of a statement.[31]

II. European and national legislatures curtail the hosting provider privilege for online platforms and demand operators to determine and remove illegal content

9 This notwithstanding, both the European and the national legislatures increased their demands on online platforms to step up their measures against certain content uploaded by its users, as have courts.[32] As a result, the (conditional) liability exemption for these neutral platform operators is crumbling.[33] The EU Copyright Directive reversed the previously widely held view[34] that the platform operator does not itself engage in any act of use under copyright law.[35] National legislative initiatives such as the Network Enforcement Act[36] in Germany and similar laws enacted in France and Austria[37] are especially aimed towards hate speech and increasingly place responsibility for (illegal) content posted by users on the platform operator with ever-growing information,

132 et seq.

28 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 (C-683/18)* (Opinion of Advocate General Saugmandsgaard-Øe, 16 July 2020), para 187.

29 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 (C-683/18)* (Opinion of Advocate General Saugmandsgaard-Øe, 16 July 2020), para 188.

30 *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v Hungary* App no 22947/13 (ECtHR, 2 February 2016), para 68 et seq.

31 BGH GRUR 2020, 1338, para 38; Wagner (n 16) 336.

32 Case C-18/18 *Eva Glawischnig-Piesczek v Facebook Ireland Limited* (CJEU, 3 October 2019), which did not see a violation of Article 15 of the e-Commerce Directive by a national court ordering Facebook to block also not identical, but equivalent content.

33 Wagner (n 16) 329; regarding search engines cf Case C-131/12 *Costeja v Google Spain* (CJEU,13 May 2014); C-136/17 – GC et al (CJEU, 24 September 2019); cf also Article 29 Data Protection Working Party, 'Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Espagnola de Proteccion de Datos (AEPD) and Mario Costeja Gonzales" C-131/12 [2014] 14/EN WP 225.

34 cf 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 (C-683/18)* (Opinion of Advocate General Saugmandsgaard-Øe, 16 July 2020), para 102

35 According to Directive 2019/790 (n 7), art 17(9), Member States shall also provide that online content-sharing service providers put in place an effective and expeditious complaint and redress mechanism that is available to users of their services in the event of disputes over the disabling of access to, or the removal of, works or other subject matter uploaded by them; Member States shall also ensure that out-of-court redress mechanisms are available for the settlement of disputes.

36 Netzwerkdurchsetzungsgesetz vom 1. September 2017 (BGBl. I S. 3352) (Network Enforcement Act), latest changes by Article 15 Nos 3 and 6 of the law dated 30 March 2021 (BGBl. I S. 448).

37 Bundesgesetz über Maßnahmen zum Schutz der Nutzer auf Kommunikationsplattformen (Kommunikationsplattformen-Gesetz – KoPl-G); BGBl. I Nr. 151/2020 (Federal Act Regarding Measures for the Protection of Users on Communication Platforms); in France the so-called *Loi Avia* was adopted in May 2020, cf. <https://www.assemblee-nationale.fr/dyn/15/textes/l15t0419_texte-adopte-provisoire.pdf; in a decision dated 18 June 2020, the French Conseil Constitutionnel struck down some of the law's provisions, cf https://www.conseil-constitutionnel.fr/decision/2020/2020801DC.htm>.

review and removal, as well as procedural and reporting obligations.[38]

10 Hate speech, online bullying, and defamation have become commonplace on the Internet[39] and false or misleading information has been surging, in particular, with regard to the current pandemic and in organized attempts to influence democratic elections in the U.S. and elsewhere. There seems to be wide consensus that the tech companies operating the largest online platforms must live up to their responsibility in combating these phenomena.[40] On the other hand, legislative acts demanding platforms to determine and remove user uploaded content as illegal have been heavily criticised not only with regard to the hosting provider privilege[41], but especially due to possible "chilling effects" for the freedom of expression and information.[42]

11 It is true that such regulation unavoidably tips the balance in favour of the complainants and against online speech. From an economic perspective, it is reasonable behaviour by the platform operators to

38 In its proposal for a Network Enforcement Act the government reasoned that there was "*currently a massive change in social discourse on the net and in social networks in particular. The culture of debate on the net is often aggressive, hurtful and not infrequently hateful. [...] Hate crime and other criminal content that cannot be effectively combated and prosecuted poses a great danger to the peaceful coexistence of a free, open and democratic society. Moreover, following the experience of the U.S. election campaign, combating criminal false news ("fake news") on social networks has also become a high priority in the Federal Republic of Germany. There is therefore a need to improve law enforcement on social networks in order to immediately remove objectively punishable content such as incitement of the people, insult, defamation or disturbing the public peace by pretending to have committed a crime*"; Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG), available at <https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RegE_NetzDG.pdf;jsessionid=BCE7F452F946378EA96140490839B26D.2_cid324?__blob=publicationFile&v=2> accessed 20 August 2021.

39 See the four day social media boycott by English professional football clubs following a series of high-profile online racist attacks: Mark Townsend, 'Footballers and clubs to boycott social media in mass protest over racist abuse' *The Guardian* (London, 24 April 2021) <https://www.theguardian.com/football/2021/apr/24/footballers-to-boycott-social-media-in-mass-protest-over-racist-abuse> accessed 20 August 2021.

40 Wagner (n 16) 337 et seq, who sees a gatekeeper role of the online platforms as a justification for their liability.

41 It was held that, in particular, the country-of-origin principle in Article 3 of Directive 2000/31/EC (the "e-Commerce Directive") and the liability provisions for hosting providers in Article 14, 15 of that Directive were violated.

42 In Germany, it was opined that the Network Enforcement Act caused platform operators to structurally decide to remove reported content and had an inherent "systemic tendency towards deletion"; Josef Drexl, 'Bedrohung der Meinungsvielfalt durch Algorithmen' [2017] ZUM 529; Thorsten Feldmann, '**Zum Referentenentwurf eines NetzDG: Eine kritische Betrachtung' [2017]** K&R 292; Eike Michael Frenzel, 'Aktuelles Gesetzgebungsvorhaben: Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (NetzDG)' [2017] JuS 414; Hubertus Gersdorf, 'Hate Speech in sozialen Netzwerken' [2017] MMR 439; Nikolas Guggenberger, 'Das Netzwerkdurchsetzungsgesetz in der Anwendung' [2017] NJW 2577; Nikolas Guggenberger, 'Das Netzwerkdurchsetzungsgesetz – schön gedacht, schlecht gemacht' [2017] ZRP 98; Bernd Holznagel, 'Das Compliance-System des Entwurfs des Netzwerkdurchsetzungsgesetzes' [2017] ZUM 2017, 615; Fiete Kalscheuer/Christian Hornung, 'Das Netzwerkdurchsetzungsgesetz – Ein verfassungswidriger Schnellschuss' [2017] NVwZ 1721; Ralf Köbler, 'Fake News, Hassbotschaft und Co. - ein zivilprozessualer Gegenvorschlag zum NetzDG' [2017] AfP 282; Karl-Heinz Ladeur/Tobias Gostomzyk, 'Das Netzwerkdurchsetzungsgesetz und die Logik der Meinungsfreiheit' [2017] K&R 390; Marc Liesching, 'Was sind »rechtswidrige Inhalte« im Sinne des Netzwerkdurchsetzungsgesetzes?' [2017] ZUM 809; Holger Lutz/Sebastian Schwiddesen, 'The New German Hate Speech Law – Introduction and Frequently Asked Questions' [2017] CRi 103; Georg Nolte, 'Hate-Speech, Fake-News, das »Netzwerkdurchsetzungsgesetz« und Vielfaltsicherung durch Suchmaschinen' [2017] ZUM 552; Boris P. Paal/Moritz Hennemann, 'Meinungsbildung im digitalen Zeitalter' [2017] JZ 641; Gerald Spindler, 'Das Netzwerkdurchsetzungsgesetz' [2017] K&R 533; Gerald Spindler, 'Rechtsdurchsetzung von Persönlichkeitsrechten' [2018] GRUR 365; Jörg Wimmers/Britta Heymann, 'Zum Referentenentwurf eines Netzwerkdurchsetzungsgesetzes (NetzDG) – eine kritische Stellungnahme' [2017] AfP 93; Marc Liesching, 'Die Durchsetzung von Verfassungs- und Europarecht gegen das NetzDG' [2018] MMR 26; Marc Liesching, in Spindler/Schmitz, TMG, 2. Edition., 2018, § 1 NetzDG Rn. 6 ff., 13 ff., 21 ff.; Matthias Ringer/Dirk Wiedemann, 'Beschwerdeverfahren bei Facebook wegen Markenverletzung - "Gefällt mir"?' [2018] GRURPrax 203; Gunter Warg, 'Meinungsfreiheit zwischen Zensur und Selbstzensur' [2018] DÖV 473.

take such complaints at face value and remove content upon notice. This saves cost and reduces legal risks of litigation in which the platform operator—with no own knowledge—is at a structural disadvantage. These regulations therefore set an incentive for the provider to keep at least a "safe distance" in their decisions leading to the removal of content which—while repulsive, indecent or otherwise offensive—may not violate the law.[43] And there is another incentive amplifying this risk of overblocking[44]: persons, who are the subject of information on the Internet, that—while legal—they consider detrimental[45], may (and will) exploit this structural disadvantage of the online platform by attacking speech with contrived or even false allegations.[46] However, this possible risk of overblocking prescribed by the legislator will not be cured by now also outsourcing conflict resolution, after the evaluation and determination of criminal content on the internet has already been transferred to the platform operators.[47]

43 BGH GRUR 2020, 1338, para 38; Daphne Keller, 'Who Do You Sue? State and Platform Hybrid Power over Online Speech' (Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 1902, 29 January 2019) <https://www.lawfareblog.com/who-do-you-sue-state-and-platform-hybrid-power-over-online-speech> accessed 20 August 2021, 3; operators could even remove content upon notification without any (cost-intensive) examination on the basis of an economic risk assessment, since the economic consequences of an unauthorized deletion are marginal compared to high fines and/or the operational expense of the establishment of legally trained staff positions to assess the content; cf Liesching (n 43) 27; id. in Spindler/Schmitz, TMG, 2nd ed., 2018, § 1 NetzDG marginal no. 25.

44 Gerhard Wagner, 'Haftung von Plattformen für Rechtsverletzungen (Teil 2)' [2020] GRUR 447, 452.

45 Examples are manifold: The manager of financial services companies who is going after blog-posts on his companies' business practices; right wing activists and conspiracy theorists pursuing critical reports on their activities or opinions.

46 cf Commission, 'Communication from the Commission to the European Parliament, the Council. The European Economic and Social Committee of the Regions, Tackling Illegal Content Online, Towards an enhanced responsibility of online platforms' COM(2017) 555 final, 18; Keller (n 44) 3.

47 The author is critical oft he approach taken by the German legislator with the Network Enforcement Act (NetzDG), which imposes on the platforms the determination whether content violates certain offences of the German Criminal Law Act: instead he favors a clear strengthening and reinforcement of the prosecutor's offices and the police for the prosecution of uploaders of criminal content on the internet; see also the study "Hass auf Knopfdruck" quoted at n. 132, which indicates that it may be a small group of users posting the majority of hateful comments; see also Johanna Spiegel, Britta Heymann, 'Ein Minenfeld für Anbieter sozialer Netzwerke – Zwischen NetzDG, Verfassungsrecht und Vertragsfreiheit' [2020] K&R 344, 349.

III. The decisions of online platforms to remove illegal content and removals for community guidelines violations

12 Such regulation unavoidably tips the balance in favour of the complainants and against online speech. From an economic perspective, it is reasonable behaviour by the platform operators to take such complaints at face value and remove content upon notice. This saves cost and reduces legal risks of litigation in which the platform operator—with no own knowledge—is at a structural disadvantage. These regulations therefore set an incentive for the provider to keep at least a "safe distance" in their decisions leading to the removal of content which—while repulsive, indecent or otherwise offensive—may not violate the law.[48] And there is another incentive amplifying this risk of overblocking[49]: persons, who are the subject of information on the Internet, that—while legal—they consider detrimental[50], may (and will) exploit this structural disadvantage of the online platform by attacking speech with contrived or even false allegations.[51]

48 BGH GRUR 2020, 1338, para 38; Daphne Keller, 'Who Do You Sue? State and Platform Hybrid Power over Online Speech' (Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 1902, 29 January 2019) <https://www.lawfareblog.com/who-do-you-sue-state-and-platform-hybrid-power-over-online-speech> accessed 20 August 2021, 3; operators could even remove content upon notification without any (cost-intensive) examination on the basis of an economic risk assessment, since the economic consequences of an unauthorized deletion are marginal compared to high fines and/or the operational expense of the establishment of legally trained staff positions to assess the content; cf Liesching (n 43) 27; id. in Spindler/Schmitz, TMG, 2nd ed., 2018, § 1 NetzDG marginal no. 25.

49 Gerhard Wagner, 'Haftung von Plattformen für Rechtsverletzungen (Teil 2)' [2020] GRUR 447, 452.

50 Examples are manifold: The manager of financial services companies who is going after blog-posts on his companies' business practices; right wing activists and conspiracy theorists pursuing critical reports on their activities or opinions.

51 cf Commission, 'Communication from the Commission to the European Parliament, the Council. The European

13 In addition to these new statutory obligations for platform operator to block or remove criminal content on the platform, the DSA takes on the removal of content based on the platforms' terms and conditions, i.e. on the contractual relationship between the uploader and the platform operator. In its Impact Assessment the Commission points out that decisions by online platforms to remove content were "often not based on an assessment of the legality of the content, [...] but they are solely governed by the discretionary powers of the platform according to the terms of services that are part of their contractual terms".[52]

14 While the public debate sometimes focuses on striking examples of nonsensical blockings, such as the removal of copies of the famous Courbet painting "L'Origine du Monde"[53] or Facebook's blocking of the passage "merciless Indian Savages" from the Declaration of Independence of the United States of America[54], more relevant for this discussion are other court decisions obligating social networks to reinstate content they have blocked for violations of their 'community standards' or 'community guidelines', which form part of the contractual relationship between platform and user. "Facebook may not delete at will" headlines the German daily newspaper *Sueddeutsche Zeitung* about a judgment by the court of appeals in Munich—not without a touch of *Schadenfreude*. It continues: "Facebook must respect freedom of expression and other fundamental rights in the same way as the state."[55]

15 Must it? These "community guidelines" or "community standards" define what is and what is not allowed on the respective platform. In order to "enforce" these guidelines and to engage their communities of registered users in keeping certain content off the platform, online platforms, and particularly social networks, already established so-called "flagging" mechanisms years ago. These mechanisms allow registered users to choose from defined categories of "guideline" violations in a drop-down-menu and report potentially incompatible content with one click and without the need for a further explanation. Community guidelines violations concern a whole universe of decisions that range from spam and deceptive practices, to graphic, violent, pornographic or abusive content and hate speech, etc.[56] Employees of the provider compare such "flags" against the alleged community guideline violation and, where applicable, remove content. Most providers put specific trust in the notifications of so-called "trusted flaggers", i.e. persons or organisations which have shown in their submissions that their judgment is trustworthy.[57] All major online platforms have complaint handling mechanisms, they inform their uploaders, whose content is removed about their decision and its basis,[58] and allow these uploaders to appeal—where this is appropriate with regard to freedom of expression. These systems are balanced, they are swift and effective, and they are used extremely widely proving the success of this tool. Online platforms are not dealing with a few hundred thousand flaggings but with numbers in the millions or even billions[59]; and there are only few appeals of these removal decisions.[60]

Economic and Social Committee of the Regions, Tackling Illegal Content Online, Towards an enhanced responsibility of online platforms' COM(2017) 555 final, 18; Keller (n 44) 3.

52 Commission, Impact Assessment (n 9) SWD(2020) 348 final, Part ½, para 51.

53 Philippe Sotto, 'French Court Issues Mixed Ruling in Facebook Nudity Case' U.S. News and World Report (March 15, 2018) <https://www.usnews.com/news/business/articles/2018-03-15/french-court-issues-mixed-ruling-in-facebook-nudity-case> accessed 20 August 2021.

54 Keller (n 44) 1.

55 'Facebook darf nicht nach Belieben löschen' Sueddeutsche Zeitung (6 September 2018) <https://www.sueddeutsche.de/digital/facebook-beitraege-loeschen-1.4119997> accessed 20 August 2021; at the time of publishing the decision rendered by the Federal Court of Justice (BGH) on 29 July 2021 (III ZR 179/20 and III ZR 192/20) on Facebook's appeal was not available as a full-text judgment. According to the press release by the BGH, the court demanded Facebook to reinstate the removed content.

56 cf the community guidelines of YouTube: 'Community Guidelines' <https://www.youtube.com/intl/ALL_en/howyoutubeworks/policies/community-guidelines/> accessed 20 August 2021, the Twitter Rules at: 'The Twitter Rules' <https://help.twitter.com/en/rules-and-policies/twitter-rules> accessed 20 August 2021.

57 The provision on Trusted Flaggers in Article 19 DSA is a different concept of regulatory stipulations for organisations, e.g. law enforcement.

58 Note, however, that the Federal Court of Justice (BGH) in its decision dated 29 July 2021 (n 50) demanded Facebook to reinstate blocked content, because Facebook's terms and conditions did not provide for such information to the uploader and were, therefore, invalid; cf press release: 'Bundesgerichtshof zu Ansprüchen gegen die Anbieterin eines sozialen Netzwerks, die unter dem Vorwurf der "Hassrede" Beiträge gelöscht und Konten gesperrt hat' (Karlsruhe, 29 July 2021) <https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/DE/2021/2021149.html> accessed 20 August 2021.

59 For some more detailed figures on YouTube and Facebook see below at footnote 81 and 82.

60 See the figures e.g. for YouTube at: <https://transparen-

C. The out-of-court-dispute-settlement in Article 18 of the draft DSA

I. The complaint and redress mechanism of the DSA

16 Article 18 DSA provides for an out-of-court dispute settlement mechanism that "recipients of the service" (in the following also referred to as the uploader) may select to resolve disputes relating to decisions by an online platform:

- *to remove or disable access to information recipients have provided,*
- *to suspend or terminate the provision of the service, in whole or in part to the recipients, or*
- *to suspend or terminate the recipients' account.*

17 Article 18 must be read in the context of Articles 15 and 17 DSA, as the new procedural redress mechanism of the DSA is composed of several steps.[61] Article 15 DSA obliges the online platform to a "clear and specific statement of reasons" for its decision including information on the redress possibilities for the recipient. Pursuant to Article 17 DSA, online platforms are required to provide the uploaders—"for a period of at least six months following the decision"—with access to an effective, cost-free internal complaint-handling system against the operator's decisions. Where a complaint contains sufficient grounds that the information is not illegal and not incompatible with the terms and conditions of the provider, the provider shall reverse the decision. Users shall be informed about the decision and the possibility of out-of-court dispute settlement and other available redress possibilities without undue delay.

18 Article 18 DSA entitles users to select any of the certified bodies for out–of-court settlement and requires online platforms to engage "in good faith" with these bodies. The provider "shall be bound by the decision taken by the body", whereas the user's right to redress against the platform's decision before a court remains unaffected by his entitlement to an out-of-court settlement. Article 18(2) DSA establishes conditions and procedures for the certification of bodies for out-of-court settlement, which shall be, inter alia, impartial and independent, 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 of terms and conditions; the body shall be easily accessible through electronic communications technology, capable of settling the dispute "in a swift, efficient and cost-effective manner", and operate "with clear and fair rules of procedure." According to Article 18(3), the online platform shall reimburse the recipient for fees and expenses if the body decides in favour of the user, but the user shall not the online platform, if the body decides in the platform's favour.

II. The personal scope of the dispute settlement mechanism in Article 18

19 "Recipients of the service" may select a body for an out-of-court dispute settlement, which includes by definition any natural or legal person using the service,[62] thereby extending this right also to companies, associations, political parties, etc. While for example the use of online platforms for political parties may be of particular importance especially in pre-election phases,[63] they do not appear to be in need of additional safeguards to exercise their rights; in particular, it is not comprehensible why a sophisticated business or political party using the platform should not be required to reimburse the online platform in case the body decides in favour of the platform.[64]

cyreport.google.com/youtube-policy/appeals> accessed 20 August 2021.

61 Martin Eifert/Axel Metzger/Heike Schweitzer/Gerhard Wagner 'Taming the Giants: The DMA/DSA Package' [2021] 58 CML Rev. 1.

62 Article 2(g) DSA.

63 cf BVerfG NJW 2019, 1935; abstract available in English at https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2019/05/qk20190522_1bvq004219en.html;jsessionid=6CB81961C1195DC92910524D32C93A52.1_cid377.

64 See Article 18(3) DSA; another lopsidedness follows from the fact that while the uploader is granted these rights and safeguards, the person whose rights may be infringed does not. Why a person affected by, for example, an infringing (defamatory) statement should not have access to such proceedings for his part is not clear against the background of the "fundamental rights" perspective that the Commission adopts with its proposal. This is not suggesting a further extension of the proposed regulations, but rather another indication that the Commission's proposal seems one-sided and half-baked; see also Eifert/ Metzger/Schweitzer/Wagner (n 58) 25.

III. The material scope of the dispute settlement mechanism in Article 18 DSA

20 The decisions subject to the out-of-court redress of Article 18 DSA can be based on either the illegality of the content or its incompatibility with the terms and conditions of the provider.

21 The DSA does not define what constitutes illegal content, but generally refers to "any information which – by itself or by its reference to an activity – is not in compliance with Union law or the law of a Member State" (Art. 2(g) DSA). This broad "horizontal" approach will require online platforms operating in all EU member states to apply the requirements of EU law, but also the standards of 27 national legal systems. Within the limits set by the country-of-origin principle of Article 3 of the e-Commerce Directive, this will present major challenges. This wide scope of application is also subject to significant "carve-outs" (see in the following 1.) and burdened with uncertainties and ambiguities (see in the following 2.). The redress is not only available for decisions by the platform on "illegal content," but also those that are based on an incompatibility with the terms and conditions of the provider (see in the following 3.).

1. The carve-outs for copyright infringements and video-sharing platform providers

22 Pursuant to Article 1(5)(c), the DSA is without prejudice to the rules laid down by Union law on copyright and related rights. While the DSA is somewhat ambivalent as to the scope of this carve-out,[65] recital 11 clarifies that Union law on copyright and related rights establishes "specific rules and procedures that should remain unaffected". This confirms that at least the provisions on "an effective and expeditious complaint and redress mechanism" in Article 17(9) of Directive (EU) 2019/790 take precedence over the provisions in Articles 17 and 18 DSA.[66] The complaint and redress mechanism in Article 17(9) of Directive (EU) 2019/790 takes copyright infringements on a platform like YouTube out of the scope of application of the DSA's out-of-court dispute settlement mechanism and—depending on the Member States' laws enacted pursuant to Article 17(9) of Directive 2019/790—requires such platforms to establish different workflows, systems and to submit itself—depending on the content in question—to different redress mechanisms.[67]

23 An even more significant carve-out follows from the recently amended Audiovisual Media Services Directive (AVMSD),[68] regarding which recital 9 of the DSA states that the DSA "should complement, yet not affect" its application. More specifically, the AVMSD shall be considered *lex specialis* in relation to the DSA.[69] Directive (EU) 2018/1808 amended the AVMSD by adding new provisions concerning so-called "video-sharing platform services", i.e. platforms devoted to user-generated content for which the platform does not have editorial responsibility,[70] such as e.g. YouTube, DailyMotion, etc. Article 28b of that Directive provides for specific obligations for video-sharing platforms regarding certain "illegal content" as defined by the *aquis communautaire*: Member States have to ensure that video-sharing platform providers under their jurisdiction take appropriate measures to protect minors, the general public against the incitement to violence or hatred directed against a group of persons or a member of a group, and the general public from content of which dissemination constitutes certain criminal offences under Union law in the areas of terrorist activities,

65 While Art. 1(5) DSA carves out copyright law, Recital 12 mentions the non-authorised use of copyright protected material shall be covered by the broad concept of illegal content within the meaning of the DSA.

66 A different view takes: Gerald Spindler, 'Der Vorschlag für ein neues Haftungsregime für Internetprovider – der EU-Digital Services Act Teil 2: Große und besonders große Plattformen' [2021] GRUR 653, who suggests that the requirements of Article 18 DSA can be used to concretize the dispute resolution mechanisms, which are only sketched out by Article 17(7) et seq. of the Copyright Directive.

67 It is the view of the European Commission that the "DSA is not an IPR enforcement tool" given its horizontal nature; therefore, the Commission considers that Article 17 of Directive 2019/790 remains "unaffected; i.e. DSA rules on limited liability, notice and action, redress and out of court mechanism [are] not applicable for [online content sharing services platforms]."; quoted after Joao Quintais/Sebastian Felix Schwemer, 'The Interplay between the Digital Servicers Act and Sector Regulation: How Special is Copyright?' SSRN (May 7 2021) <https://privpapers.ssrn.com/sol3/papers.cfm?abstract_id=3841606> accessed 20 August 2021.

68 Audiovisual Media Services Directive (n 8).

69 Recital 9 continues: "However, the rules of this Regulation apply in respect of issues that are not or not fully addressed by those other acts as well as issues on which those other acts leave Member States the possibility of adopting certain measures at national level"; see also: Commission, 'Explanatory Memorandum' (n 1) COM(2020) 825 final, 4.

70 cf Art. 1 lit. b) of the Audiovisual Media Services Directive (n 8).

child sexual abuse materials, and racism and xenophobia.[71] Article 28b(3) establishes some general principles Member States have to abide by in determining the appropriate measures (e.g. nature of the content and the harm it may cause, the persons to be protected, the legitimate interests at stake, as well as the general public interest), but also specific requirements, such as a transparent and user-friendly mechanism for users to report content, age verification systems, content rating systems for users, parental control systems, as well as a complaint handling mechanism in relation to all of these points. For the implementation of these measures, Member States shall encourage the use of co-regulation and ensure that out-of-court redress mechanisms are available for the settlement of disputes between users and video-sharing platform providers. These provisions are detailed and comprehensive mandates for the transposition by Member States into national law. The measures are aligned with the objects of the directive (e.g. protection of minors) as well as the specific content available on video-sharing platforms. Accordingly, these are not "issues that are not or not fully addressed" by Directive 2018/1808 or "which are left to the Member States" within the meaning of recital 9 of the DSA. Rather, the provisions in Article 28b of the AVMSD in some parts go beyond those in the DSA and therefore take precedence.

24 Regulation (EU) 2019/1150 (the P2B-Regulation) prescribes for "online intermediation services" its own internal complaint-handling mechanism (Article 11) and a mediation process that differs significantly from the ADR provisions in Article 18 DSA. Article 1(5)(g) DSA provides that the DSA is without prejudice to this regulation; in the Explanatory Memorandum, the European Commission again explains that in ensuring "appropriate transparency, fairness and effective redress possibilities, [Regulation (EU) 2019/1150] will apply as *lex specialis*."[72] There is considerable overlap between the DSA and the P2B-Regulation: platforms like eBay or Amazon are online intermediation services and online platforms within the meaning of the DSA. YouTube is an online platform and – e.g. regarding films offered on the platform against payment – an online intermediation service. Moreover, as recital 13 specifically lists online marketplaces as an example for online platforms, the comments and ratings segments on those platforms may not qualify as a "purely ancillary feature", so as to exempt it from the online platform provisions of the DSA.

25 Accordingly, copyright infringements are largely—at least for online content-sharing service providers—outside the scope of application of the DSA and there is a strong argument that Articles 17 and 18 DSA do not apply to video-sharing platform providers concerning user-generated videos[73] (and audio-visual commercial communications) in relation to the content defined in Article 28b of Directive 2018/1808. With further carve-outs following from the P2B-Regulation, it is unclear what will remain for the redress mechanism in the DSA. More importantly, however, this patchwork quilt of overlapping regulation is creating legal uncertainty for both providers and internet users.

2. Ambiguities with regard to the scope of application of the out-of-court settlement mechanism

26 The scope of application of Article 18 is further burdened with ambiguities. Other than the AVMSD, the DSA does not specify what content it considers "illegal",[74] but makes a horizontal reference to non-

71 According to that provision Member States shall ensure that videosharing platform providers under their jurisdiction take appropriate measures to protect: (a) minors from programmes, user-generated videos and audiovisual commercial communications which may impair their physical, mental or moral development in accordance with Article 6a(1); (b) the general public from programmes, user-generated videos and audiovisual commercial communications containing incitement to violence or hatred directed against a group of persons or a member of a group based on any of the grounds referred to in Article 21 of the Charter; (c) the general public from programmes, user-generated videos and audiovisual commercial communications containing content the dissemination of which constitutes an activity which is a criminal offence under Union law, namely public provocation to commit a terrorist offence as set out in Article 5 of Directive (EU) 2017/541, offences concerning child pornography as set out in Article 5(4) of Directive 2011/93/EU of the European Parliament and of the Council (*) and offences concerning racism and xenophobia as set out in Article 1 of Framework Decision 2008/913/JHA.

72 Commission, 'Explanatory Memorandum' (n 1) COM(2020) 825 final, p 4.

73 Directive (EU) 2018/1808 clearly spells out that measures shall be taken concerning "programmes, user-generated videos and audiovisual commercial communications"; the German Network Enforcement Act – in its latest amendment – carves out content that is not user-generated videos or broadcasts from the Directives application, i.e. video descriptions and comments. This seems an odd differentiation, also given the fact that comments and descriptions usually do not exist independent of the content (e.g. a user-generated video) to which they refer.

74 Article 28b of Directive 2018/1808 names the protection of minors from content which may impair their physical, mental or moral development in accordance with Article

compliance with Union or Member State law. In addition to the corpus of Union law, this broad definition demands online platforms to comply with the legal requirements of all 27 Member States, which especially in the area of free speech vary considerably.[75] The DSA does not give any guidance on the criteria to be applied when examining the alleged illegality of the content in question, it does not specify the intensity with which the question of illegality must be measured, nor how to proceed within a spectrum of justifiable decisions if at all. Not only do platform operators bear a considerable decision-making risk here, it also remains unclear how the out-of-court dispute settlement bodies will tackle this highly contextual and complex range of issues. With different legal systems and traditions in the different Member States with regard to speech issues, this does not resonate well with the legislator's express aim of the "approximation of national regulatory measures at Union level concerning the requirements for providers of intermediary services is necessary in order to avoid and put an end to fragmentation of the internal market and to ensure legal certainty".[76]

27 Moreover, Article 18 allows the recipient of the service "to select any out-of-court dispute" certified in accordance with Article 18(2) with no restriction on the Member State in which such body is certified. There is also no restriction on whether the recipient may select multiple bodies in different Member States. It is an odd consequence of this provision, that a recipient whose content has been removed or disabled in one Member State under the (defamation) laws of that state may turn to an out-of-court settlement body in another Member State. It appears out-right absurd that this body may then decide—possibly with binding effect for the service provider—that removed content that violates the defamation laws of that Member State must be reinstated.

28 A further ambiguity is created with regard to the country-of-origin principle, which is a key principle of the e-Commerce Directive and confirmed and extended in the AVMSD.[77] This principle is meant to avoid that providers of intermediary services established in a Member State have to comply with all Member States' rules. Recital 33 of the DSA provides for an exception to this principle. It shall not apply "to orders to act against illegal content" by a Member State addressed to intermediaries not established within that Member State where such orders "relate to specific items of illegal content". While Article 8 DSA lays down the welcome clarification which conditions an "order to act against illegal content" by a relevant national judicial or administrative authority must fulfil, the DSA fails to explain the relationship of orders under this Article 8 and its specific conditions to the "remnants" of the former provisions of the e-Commerce Directive which found entry into the new intermediary privileges in Articles 3(3), 4(2), and 5(4) DSA. According to these paragraphs, the respective liability privilege "shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement". In the case law in Germany, these paragraphs are the hinges upon which the civil law claims to cease and desist are hung,[78] claims which under this case law need not fulfil the specific requirements of Article 8. Based on this interpretation, different out-of-court settlement bodies may apply the laws of different Member States to the same set of facts which may lead to a race to the bottom to that body providing the most beneficial outcome for the recipient of the service.

29 Since Article 8 DSA appears to be the more specific rule, it will have to be considered *lex specialis* to Articles 3(3), 4(2) and 5(4) DSA. However, in newly formulated legislative acts it would be desirable to avoid such ambiguities, which are being put into effect already in the legal discussion in Germany, where some voices want to read the "order" in recital 33 to also extend to civil law claims to cease and desist.[79]

6a(1), the protection of the general public from content containing incitement to violence or hatred directed against a group of persons or a member of a group based on any of the grounds referred to in Article 21 of the Charter, or the dissemination of which constitutes an activity which is a criminal offence under Union law, namely public provocation to commit a terrorist offence as set out in Article 5 of Directive (EU) 2017/541, offences concerning child pornography as set out in Article 5(4) of Directive 2011/93/EU of the European Parliament and of the Council (*) and offences concerning racism and xenophobia as set out in Article 1 of Framework Decision 2008/913/JHA.

75 See for instance the specific prohibitions in Germany on the denial of the holocaust in § 130 StGB (German Criminal Code).

76 cf Recital 4 DSA.

77 Article 28a of Directive 2018/1808 extends the country-of-origin principle to video-sharing platform services "deemed to be established in a Member State".

78 BGH GRUR 2018, 1132 para 47; Case C-484/14 *Tobias Mc Fadden v Sony Music Entertainment Germany GmbH* (CJEU, 15 September 2016).

79 Bernd Holznagel, 'Chapter II des Vorschlags der EU-Kommission für einen Digital Services Act' [2021] CR 123; Gerald

3. The extension to decisions based on the providers' terms and conditions

30 It is not a small matter which lies behind the words "incompatible with the terms and conditions of the provider" in Article 17(1) DSA, as this applies the obligations under Articles 15, 17, and 18 DSA not only to decisions on the *illegality* of the content, but also to such decisions based on a non-compliance with the platform operators' terms and conditions. With this extension to decisions based on contractual relationships, the Commission takes account of the assumption that the freedom of opinion and information may be significantly influenced by online platforms and who should therefore not be free in their decision to remove content from the platform or the blocking of accounts. While recital 38 DSA acknowledges that "the freedom of contract of providers of intermediary services should in principle be respected", it was "appropriate to set certain rules on the content, application and enforcement of the terms and conditions of those providers in the interests of transparency, the protection of recipients of the service and the avoidance of unfair or arbitrary outcomes".[80] In its Impact Assessment, the Commission emphasizes that the removal of content "can have severe consequences on the rights and freedoms of their users", in particular their freedom of expression. The report continues: "These decisions are often not based on an assessment of the legality of the content, nor are they accompanied by appropriate safeguards, including justifications for the removal or access to complaints mechanisms, but they are solely governed by the discretionary powers of the platform according to the terms of services that are part of their contractual terms."[81]

31 Removal decisions based on violations of the terms and conditions of the provider concern a wide range of decisions from spam, deceptive practices, to graphic, violent, pornographic or abusive content and hate speech, etc.[82] Not only are the reasons for such removals manifold, the removal numbers illustrate the diseconomies of scale associated with their inclusion for an out-of-court settlement mechanism: Facebook took action on more than 95 million pieces of content for hate speech and approximately 130 million for adult nudity and sexual activity[83], and YouTube removed in 2020 more than 200 million videos and 4.9 billion of comments posted by its users for community guidelines violations.[84] An obligation on the platform operator to further "administer" and impose procedures on this swift, intuitive and efficient process with requirements to provide "clear and specific statements of reasons" (Article 15 and the detailed requirements in paragraph 2 lit a) through f)), demands for a formalized complaint-handling system with further reporting obligations (Article 17) and finally an out-of-court settlement process (Article 18) will likely render the entire system unfeasible. As a consequence, systems currently working extremely effectively will lose their power to efficiently prevent misuse of the service, and the DSA will do a disservice to its own goals.

D. The Out-of-court redress in Article 18 DSA misses its objective, it encroaches the fundamental rights of the online platforms and frustrates their effective own initiatives

32 With its proposal, the Commission intends "to ensure harmonised conditions for innovative cross-border services to develop in the Union"; the DSA was necessary "to ensure effective harmonisation across the Union and avoid legal fragmentation".[85] Besides the requirements of the stated legal basis of

Spindler, 'Der Vorschlag für ein neues Haftungsregime für Internetprovider – der EU-Digital Services Act (Teil 1)' [2021] GRUR 545.

80 It remains unclear whether and how these provisions of the DSA can influence the contractual relationship between the platform and its users, which remains at the disposal of the parties. It is therefore likely that the obligations and regulatory instruments will rather be enforced by the competent authorities in accordance with the provisions of Chapter IV of the draft DSA. It is further unclear, whether and on what basis violations of these obligations by the platform give rise to civil law claims by the users; doubtful as here also Spindler (n 63) 654, who assumes that enforcement will occur as public law enforcement.

81 Commission, Impact Assessment, COM(2020) 825 final, para 51.

82 cf the community guidelines of YouTube at <https://www.youtube.com/intl/ALL_en/howyoutubeworks/policies/community-guidelines/>, the Twitter Rules at <https://help.twitter.com/en/rules-and-policies/twitter-rules>.

83 cf Facebook Transparency Center, https://transparency.fb.com/data/community-standards-enforcement/hate-speech/facebook.

84 cf Google Transparency Report, YouTube Community Guidelines enforcement, available at <https://transparencyreport.google.com/youtube-policy/removals?hl=en>.

85 Commission, 'Explanatory Memorandum' (n 1) COM(2020) 825 final, 3, 5.

the DSA (Article 114 TFEU)[86], the provisions in Article 18 DSA—viewed from the perspective of the platform operator—must also meet the conditions of Article 52 of the Charter.[87] According to that article, limitations on the exercise of the rights and freedoms recognised by the Charter must be provided for by law and respect the essence of those rights and freedoms; they are further subject to the principle of proportionality and may only be made if necessary to meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others. The relevant freedoms of the platform operators in this regard follow from the freedom to conduct a business in Article 16 and right to an effective remedy and a fair trial in Article 47 of the Charter.

33 The out-of-court redress in Article 18 DSA misses its objective, as it promotes fragmentation rather than approximation (D.I.). It does not recognize the platform operators' freedom of contract as an outflow from Article 16 of the Charter (D.II.). The proposed out-of-court redress is in violation of the right to an effective remedy and to a fair trial in Article 47 of the Charter (D.III.), and it frustrates voluntary own-initiative investigations by the platform in violation of the principle of proportionality (D.IV.).

I. Fragmentation instead of approximation

34 Already on the Union level, the DSA is not approximating different regulation, but rather promotes fragmentation and creates legal uncertainty with regard to its scope of application.[88] Different rules and procedures for video-sharing platforms, for online content-sharing platforms, for online intermediation services, for online platforms, and for different areas of law leave a scattered landscape for providers whose services may fall within more than one of these definitions. The same service may therefore be subject to different regulations with regard to alternative redress possibilities, increasing the demands on the operator, who will have to establish and allocate separate resources, systems and workflows for different redress mechanisms to meet their requirements.

35 "On the merits" the DSA does not even attempt to harmonize regulation at Union level,[89] but subjects online platforms to the requirements of the laws in all 27 Member States, "irrespective of the precise subject matter or nature of that law", with further uncertainties resulting from exceptions to the country-of-origin principle.[90] An approximation does not lie in uniform procedural regulatory requirements, as the Commission fails to recognize the effects of its content moderation rules. The uploader whose content has been removed or account blocked may select any certified body for an out-of-court dispute settlement in any Member State. Furthermore, the DSA does not provide any guidance for which criteria and which standard the redress body shall apply in examining the alleged illegality of the content in question. Especially in the area of free speech, the legal assessment as to whether content is lawful is highly contextual and subject to complex factual and legal determinations and the balancing of conflicting fundamental rights. And this assessment and balancing become even more complex with the "addition" of an intermediary service to the equation.[91] Without standards and guidance for this assessment, the quality of the decision making process and the decision will likely vary significantly from body to body and Member State to Member State, resulting in a patchwork "case-law" of deviating decisions and a classic race-to-the-bottom with all the wrong incentives; the uploader whose content is removed will turn to the certified body that is likely to grant their claim. As a consequence, we will see bodies in certain Member States decide more uploader-friendly

86 Critical of Article 114 TFEU as a suitable basis: Jörg Ukrow, 'Die Vorschläge der EU-Kommission für einen Digital Services Act und einen Digital Markets Act' Institute of European Media Law, 8 et seq <https://emr-sb.de/wp-content/uploads/2021/01/Impulse-aus-dem-EMR_DMA-und-DSA.pdf> accessed 20 August 2021.

87 Case C-401/19 *Republic of Poland v European Parliament, Council of the European Union* (Opinion of AG Saugmandsgaard-Øe, 15 July 2021), para 88 et seq.

88 See above III.3.a).

89 In criticising the effects of subjecting service providers to the legal systems of all 27 Member States, Nettesheim, suggests a harmonization: "The emergence of a common European area of fundamental rights, shaped by the ECHR and the European Charter of Fundamental Rights (CFR), makes it possible today to harmonize the basic principles of what must be permitted on (very large) online platforms and what can or should be prohibited under European Union law"; Martin Nettesheim, 'Die unionsrechtliche Regulierung großer Internet-Plattformen: Die Kommissionsentwürfe für einen Digital Markets Act und einen Digital Services Act' Bundestagsdrucksache 19(21)136) <https://uni-tuebingen.de/fakultaeten/juristische-fakultaet/lehrstuehle-und-personen/lehrstuehle/lehrstuehle-oeffentliches-recht/nettesheim/> accessed 20 August 2021.

90 See above III.3.b).

91 See above II. and *Magyar Tartalomszolgáltatók v Hungary* App no. 22947/13 (ECtHR, 2 February 2016), para 68 et seq.

than in others and we will see bodies that may differ in their findings on speech along different political, social and/or religious beliefs. The result of Article 18 DSA is more fragmentation, not less.

II. The parties' freedom of contract is not sufficiently regarded in the proposed complaint and redress mechanism

36 Platform operators can rely on the freedom to conduct a business guaranteed in Article 16 of the Charter, which protects them, in principle, from obligations which may have a significant impact on their activity.[92] This paper will not discuss in this respect the significant measures required by the online platforms to adapt workflows, dedicate resources and invest in systems, but wants to put the focus on another concern with regard to the rights from Article 16 of the Charter, resulting from the extension of the DSA's content moderation measures to removals based on community guidelines' violations.

37 The freedom of contract is an essential element of the protection granted by Article 16 of the Charter in the jurisdiction of the CJEU. The scope of protection of the freedom of contract of companies implies the free choice of the contractual partner and the design and amendment of the content of the contract.[93] The Commission acknowledges the importance of this freedom in recital 38, but considers regulation appropriate for the avoidance of "unfair or arbitrary outcomes". This is grounded in the Commission's assumption that decisions by the platform operator on the basis of their terms and conditions may be arbitrary and untransparent and consequently oppress legal speech. This somewhat sweeping assumption requires a closer examination in law and fact.

1. The online platforms must have discretion in their decision to remove content

38 According to the Explanatory Memorandum, the DSA "seeks to foster responsible and diligent behaviour by providers of intermediary services to ensure a safe online environment, which allows Union citizens and other parties to freely exercise their fundamental rights, in particular the freedom of expression and information".[94]

39 Somewhat neglected in the current debate on the perceived influence and a consequential responsibility of online platforms with regard to the freedom of expression is that the fundamental rights of the Charter are addressed to the institutions and bodies of the Union.[95] Also, the case law of the ECtHR that is sometimes referred to in this discussion when pointing out the importance of online platforms for the exercise of free speech on the Internet concern cases where it was a judicial or administrative authority of a treaty state to the Convention that encroached a citizen's rights from Article 10 ECHR.[96] In this relationship—i.e. citizen v. state—the fundamental rights and especially the freedom of expression apply directly and fully. However, the freedoms of the Convention, in general, do not apply horizontally between private persons.[97] Regarding the Charter it is equally doubtful, whether the fundamental freedoms granted under its articles have effect in determining or resolving relationships between private parties.[98] An argument against

92 cf 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 (C-683/18)* (Opinion of Advocate General Saugmandsgaard-Øe, 16 July 2020), para 240; see also Case C-360/10 *SABAM v Netlog* (CJEU, 16 February 2012), para 44 et seq; Case C-70/10 *Scarlet Extended/SABAM* (CJEU, 24 November 2011), para 46 et seq.

93 cf Case C-240/97 *Spain v Commission* (CJEU, 5 October 1999), para 99; case C-426/11 *Mark Alemo-Herron* (CJEU, 18 July 2013), para 32; Case C-283/11 *Sky Austria* (CJEU, 22.1.2013), para 42 et seq; Case C-277/16 *Polkomtel* (CJEU, 20 December 2017), para 50.

94 Commission, 'Explanatory Memorandum' (n 1) COM(2020) 825 final, p 6.

95 Article 51 of the Charter; the Member States are bound when they are implementing Union law.

96 *Cengiz at al. v Turkey* App nos. 48226/10 and 14027/11 (ECtHR, 1 December 2015), para 52; *Times Newspapers Ltd. v United Kingdom* App nos. 3002/03 and 23676/02 (ECtHr, 10 March 2009), para 27; *Delfi AS v Estonia* App no. 64569/09 (ECtHR, 16 June 2015), para 110.

97 See also Eifert/Metzger/Schweitzer/Wagner (n 58) 27.

98 There are some decisions by the ECtHR and the CJEU which can be interpreted as applying the freedoms of the Charter or the Convention respectively also between private parties. However, these cases concerned the effect of Article 10 of the Convention in the workplace and the relationship between employee and employer, where the state had a positive obligation to protect the right to freedom of expression even in the sphere of relations between individuals; cf. e.g. *Heinisch v Federal Republic of Germany* App no 28274/08 (ECtHR, 21 July 2011) with further references. In the debate in Germany, where the doctrine of

binding private parties to the freedoms of the Charter is that it does not appear to be fundamentally necessary in order to realize the internal market. Moreover, propagating such binding effect may disregard the wilful decisions of private individuals as expression of their autonomy.[99] With regard to social networks, the Federal Constitutional Court of Germany has held in a recent temporary restraining order decision that it has not yet been conclusively clarified either in the case law of the civil courts or in the case law of the Federal Constitutional Court, whether and, if so, which legal requirements may arise in this respect for operators of "social networks on the Internet"; the constitutional legal relationships are still unresolved in this respect.[100] This contribution cannot dive into the details of this complicated and far-reaching legal issue. But for the purposes of this paper it may suffice to say that it is too short-sighted to simply apply the same standard of protection of the freedom of expression and information vis-á-vis state authorities also to relationships between private parties in the private marketplace.

40 The boundaries of lawful free speech in their function as a defensive right against encroachments by legislative, administrative or judicial authorities are very wide.[101] Private companies cannot be held to this same standard. If this standard were to be read into the provisions of Articles 15, 17, and 18 DSA, those provisions would leave almost no leeway for providers to give their commercially operated network a certain orientation in order to gear it towards target groups, or to create respectful interactions within its "community", or to minimise a liability risk due to the dissemination of possibly illegal content.

41 The use of online services by the individual user is foremost subject to contractual agreements laid down in the providers' general terms and conditions and agreed to by the user during the registration process. In these terms and conditions, online platforms usually reserve the right to remove content that is in conflict with these agreed rules/guidelines. These guidelines may stipulate that the platform is dedicated to a specific subject matter or purpose and declare content outside this subject matter not permissible (e.g. a social network dedicated to a certain type of sport or pastime); they may formulate rules on how to behave and interact on the platform ("netiquette") or stipulate that certain content is generally not permissible, even though such content may not be illegal (e.g. certain types of nudity).[102] The content and purpose of such "house rules" may be manifold and as such are protected by the service provider's contractual freedom under Article 16 of the Charter. It is also within the scope of protection granted by Article 16 of the Charter that private companies take measures to protect them against legal risks, including the avoidance of litigation. It is therefore not only in the interest, but also protected under Article 16 of the Charter for online platforms to reserve in these guidelines (or their interpretation) a corridor of discretion that keeps a "safe distance" to the illegality. In carrying out this balancing of conflicting fundamental rights, the German Federal Court of Justice (BGH) in its recent Facebook de-

"mittelbarer Drittwirkung" [indirect third party effect] is well-established by the Federal Constitutional Court, such indirect effect is sometimes also afforded to the freedoms of the Charter; cf Jarass, Charta der Grundrechte, Art. 51 para 30 et seq; Schwerdtfeger in Meyer/Hölscheidt, Charta der Grundrechte der Europäischen Union, Art. 51 para 57 et seq.

99 cf Forsthoff in Grabitz, Hilf, Nettesheim, Das Recht der Europäischen Union, Art. 45 AEUV para. 165.

100 BVerfG NJW 2019, 1935; available at <https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2019/05/qk20190522_1bvq004219.html> with an abstract in English.

101 For German constitutional law, this follows instructively from a decision by the Federal Constitutional Court (BVerfG NJW 2010, 47, para 54): "The possible confrontation with disquieting opinions, even if in their conceptual consequence they are dangerous, and even if they aim at a fundamental transformation of the valid order, is part of the state based on freedom. Protection against an impairment of the "general feeling of peace" or the "poisoning of the intellectual atmosphere" constitute no more reason for an encroachment than does the protection of the population against an insult to their sense of right and wrong by totalitarian ideologies or an evidently false interpretation of history. Neither does the goal of establishing human rights in the legal awareness of the population permit the suppression of contrary views. Instead, the constitution trusts that society can cope with criticism, and even polemics, in this regard, and that they will be countered in a spirit of civil commitment, and that finally citizens will exercise their freedom by refusing to follow such views. By contrast, the recognition of public peace as a limit of what is acceptable as against unacceptable ideas solely because of the opinion as such would disable the principle of freedom, which itself is guaranteed in Article 5.1 of the Basic Law." Decision available in English at <https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2009/11/rs20091104_1bvr215008en.html> accessed 20 August 2021.

102 cf the community guidelines of YouTube: 'YouTube Guidelines' <https://www.youtube.com/intl/ALL_en/howyoutubeworks/policies/community-guidelines/> accessed 20 August 2021, the Twitter Rules: 'Twitter Rules' <https://help.twitter.com/en/rules-and-policies/twitter-rules> accessed 20 August 2021.

cisions came to the conclusion, that the social network is in principle entitled to require its users to comply with certain communication standards that go beyond the requirements of criminal law (e.g. insult, defamation or incitement of the people). In particular, it may reserve the right to remove posts and block the user account in question in the event of a breach of the communication standards.[103]

42 Even if one were to assume that the fundamental rights of the Charter can also be effective in disputes between private parties by way of indirect (third-party) effect,[104] this would not lead to a "must-carry"-obligation for the online platform. While under such a regime it could be argued, that the service provider, especially where the platform is of a general nature and not limited to a specific subject matter or purpose, may not be entitled to reserve the right to arbitrarily decide on the removal of content, there must be room for service providers to remove content which otherwise may not be illegal in accordance with its house rules. However, a platform operator cannot be obliged to allow any content on the platform, if such content only complies with the limitations of Article 11 of the Charter. While the fundamental rights of the uploader may influence his relationship with the online platform, such effect is indirect, and must recognize and bring to effect the fundamental rights of both parties. To this end, the service providers' right under Article 16 of the Charter must be recognized to not only devise its house rules, in order for its users to be able to use the platform free of any hostility and disrespectful behaviour, but also to protect its interest by reducing the risk of exposure to legal enforcement or fines. In particular, as much of what is repulsive, indecent and distasteful under any consideration—such as racist and other hateful content in particular—may (still) be covered by the freedom of expression under Article 11 of the Charter, the service provider must be able—in balancing the various interests and rights—to keep such content from the platform, as long as the terms of use providing for such rights are transparent and not arbitrary.

2. No guidelines as to expertise, standards for the out-of-court settlement body's decision

43 The DSA gives no guidelines at all on the standard the certified out-of-court settlement bodies shall apply in finding their decision. Article 18(2) DSA only requires generally, that such body has demonstrated "the necessary expertise in relation to the issues arising in one or more particular areas of illegal content". It is not clear, what "necessary expertise" means. Directive 2013/11/EU on ADR for consumer disputes made such necessary expertise, knowledge and skills a requirement, "as well as a general understanding of the law". Can one draw from this the reverse conclusion that knowledge of the law (not even a general understanding) is not required under the DSA? The settlement shall take place in accordance "with clear and fair rules of procedure", without specifying what this means in detail. This, in itself, is a violation of Article 52 of the Charter, which not only requires that any limitation on the exercise of right protected by the Charter must be provided for by law, but also that the legal basis must be sufficiently clear and precise.[105]

44 The determination of whether the removal of content[106] uploaded by a third person violates this person's freedom of expression, or more precisely, whether such removal decision is "lawful" in the context of balancing fundamental rights or in the application of contractual terms between the parties, is fully rights-based. It is not a question of finding a consensual compromise in commercial relationships that helps both parties by finding a swift and reasonable resolution.[107] As explained above, this is an entirely normative decision, which includes at its core the balancing of conflicting fundamental rights. There is no room for give and take. Such decision must naturally be reserved to judges or other legal professionals who possess a keen understanding of the law and operate on the basis of fundamental

103 This is the wording used in the press release by the BGH concerning these judgments; to be confirmed once the full-text judgment is available; cf <https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/DE/2021/2021149.html>. Facebook was nevertheless ordered to reinstate the removed content in these decisions as its terms and conditions did not obligate Facebook to inform the uploader at least afterwards that his content was removed and beforehand in case of account suspensions.

104 cf the principles established by the Federal Constitutional Court of Germany on the so-called *Drittwirkung*, BVerfG GRUR 2020, 35, para 76; with references to the established case law; available in English at <https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2019/11/rs20191106_1bvr001613en.html> accessed 20 August 2021.

105 cf Case C-419/14 *WebMindLicenses Kft.* (CJEU, 17 December 2015), para 81.

106 Or the decision to suspend or terminate in whole or in part the provision of the service to the recipient, or to suspend or terminate the recipient's account respectively.

107 Critical already regarding out-of-court settlement by private bodies in the area of consumer rights enforcement Eidenmüller/Engel (n 2) 261.

due process principles.[108] How would a private body assess and decide on these issues? What standard would it apply? How are the requirements of due process met? Who would be heard? And how would such body investigate and establish the facts relevant to the content, and its context, as the assessment as to whether certain content on the Internet is illegal is often highly contextual and therefore complex? How and on the basis of what standards would such private organization apply the terms of service of the online platforms and decide on the issue of whether fundamental rights have effect on the contractual relationship between the online platform and its users? Neither does the DSA answer these pertinent questions nor are they discussed in the Explanatory Memorandum or the Impact Assessment. This is all the more surprising in light of the long catalogue of decisions by both the ECtHR and the CJEU on the balancing of the freedom of expression, which constitutes one of the essential foundations of a democratic society and one of the basic conditions for its progress and for each individual's self-fulfilment[109], and particularly the right to protection of reputation as protected by Article 8 of the Convention as part of the right to respect for private life. The ECtHR has repeatedly emphasized that, as a matter of principle, the rights guaranteed under Articles 8 and 10 deserve equal respect and has established a set of principles for this particular balancing.[110]

III. The out-of-court dispute settlement mechanism in Article 18 DSA is a violation of the right to an effective remedy and to a fair trial in Article 47 of the Charter

45 The out-of-court dispute settlement mechanism of Article 18 DSA encroaches upon the online platform's rights from Article 47 of the Charter.

1. The out-of-court settlement body's binding decision violates the online platform's rights from Article 47 of the Charter

46 While the online platform "shall engage in good faith" with the out-of-court settlement body selected by the uploader, it "shall be bound by the decision taken by the body" (Article 18(1) DSA). Conversely, such decision is without prejudice to the uploader's right to redress the decision before a court of law. As Article 18(1) 44 DSA only mentions "the recipient" for such redress, online platforms may not have such right.[111] Besides the ambiguity of the quoted language, a binding effect of the out-of-court settlement body's decision on the online platform is an obvious violation of the platform's rights from Article 47 of the Charter.

47 A fundamental principle of justice in dispute systems design is unconditional access to justice.[112] The Commission addressed this aspect of Article 47 of the Charter only with regard to the "recipient of the service". Presumably, the Commission envisages the uploader vis-á-vis the online platform in a weak position and therefore did not want to deprive it of any possibility to pursue its claims. The proposal fails to recognize, however, the serious effects a binding decision by the out-of-court settlement body would have on the fundamental rights of the online platform, as this would effectively establish a "must carry"-obligation on the part of the platform, imposed on the platform by a private organization, and without any possibility of redress.

48 In accordance with these requirements of Article 47 of the Charter, the "predecessors" of the DSA in devising ADR and ODR mechanisms have followed a different path. Directive 2013/11/EU on alternative dispute resolution for consumer disputes spells out in recital 45 that "this Directive should not prevent parties from exercising their right of access to the judicial system." Similarly, the AVMSD as amended by Directive (EU) 2018/1808 states in recital 50: "The right to an effective remedy and the right to a fair trial are fundamental rights laid down in Article 47 of the Charter. The provisions of Directive 2010/13/EU should not, therefore, be construed in a way that would prevent parties from exercising their right of access to the judicial system."[113] It

108 Regarding consumer rights cf. Eidenmüller/Engel (n 2) 288 et seq.

109 *Magyar Tartalomszolgáltatók v Hungary* App no. 22947/13 (ECtHR, 2 February 2016), para 54; *Delfi AS v Estonia* App no 64659/09 (ECtHR, 10 October 2013), para. 78; each with further references.

110 *Magyar Tartalomszolgáltatók v Hungary* App no. 22947/13 (ECtHR, 2 February 2016), para 60 et seq.

111 Daniel Holznagel, 'The Digital Services Act wants you to "sue" Facebook over content decisions in private de facto courts' (verfassungsblog.de, 24 June 2021) <https://verfassungsblog.de/dsa-art-18/> accessed 20 August 2021.

112 Eidenmüller/Engel (n 2) 282.

113 See also the almost identical language in recital 26 of

is not comprehensible, why the Commission opts for its one-sided solution, especially in this field of law, which necessarily involves fundamental rights in all four corners of this particularly multipolar constellation of communication.[114]

2. The transfer of original tasks of the judiciary to private entities

49 Out-of-court dispute settlement mechanisms usually aim at a consensual dispute settlement, placing emphasis on interests rather than on the legal positions of the parties or on the rights asserted.[115] The suitable disputes for such ADR/ODR systems are those that are concerned with the entitlement to material benefits rather than those concerned with fundamental rights.[116] Alternatively, where a rights-based analysis involving fundamental rights is at the core of a dispute, it is the original task of the public courts under Article 47 of the Charter to provide and enforce solutions. Particularly in the legally sophisticated field of free speech it does not appear possible to leave the solution of disputes to non-legal private providers, which may not be trained or incentivized for this task and which operate outside the procedural safeguards of the court system.[117]

50 Moreover, the transfer of such normative decisions to private bodies gives rise to a load of further problems: (1) the out-of-court settlement bodies certified under Article 18(2) DSA need to be sufficiently funded to be able to operate, (2) where such funding shall come from is not provided for in the draft DSA, (3) there is an incentive for out-of-court settlement bodies to try to attract as many settlement proceedings as possible, and (4) in pursuit of that goal, a consequential incentive to tend to decide in favour of the applying uploader. Where conflicts are shifted to private service providers who have an incentive to follow the applicants' interests, efficiency may be put above judicial scrutiny and the observance of due process standards.[118]

51 There are no specific arrangements for the oversight of such out-of-court settlement bodies and the experience with this aspect under Directive 2013/11/EU does not seem very positive.[119] As a consequence, there are also doubts as to the quality of the decision making bodies and the resulting quality of their decisions.[120] Moreover, as uploaders may select any certified out-of-court settlement body there will likely be a diversity of quality standards across the EU. This situation is likely to create a risk of out-of-court settlement body shopping, leading to a race to the bottom.[121]

52 As the decisions to be rendered by the out-of-court settlement bodies are by their nature normative and rights-based, it follows that the qualifications of persons that are entrusted with such decisions must be competent to administer these processes. Clearly, and especially in this highly complex field, this can only be carried out by trained lawyers, who are familiar not only with the applicable Union and national laws but also with the book(s) of relevant case law. If—as in the present context—the goal of the process is rights enforcement, only legal professionals are in a position to do justice to this goal.[122] This is not reflected in the DSA.

IV. No proportionality/contradiction with good-Samaritan principle in Art. 6

53 The inclusion of removal decisions based on violations of the providers' terms and conditions, is not meeting the requirement of the principle of proportionality within the meaning of Article 52(1) of the Charter. The flagging systems as they have been established by all leading online platforms in order to enforce their community guidelines are swift and efficient, and they widely used by registered users of the respective platforms.[123] The success of these systems is due to their simplicity, their easy accessibility and their fast decision making by using formalized complaints and electronic means. Requiring online platforms to submit—besides

Regulation (EU) No 524/2013 on online dispute resolution for consumer disputes.

114 See above II.

115 Eidenmüller/Engel (n 2) 273.

116 cf Pablo Cortes, 'Online Dispute Resolution for Consumers in the European Union' (Rutledge 2011), 3 et seq.

117 cf Eidenmüller/Engel (n 2) 283.

118 Eidenmüller/Engel (n 2) 263.

119 Biard (n 5) 113; Eidenmüller/Engel (n 2) 289.

120 Holznagel (n 108).

121 Biard (n 5) 113.

122 Eidenmüller/Engel (n 104) 263.

123 See above II.

extensive reporting and an internal complaint-handling mechanism—to an out-of-court dispute settlement regarding only a small fraction of these billions of removal decisions[124], is obviously out of proportion.

54 Such requirement may very well become its own source of disputes, when being abused by complaining uploaders.[125] This is not a theoretical issue especially in the area of hate speech. There are studies confirming the suspicion that in the field of hate speech, there are few originators responsible for a very high proportion of hate speech content, and that these users often comment qualitatively differently than "normal" users. The study "Hass auf Knopfdruck" ("hate at the push of a button") of the Institute for Strategic Dialogue (ISD) has mapped the rise and nature of far-right hate speech in Germany. It combines quantitative data-analysis from Facebook comment sections with insights gained from ethnographic research in far-right chat groups. The study found: "Hate speech among media articles on the major German-language news sites on Facebook is produced, 'pushed' and distributed by a small group of accounts - measured by the number of all users. The distribution is often coordinated in terms of content and time."[126] Not only will these convinced perpetrators not be deterred from posting blocked content again; they will likely take any opportunity to confront and attack people with deviating opinions and thus instrumentalise content moderation procedures for their purposes. The out-of-court dispute settlement mechanism in Article 18 DSA provides such an opportunity without a cost-risk and—combined with the incentives for out-of-court settlement bodies to decide "complaint-friendly"—creates a risk that content is re-uploaded to the platform although its removal was well-founded because the reported content is illegal or violates the terms of service of the provider.

55 Article 6 DSA intends to reward voluntary own-initiative investigations (the so-called "good-Samaritan principle"). The flagging systems voluntarily established by the online platforms can be subsumed under this term. Making these systems subject to the extensive obligations in Article 15, 17 and 18 DSA can cause an online platform to curtail these systems or shut them down entirely. The ECtHR has held regarding the imposition of liability of an internet portal for its third-party comments section: "Such liability may have foreseeable negative consequences on the comment environment of an Internet portal, for example by impelling it to close the commenting space altogether."[127] The interference with these functioning systems would thus run contrary to the principle established in Article 6 DSA.

E. Outlook

56 The DSA, in providing for content moderation and an out-of-court dispute settlement mechanism, intends to empower the uploader and make available to them an easily accessible, swift and effective as well as cost-free redress against decisions by the online platform to remove their content. There is nothing wrong with this intention, but the Commission operates with its proposal on premises which do not or at least not fully hold true. Also, the implementation itself is defective.

57 It is true that the removal of users' content by platforms "can have severe consequences on the rights and freedoms of their users" and that the platforms' decisions are often not based on an assessment of the legality of the content but "according to the terms of services that are part of their contractual terms". Moreover, "in some cases, content can also be removed erroneously, even if it is not illegal, nor in violation of the terms of service" stemming from erroneous reporting by other users, abusive notices, or from platforms' own detection systems, not least when automated tools are used. Despite all these facts, the opting for the redress mechanism as devised in Article 18 DSA is short-sighted and does not match the requirements and risks.[128]

58 Making the decision of the out-of-court settlement body binding upon the online platform is the most obvious mistake of the proposal. Similarly, it does not appear necessary to let legal persons such as businesses or political parties participate in the "privileges" granted by Article 18 DSA. But more importantly there is doubt as to the premise of the Commission that the protection of fundamental rights of the uploaders require an enforcement as regulated in the DSA. Every major online platform has a functioning internal complaint-handling mechanism. As part of these systems, an uploader whose content is removed or access to it disabled,

124 On the numbers see above at n 81 and 82.

125 Ethan Katsh/ Orna Rabinovich-Einy, 'Digital Justice – Technology and the Internet of Disputes' [2017] 117.

126 Institute for Strategic Dialogue (ISD) "Hass auf Knopfdruck - Rechtsextreme Trollfabriken und das Ökosystem koordinierter Hasskampagnen im Netz" (2018); available at <https://www.isdglobal.org/isd-publications/hass-auf-knopfdruck/>.

127 *Magyar Tartalomszolgáltatók v Hungary* App no. 22947/13 (ECtHR, 2 February 2016), para 86.

128 cf Commission, 'Impact Assessment' (n 9), para 51.

or whose account is suspended or terminated, is informed of such decision by the online platform. All major platforms also provide for a possibility to appeal such decision. A reasonable regulation of the requirements of such system is certainly helpful to harmonize standards.

59 An out-of-court dispute settlement process in the form of Article 18, however, is not necessary and even counter-productive to the goals of the DSA. There is already an appeal mechanism for any removal decision by e.g. YouTube, which is used only by a fraction of uploaders, clearing the suspicion of overblocking. The fact that these easily accessible, swift and cost-free appeal mechanisms are rarely used by uploaders whose content have been removed, does not support the need for an out-of-court redress mechanism. In the same vein, there is only a limited number of court cases in Germany by uploaders demanding that their content is being reinstated. In Germany, there is effective legal protection available through the court system, e.g. the possibility of interim injunctions at relatively low cost[129] and the right way to correct legal standards for this assessment. Secondly, experience with this case law shows that the overwhelming number of plaintiffs demanding the reinstatement of their content are political activists from the far-right of the political spectrum, deniers of the current pandemic or certain aspects related to it, or business people operating in the twilight of grey markets. It goes without saying that all these people have a right to be heard with their appeal. But neither the number of cases nor the position of the plaintiffs appear to underscore a need for an additional out-of-court redress mechanism.

60 Establishing systems of out-of-court redress operated by private and competing organizations in all Member States would effectively duplicate a quasi-judicial landscape of ADR providers next to the courts.[130] The transaction costs in regulating these private providers to secure minimum standards will be significant and an inefficient duplication of resources.[131] Moreover, the enforcement of these bodies' decisions remains unclear, their impartiality as well as their oversight questionable.

61 The biggest point of criticism, however, remains that the decision on the lawfulness of content is a normative decision reserved for the judiciary. The benefits of easy access, of swiftness, and decision-making via electronic means cannot outweigh the severe flaws of the envisaged redress mechanism. Instead, it would be much more prudent and efficient to modernize the existing judicial infrastructure in the Member States. This could build on existing elements or by providing for amendments to the existing courts system to address (real or assumed) needs of private persons to effectively pursue their rights. The pandemic has brought experience in online court hearings that could be put to use for the cases in question.[132] Further tools could be the lowering of court and attorney's fees for such proceedings,[133] a more generous handling of legal aid, or the possibility of mandating certain not-for-profit bodies, organisations or associations to bring claims, mandated by a recipient of the service.[134] In light of the possibility for abuse of any such redress mechanism,[135] however, there also should be hurdles to pursue one's rights.[136] One could also think of a right of associations to sue similar to such right granted under German laws against illegal clauses in general terms and conditions. With such right to sue, there would be effective measures of redress against arbitrary clauses in terms of conditions of providers.

129 Court costs as well as attorneys' fees are calculated on the basis of the value of the matter in dispute, which is usually set at EUR 5,000.00; cf. also Holznagel (n 108).

130 Holznagel (n 108) speaks of de facto-courts and questions the Unions respective competence.

131 Eigenmüller/Engel (n 2) 296.

132 § 128a ZPO (German Code of Civil Procedure) allows for oral hearings to take place by means of video and audio transmission, which has been put into effect during the current pandemic.

133 The German copyright act in § 97a provides such cost-reduction in certain proceedings.

134 Such representation is already provided for in Article 68 DSA.

135 See above IV.4.

136 It must also be recognized that online platforms cannot be equated to public broadcasting or to "essential facilities" monopolizing communication on the internet and functioning as a bottleneck to speech. Without going in to any detail on this issue, online platforms – as already the plural indicates – do not monopolize speech on the internet. If someone cannot post his speech on Facebook, he can do so on Reddit or Twitter, etc. He could also post the content on his own website and search engines will provide at least some accessibility.

NFTs And Copyright Quandary

by **Adarsh Vijayakumaran***

Abstract: NFTs have garnered massive investor attention in the last few years. While the technology is still at its nascent stage, the massive price pump for major NFTs such as Dragon kitty, Shatner's digital cards, etc. show that NFTs are going to be with us for a very long time along with other blockchain innovations. The present article focuses on the right to create NFT as part of the statutory bundle of rights provided under the Copyright Act. The article discusses the copyright jurisprudence through historical lenses to exhibit that the copyright law has always been in a state of constant evolution encompassing wide variety of technological innovation on one hand and protecting the rights of the creators on the other. The article addresses questions such as if NFTs can be copyrighted, whether creation of an NFT without authorization amounts to copyright infringement, whether there exists a right to create an NFT among others. Finally, the article concludes the discussion by suggesting various ways in which the NFTs can be availed without the hullaballoo of copyright infringement by introduction of delimitation of rights and liabilities clauses within smart contracts, and by recognizing the right to create NFT as part of the copyright framework.

Keywords: NFTs; Copyright; Tokens; Blockchain

Recommended citation: Adarsh Vijayakumaran, NFTs And Copyright Quandary, 12 (2021) JIPITEC 402 para 1

A. Introduction

1 Non-fungible tokens (NFTs) have recently generated an unparalleled level of mainstream interest in blockchain technology with a weekly trading volume of $8.2 million.[1] NFT is a unit of data on a digital ledger called a blockchain.[2] Each NFT represents a unique digital item, and thus they are not interchangeable.[3] NFTs can represent digital files such as art, audio, videos, items in video games and other forms of creative work.[4] The idea behind NFT is that, while anyone can read the article or view the tweet, NFTs would give the owner a representation

* The Author is a B.A.LLB (Hons.) student at the National University of Advanced Legal Studies, Kerala, India. He wishes to thank Adv. Ashwini Sharma, Founding Partner, Maadhyam Law Associates for encouraging him to write on NFTs.

1 Lawrence Wintermeyer, *Non-Fungible-Token Market Booms As Big Names Join Crypto's Newest Craze,* FORBES (Feb. 12, 2021, 8:00AM), https://www.forbes.com/sites/lawrencewintermeyer/2021/02/12/non-fungible-token-market-booms-as-big-names-join-cryptos-newest-craze/?sh=2c7b3cab460a.

2 Adarsh Menon, *NFTs Explained: What they are, how they work, and their* future, GITCONNECTED(Apr. 03, 2021), https://levelup.gitconnected.com/nfts-explained-what-they-are-how-they-work-and-their-future-8808937d92b3.

3 Edd Pritchard, *NFTs represent unique digital content that are not interchangeable,* CANTONREP (Mar. 24, 2021), https://www.cantonrep.com/story/news/2021/03/24/non-fungible-nft-token-digital-ownership-certificates/6987626002/

4 *Id.*

of "ownership" in that work.[5] However, the empirical constraint of owning an NFT is different from the traditional ownership of assets. This is because owning an NFT by itself doesn't grant the right to print or distribute the work without the copyright holder's permission.[6] The situation becomes even worse when an unauthorized person makes an NFT without the copyright holder's permission. This article will trace the need to create a suitable framework under India's current copyright law in regulating the unauthorized creation of NFTs and the rising need to recognize the right to create NFT as part of the statutory bundle of rights under section 14 of the Copyright Act 1957.

2 In order to do that, the authors in Part B of this paper will provide a primer on Blockchain and NFTs and in Part C will study the challenges associated with NFT for both the buyer and the copyright holder. Part D of this paper will provide an overview of the concept of ownership and copyright jurisprudence while Part E will analyze NFTs *vis a vis* Copyright Act, 1957. This part will discuss the difference between ownership of a 'work of copyright' as against ownership of an 'NFT', and whether NFTs can be copyrighted as well as who can legally create an NFT. Part F of this paper will explore the right to create an NFT as part of the statutory bundle of rights under section 14 of the Copyright Act. Part G of this paper will provide a way ahead as to how law should balance the interest of various stakeholders to come to a middle ground. Part H will conclude this discussion.

B. Blockchain & NFTs?

3 Blockchain is a novel data structure of storing information on a computer by synchronizing data over multiple nodes.[7] It is a unique facility of the distributed ledger technology (DLT), where the transactions are grouped in a block, and each new block includes a hash of the previous one, chaining them together.[8] This shared record of transactions serves as a single point of truth agreed by the network participants' consensus.[9]

4 However certain the technology behind blockchain is, it is equally uncertain who its original inventor was. The technology of blockchain is linked very much to Bitcoin that has gained traction over the years. The inventor of Bitcoin blockchain, Satoshi Nakamoto, is believed to be an anonymous individual or group that, through their nine-page bitcoin white paper in 2008, introduced a decentralized, free to use value-transfer system.[10]

5 Whenever a transaction is created in a blockchain network, a pre-fixed amount of crypto tokens will move from the sender's address to the receiver's address.[11] Crypto tokens, or crypto assets, are special kinds of virtual currency tokens that reside on their underlying blockchains and represent an asset or utility.[12] While blockchain facilitates the transactions, it is these crypto tokens that are actually transferred.[13]

I. Smart Contract

6 Smart contract takes an important role in a discussion about blockchain. Unlike the Bitcoin blockchain, which was developed primarily to record Bitcoin transfers, Ethereum was developed to both enable the transfer of Ether, its native cryptocurrency, and include a self-executing software programming language, facilitated by the brain-child of Nick Szabo, the smart contract.[14] The trend was followed by

5 Kayleigh Barber, *What is an NFT?,* DIGIDAY (Mar.11, 2021), https://digiday.com/media/wtf-is-an-nft/

6 *See* Jonathan Bailey, *NFTs and Copyright* , PLAGIARISM TODAY (Mar. 16, 2021), https://www.plagiarismtoday.com/2021/03/16/nfts-and-copyright/#:~:text=Other%20than%20purchasing%20the%20token,without%20the%20copyright%20holder%27s%20permission.&text=It%20confers%20to%20you%20no,more%20unique%20connection%20to%20it.

7 *See* Adarsh Vijayakumaran, Legally Blocked: Evolution and legality of smart contracts. S. RAIZADA ET. AL., ADVANCEMENT IN LEGAL RESEARCH: TRANSDISCIPLINARY AND INNOVATIVE DIMENSION, 231 (2019).

8 *See id.*

9 *See id.*

10 *See* Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN (last visited Mar. 21, 2021), https://bitcoin.org/bitcoin.pdf.

11 *See What is a Blockchain Token? Intro to Cryptographic Tokens*, BLOCKCHAIN HUB (last visited Mar. 11, 2021), https://blockchainhub.net/tokens/.

12 *See id.*

13 *See generally* Marco Iansiti & Karim R. Lakhani, The Truth About Blockchain, HARVARD BUSINESS REVIEW (last visited Apr. 02, 2021), https://hbr.org/2017/01/the-truth-about-blockchain.

14 Stuart D. Lev & Alex B. Lipton, *An Introduction to Smart contracts and their Potential and Inherent Limitations,* Harard Law School Forum on Corporate Governance (May 26, 2018), https://corpgov.law.harvard.edu/2018/05/26/an-intro-

other blockchain engineers making smart contracts an important part of their specific blockchain.

7 These smart contracts are a set of promises, including protocols within which the parties perform on the other promises.[15] These protocols are usually implemented with programs on a computer network, or in other forms of digital electronics, thus these contracts are "smarter" than their paper-based ancestors.[16] For example the underlying blockchain in Inmusik enables the validation of the ownership of a song through a transparent tagging system.[17] Because of which, the party who creates the track gets their portion of fees allocated from the royalties.[18] Similarly, the smart contracts associated in NFTs are used to implement various arrangements of their underlying code.

II. Fungibility

8 An important characteristic of a crypto token is its fungibility. Fungibility determines whether or not items of the same or similar type are exchangeable and of equal value when transferred or utilized.[19] Each crypto tokens for this purpose uses its own standard of tokens. While ERC-20 is the final token standard for fungible third party identical tokens recorded on the Ethereum blockchain, ERC-721, ERC-1155 etc., is the finalized coding standard interface for non-fungible tokens in the Ethereum chain.[20] Similarly, different blockchain tokens use different standards.[21]

duction-to-smart-contracts-and-their-potential-and-inherent-limitations/.

15 *See* Adarsh Vijayakumaran, *supra* note 7.

16 *See* Adarsh Vijayakumaran, *supra* note 7.

17 *See* Sam Daley, *17 Blockchain Music Companies You Should Know,* BULLET IN (Mar. 16, 2019), https://builtin.com/blockchain/blockchain-music-innovation-examples.

18 *See id.*

19 Tony M. Evans, *Cryptokitties, Cryptography, and Copyright: Non fungible Digital Creativity on the Blockchain*, Copyright Symposium, 12 (last visited Apr. 15, 2021), https://copyrightsymposium.byu.edu/papers/CryptoKitties_Cryptography_and_Copyright.pdf.

20 *See id*; *See also How to deploy an NFT token*, TOMO CHAIN DOCS (last visited Apr. 5, 2021), https://docs.tomochain.com/developer-guide/tutorials/how-to-deploy-a-nft-token.

21 *See id.*

III. Non-Fungible Tokens (NFT)

9 NFT represents a data unit in a blockchain ledger where each NFT represents a unique digital item that is not interchangeable.[22] NFTs can be used to represent digital files such as art, audio items, video items, tweets and even a video game-based avatar.[23] While digital files are easily reproducible in multiple numbers, NFTs representing them are traced on their underlying blockchain, providing buyers with proof of ownership.[24]

10 NFTs are very much similar to other cryptographic tokens such as Namecoin and DOGE Coin. However, unlike these creatures of fungibility where each coin can be exchanged with another, NFTs most often represent the ownership of the NFT itself and sometimes even the underlying assets and even the copyright. Nevertheless, the value of each NFT is unique and is determined by the end buyer.

11 Usually, an NFT is created by uploading a file, such as an artwork, to an NFT auction market which creates a copy of the file recorded on the digital ledger as an NFT that can be bought with cryptocurrency and resold.[25] Although an artist can sell an NFT representing a work, the artist is not proscribed from retaining the copyright to the work and creating more NFTs.[26] Therefore, it doesn't necessarily mean that a buyer of the NFT gains exclusive access to the work or gains possession of the "original" digital file. Moreover, the person who uploads work as an NFT does not have to prove that they are the original artists leading to NFTs often being uploaded without the original creator's permission.[27]

22 *See* Edd Pritchard, *supra* note 3.

23 Ryan Browne, NFTs: Why crypto art and sports collectibles are suddenly so popular, CNBC (Feb. 25, 2021), https://www.cnbc.com/2021/02/25/nfts-why-digital-art-and-sports-collectibles-are-suddenly-so-popular.html.

24 *See* Kayleigh Barber, supra note 5.

25 *See NFT Shop*, CHIPPR ROBOTICS (last visited Apr. 17, 2021), https://www.chipprbots.com/projects/nft-shop/.

26 *See generally* Kal Raustiala &Christopher Jon Springman, *NFTs might not solve the digital art authenticity problem* (Apr. 14, 2021), http://slate.com/technology/2021/04/nfts-digital-art-authenticity-problem.html

27 *See* Dan Gross, *Non-fungible tokens: What they are and why artists are upset about work being 'tokenized'*, RochesterFirst (Mar. 10, 2021), https://www.rochesterfirst.com/news/digital-exclusives/non-fungible-tokens-what-are-they-and-why-are-artists-upset-about-their-work-being-tokenized/

12 Nevertheless, NFTs have gained traction over time. With the gratefulness of blockchain technology, gamers and collectors can now become the immutable owners of in-game items and other unique assets and make money from them. In some cases, players can create and monetize structures like casinos and theme parks in virtual worlds, such as the Sandbox and Decentraland.[28] Then, there are crypto millionaires like William Shatner, who issued 90,000-star trek based digital cards on the WAX blockchain showcasing various images of himself. Each of these cards which were initially sold for approximately $1, now provides Shatner with passive royalty income every time one is resold.[29] There are also cases such as the famous dragon crypto kitty valued at 600 ETH and an Axie named Angel from the NFT-based game Axie Infinity sold for 300 ETH.[30] No matter what an asset entails, NFT markets are often filled with crypto connoisseurs who see value where the naked eyes fail.

C. Challenge with NFTs

13 NFTs are today exploding with popularity which begs the question: how do they fit into the existing frameworks that govern the finance, technology, and cryptocurrency industries? Since NFTs are non-fungible and unsuitable for trading on cryptocurrency exchange platforms such as Binance or Coin DCX, it is unrealistic to treat NFTs like a normal "commodity" or even a "security" (subject to the underlying contracts). And while there are specific laws that govern the behavior of the underlying artifact that NFT represents, the current global framework is unclear in understanding what rules should govern the NFT as a whole. As it turns out, although most NFTs are digital representations in web 3.0 they are, in reality, nothing but representations of an off-chain asset. Hence, with little surprise, many of the challenges associated with off-chain assets are directly or indirectly relevant to NFTs as well.

14 The distinction between the token and the digital object to which it binds is crucial in understanding the challenges associated with NFT. In the case of most fungible crypto assets, the ownership of private key vests with the person, the ownership of assets like BTC, ETH, etc as well.[31] However, coming to the case of an NFT, the ownership of a token may or may not mean you own the digital object to which the token maps. This is because blockchains use a hash function to establish uniqueness, but a JPEG file and its copy both produce the same hash.[32] This problem was reduced drastically with the introduction of "issue systems" that allow information to be retrieved based on its content rather than location, e.g. a decentralized network like InterPlanetary File System (IPFS) solves this problem by allowing an NFT to bind with an IPFS URL such that you own the resource but the copy of the JPEG is a different resource.[33]

15 However, the challenges associated with NFTs become huge when multiple non-fungible tokens can be mapped to the same underlying digital file, IPFS URL or different copies of the same digital file.[34] This means on-chain ownership is not sufficient for off-chain objects unless the legal framework governing an NFT owner's rights respects and enforces these rights in the off-chain world. For example, say A has copyright ownership over an Art K, and A decided to sell the NFT of it to B. Since the asked price was too high, B decided to link an NFT within a different blockchain to this asset without A's authorization and sold it to C. Now, since B has sold only an NFT linked to this asset, can A claim that his Copyright has been infringed? Can there be even a right to create an NFT under Copyright Law? And what happens if the artist them/itself makes different NFTs of the same asset and sells it to other buyers at various points in time? What rights do the buyers have in this scenario?

16 The above questions essentially point to the question: what does a person get when they buy an NFT? The answer to these questions depends on what an NFT marketplace will do to honor and enforce an NFT

28 *The World Of NFT: Non Fungible Token*, SOLULAB (last visited Apr. 20, 2021), https://www.solulab.com/the-world-of-nft/#:~:text=Players%20can%20also%20create%20and,currency%2C%20on%20a%20secondary%20market.

29 *See* William Shatner, *Makes History on the WAX Blockchain!,* GLOBAL NEWSWIRE (last visited Apr. 02, 2021). https://www.globenewswire.com/news-release/2020/07/31/2071168/0/en/William-Shatner-Makes-History-on-the-WAX-Blockchain.html.

30 Ollie Leech, *What Are NFTs and How Do They Work?,* CoinDesk (last visited Mar. 23, 2021), https://www.coindesk.com/what-are-nfts.

31 *See generally* Public Keys and Private Keys: How they work with Encryption, COMODO (last visited Apr. 17, 2021), https://www.comodo.com/resources/small-business/digital-certificates2.php.

32 See Ajit Tripathi, *NFTs can Bring the real world on chain*, CoinDesk (Mar. 17, 2021), https://www.coindesk.com/nfts-can-bring-the-real-world-on-chain.

33 *See id.*

34 *See generally NFTs explained: daylight robbery on the blockchain*, Malwarebytes Labs (Mar. 19, 2021), https://blog.malwarebytes.com/explained/2021/03/nfts-explained-daylight-robbery-on-the-blockchain/.

owner and the copyright holder's rights.[35] In the absence of specific laws regulating the NFT and NFT marketplace such a voyage is unintelligible. However precarious it seems, the issues associated with the NFTs can be resolved adequately by understanding ownership, intellectual property jurisprudence and the technology itself.

D. Understanding Copyright

17 "Thou shalt not steal" is an axiomatic underpinning for both law and morality of all societies.[36] The concept of ownership that has caused many perplexities to the jurists' worldwide stems from this moral and legal norm of not infringing someone else's right.[37] In fact, our law has never known any other meaning for a title or ownership to a property than a relatively better right to possess, which of course means a better right to enjoy through such control without someone else stealing it away. For example, Austin pointed out a century ago the variable meaning of "ownership", as involving (a) indefinite and exclusive liberties of user-protected (b) by the right to exclude others from participation therein, and (should they oust the owner) by the right (c) to recapture the thing which is the object of ownership-plus (d) indefinite duration of such liberties of the user.[38] While this definition manifestly assumes ownership of real property, a person's rights to possessing intellectual property such as copyright are not much different. These physical controls of all the varieties and the absolute ability to exclude others are the central aspects of the possessory interest in any property.[39]

18 Initially, the debate was if there should be an ownership to protect an incorporeal body? For example, Justice Thompson in 1834 raised the criticism on copyright protection by explaining that "it is a well-established maxim, that nothing can be an object of property which has not a corporal substance."[40] Yeates captures this essence and articulated that the whole existence [of Copyright] is in the mind alone, incapable of any other modes of acquisition or enjoyment than by mental possession. Indeed, no tort can affect them; no fraud or violence diminish or damage them.[41]

19 However, modern copyright law has completely disregarded the above arguments. The earliest recorded historical case law on copyright ownership descends from Ireland in the 6th century A.D., wherein a dispute arose over the granting of copyright protection over a "vulgate" which was manually copied by St. Columba—a monk.[42] While delivering the judgment, the high king Diarmait noted that just like "to every cow belongs her calf, therefore to every book belongs its copy."[43] Judge Posner also introduced a similar analogy wherein he said the need to prevent non-owners from exploiting the property's value is closely aligned with that of farmers' need to protect their crops from being stolen.[44]

Statutory Recognition

20 The origin of statutory recognition of copyright law in most European countries stems from the church's and government's effort to regulate and control printers' output.[45] While the government and church supported the dissemination of government information and bibles among the common folks, dissent and criticism also circulated rapidly with printers' coming.[46] As a result, governments established controls over printers across Europe, requiring them to have official licences to trade and produce books as well as the exclusive right to print particular works for a fixed period of years, and preventing others from printing the same work during that period.[47]

35 See *generally* Ajit Tripathi *supra* note 32.

36 *See* Jon M. Garon, *Normative Copyright: A conceptual Framework for Copyright Philosophy and Ethic,* 88(5) CORNELL LAW REVIEW 1280, 128-1281 (2003).

37 *See generally* Igor Chirosca, *The Work of Fine-Art - A Source of Potential Conflicts between the Author and the Owner of the Material Support of the Work*, 2009 ROM. J. INTELL. PROP. L. 28 (2009).

38 *See* FRANCIS SAMUEL PHILBRICK, PROPERTY 105-250 (P. F. Collier & Son 1939).

39 Thomas W Merill, *Property And The Right To Exclude*, 77(4) NEBRASKA LAW REV 730, 730-35 (1998).

40 *See* Jon M. Garon *supra* note 36, at 1287.

41 *See* Jon M. Garon *supra* note 36, at 1287.

42 *See* Ruth Suehle, *The story of St. Columba: A modern copyright battle in sixth century Ireland*, Opensource (Jun. 09, 2011), https://opensource.com/law/11/6/story-st-columba-modern-copyright-battle-sixth-century-ireland,

43 *See Id.*

44 *See* Jon M. Garon *supra* note 36, at 1286.

45 *See* BENEDICT ATKINSON & BRIAN FITZGERALD, A SHOT HISTORY OF COPYRIGHT: THE GENIE OF INFORMATION 16-22 (SPRINGER 2014).

46 *See id.*

47 *See id.*

21 In 1710 in the U.K. Parliament, the Statute of Anne was enabled to encourage "learning by vesting the copies of printed books in the authors or purchasers of such copies."[48] Though the coming of the Statute of Anne marked a historical moment in the development of copyright, the debates ranged when the statutory protection of 14 years of copyright under the Statute of Anne began to expire.[49] To defend their dominant position, the booksellers shifted to common law and sought injunctions for works by authors that fell outside the Statute of Anne's protection.[50] The debate was finally settled in 1774 where it was decided by the House of Lords that the author had the sole right of printing and publishing his book, but that once a book was published, the rights in it were exclusively regulated by the Statute—a classic case of *generalia specialibus non derogant*. Nevertheless, the comings of Copyright Act, 1911 considerably extended the earlier time slab to life and 50 years—a handsome victory for most booksellers.[51]

22 The first copyright law of India was enacted by the British colony in 1847 as an imitation of the English Law.[52] Later it was replaced by the Copyright Act of 1914.[53] While India's Constitution does not make an explicit remark on intellectual protection, Article 300A of the Indian Constitution prevents deprivation of property from persons except under the authority of law.[54] Today, the Copyright Protection Act, 1957 (as amended in 2012) governs the copyright framework in India.[55] It designates the owners with the rights of reproduction, communication to the public, adaptation and translation of their work.[56] The Copyright law grants protection to literary, dramatic, musical and artistic work.[57]

23 Regardless of a variety of laws that govern copyright protection in different jurisdictions, the philosophical rationale for granting such protection has remained consistent. The copyright ownership rationale relies on the three prongs: economic interest, moral interest and natural rights interest with some slight variations. The economic interest propounds an incentive-based approach where the creator is rewarded through protection for his making for the creation he has made of public value.[58] The moral right ascribes a moral consideration of protection for one's making as it is morally right to give such a grant for the labour he has done.[59] The natural interest that goes side by side with moral interest hinges that every person has a property right to their intellectual labour.[60] Justification of copyrights in lines of these interests is approximated as either deontological or consequentialist.[61] No matter what the creation is, if one was/should be given protection under the copyright jurisprudence, they necessarily pass through these philosophical rationales. This is the reason that every product in literary, scientific and artistic domains that were not previously classified as copyrightable are protected despite the form of its expression. The vesting of copyright ownership under this jurisprudence aims to mitigate the creation from being violated through different means.

48 *See* JANE C. GINSBURG, INTELLECTUAL PROPERTY STORIES (FOUNDATION PRESS 2006).

49 *See* Id.

50 See ROGER PARRY, ASCENT OF MEDIA FROM GILGAMESH TO GOOGLE VIA GUTTENBERG 5-102 (Nicholas Brealey Publishing 2011),

51 *See* J. A. L Sterling, Crown Copyright in the United Kingdom and other Commonwealth countries, LEXUM (Last accessed Apr. 11, 2021), https://lexum.com/conf/dac/en/sterling/sterling.html.

52 Upendra Baxi, Copyright Law and Justice in India, 28(4) JOURNAL OF THE INDIAN LAW INSTITUTE 497, 497-540 (1986).

53 *See id.*

54 IND. CONST. art. 300A.

55 *See The Copyright Act 1957,* Copyright, (last access Apr. 02, 2021), https://copyright.gov.in/documents/copyright-rules1957.pdf.

56 *See id* **§14.**

57 *See id* **§14.**

58 See William Landes & Richard A. Posner, An economic analysis of Copyright Law, An Economic Analysis of Copyright Law, Cyber Harvard (Last accessed Apr. 05, 2021), https://cyber.harvard.edu/IPCoop/89land1.html.

59 *See* Betsy Rosenblatt, Moral Rights Basics, Cyber Harvard (Last accessed Apr. 05, 2021), https://cyber.harvard.edu/property/library/moralprimer.html.

60 *See Basic Notions of Copyright And Related Rights,* WIPO (last accessed Apr. 2, 2021), https://www.wipo.int/export/sites/www/copyright/en/activities/pdf/basic_notions.pdf.

61 *See* Robert P. Merges, *The Philosophical Foundations of IP Law: The Law and Economics Paradigm* (UC Berkely Public Law Research Paper No.2920713), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2920713#.

E. NFT vis a vis The Copyright Act, 1957

24 The copyright jurisprudence has always been in a state of constant evolution. The Act has been amended in 1983, 1984, 1985, 1991, 1992, 1994, 1999 and 2012 to meet various national and international requirements.[62] It is interesting to note that every time an amendment happens in the Copyright Act, it connotes that the law has encompassed novel inputs within its ambit to recognize the rights of a copyright owner, which again is viewed through the lens of natural interest, moral interest and economic interest of the creator.[63] Nevertheless, more than conferring certain rights on creators that flow historically through the lens of copyright philosophies, the primary reason the law has accepted the rights of owners of their work as against any external infringement has been to stimulate activity and progress in the arts for the intellectual enrichment of the public.[64]

25 As per section 2(y) of the Copyright Act, a work in which copyright subsists includes literary, dramatic, musical and art works.[65] This consists of both sound recordings as well as cinematography.[66] The question of copyright is of utmost relevance in NFTs as they are nothing but blockchain engraved literary, musical or art work.[67] While owning an NFT does not by itself confers the owner of an NFT with the ownership of the artwork or even the copyright of that work, the question, if there is a right to create an NFT, is important since NFTs are of utmost economic value, and are "unique" meaning, there can only be one NFT of a particular artifact created in a specific blockchain.

26 Section 14 of the Copyright Act confers the creators of copyrighted work to do or authorize the doing of reproduction, communication, adaptation and translation of the work.[68] The tricky part is whether the rights available to the owners under section 14 of the Copyright Act confers the copyright owner with the creation of an NFT as well? More importantly, should the creation of an NFT be viewed separately from its underlying creative work? Furthermore, can there be a right to create separate NFTs for the same artwork? These questions that first arose in part C of the article will be addressed here. This part of the article must be read with part B of this article, where an extensive discussion has been made on NFTs. Nevertheless, the process of making an NFT is reemphasized in this section for easier comprehension.

I. Ownership of a 'work of copyright' vs. ownership of an 'NFT'

27 The ownership of NFT as a unique token against ownership of content that the NFT is linked with requires a clear distinction. Various buyers and crypto enthusiasts worldwide often perceive that you own the work once you buy an NFT of a particular creative work.[69] This notion is fallacious from its very origin. The reality is fundamentally different. When someone purchases an NFT linked to a piece of content, they don't automatically purchase the underlying intellectual property rights in such a piece of content. What happens here is that they have purchased the NFT associated with it and nothing more (absent certain documentation)[70].

62 Abhay Pandey, *Development In Indian IP Law: The Copyright (Amendment) Act 2012*, Intellectual Property Watch (Jan. 22, 2013), https://www.ip-watch.org/2013/01/22/development-in-indian-ip-law-the-copyright-amendment-act-2012/.

63 *See* for e.g. *id; Also see* Zakir Thomas, *Overview of Changes to Indian Copyright Law,* 17 JOURNAL OF INTELLECTUAL PROPERTY RIGHTS 324, 324-334 (2012).

64 *See generally* University of Oxford v. Rameshwari Photo Copy Services, 2016 SCC Online Del 5128, **¶80** (India).

65 *See* for e.g. Gramophone Company of India Ltd. v. Birendra Bahadur Pandey & Ors, 1984 AIR SC 667; Also *see* Entertainment Network (India) Limited v. Super Casette Industries Limited, 2009 AIR SC 1150.

66 *See* Super Casette *id* **¶28.**

67 *See* Jaideep Reddy Et. Al., Cryptocurrency: The status and future of NFTs and crypto art in India, The Economic Times (Apr. 08, 2021), https://economictimes.indiatimes.com/tech/catalysts/the-status-and-future-of-nfts-and-crypto-art-in-india/articleshow/81970883.cms#:~:text=Simply%20put%2C%20non%2Dfungible%20tokens,and%20even%20casks%20of%20whisky.

68 The Copyright Act, 1957, No. 14, Acts of Parliament, 1957, **§14** (India).

69 *See* for e.g. Andrew R. Chow, *What Are NFTs and Why They Are Shaking Up the Art World*?, Time (Mar. 22, 2021), https://time.com/5947720/nft-art/.

70 *See* Ghaith Mahmood, *NFTs: What Are You Buying and What Do You Actually Own?,* The Fashion Law (Mar. 18, 2021), https://www.thefashionlaw.com/nfts-what-are-you-buying-and-what-do-you-actually-own/. ("Many market participants claim that NFTs can be used to prove authenticity. In fact, NFTs can authenticate ownership of a token itself, as well as the unique history of how such token was developed and linked to a creative work — on the public blockchains, anyone can see an owner's wallet address and its linked metadata, as such information is available as a public record.

28 Referring to part B of our discussion, NFT is nothing but a non-fungible unique cryptographic token. Under Section 14 of the Copyright Act, as mentioned previously, a copyright owner has certain exclusive rights to reproduce, prepare adaptations of a work, perform, display and distribute the copyrighted works in public.[71] As a general rule, the purchase of a piece of art does not transfer all copyright in such work to the buyers that work.[72] Instead, when someone buys a painting from an art gallery, they acquire the physical painting itself, which they can display, but not the underlying rights to reproduce, make adaptations of works or distribute copies of that painting.[73] The underlying copyright only transfers if the copyright's owner evidence in writing that they intend to transfer those rights alongside the composition of the work to the buyer.[74] Unless the NFT owner has received such explicit permission from the seller, the NFT owner does not automatically acquire the legal right to take pictures of the creative work attached to the NFT and make copies of it to distribute in any form to the public. This same principle applies to the artwork's ownership. Unless the owner of the original asset sells the work to the buyer with underlying documentation as to the rights associated with it in the NFT, the buyer does not actually possess the work. This means, absent specific documentation, the purchaser of an NFT acquires through that purchase a right to the NFT only and that too, to display the related media in their token wallet for personal purposes and to sell it to prospective buyers when needed.

29 Therefore, due regard must be given to the properties of an NFT as noted in its smart contract. If the smart contract does not vest with the buyer either the ownership of the asset itself or the copyright ownership, then what you are probably buying is just the NFT itself and nothing more. Most often, it happens that crypto-pirates associate an unauthorized piece of content with the blockchain and make an NFT out of it, absent laws restricting such linking, the NFT sold due to it only vests with the buyer of the token and not any other rights. This point has to be noted whenever someone buys a new NFT. While it is a general habit that NFTs are traded inattentive of their actual value, the knowledge that there are other rights a user will possess will help enrich the buyer mark the right price for the Token since the Token's value, in that case, will be cryptography and rights value (if any).

II. Can NFTs be copyrighted?

30 Crypto marketplaces today are flooded with NFTs as new players are entering the market every day. Very recently, Wazir X—an India based crypto exchange platform, launched its version of an NFT auction site.[75] These developments have created a seamless exchange of digital assets and intellectual properties, including art pieces, audio files, videos, programs and even tweets, as part of the greater blockchain ecosystem attracting users from everywhere in India.[76] It is at this time of ascending transcendence of blockchain becoming the next internet, the question of the right to create an NFT becomes all the more essential.

31 Indeed, section 14 of the Copyright Act vests the author with a bundle of statutory rights that enables the author to create various methods of public display of their work as well as prevent others from doing so.[77] Still, when it comes to NFT, the Act does not explicitly identify blockchain enabled digital or digitized works as copyrightable subject matter because

However, a simple NFT by itself cannot help with matching the creator or owner of an NFT to a real person in the physical world, nor does it validate that the creator of the NFT has the underlying rights to tie that NFT to any specific creative work.")

71 The Copyright Act, 1957, No. 14, Acts of Parliament, 1957, **§14** (India).

72 *See generally* Rich Stim, *Copyright Ownership: Who Owns What? - Copyright Overview*, Stanford Copyright and Fair Use Center (last visited Apr. 20, 2021), https://fairuse.stanford.edu/overview/faqs/copyright-ownership/.

73 *See generally Principles of Copyright*, WIPO (last accessed Apr. 17, 2021), https://www.wipo.int/edocs/pubdocs/en/copyright/844/wipo_pub_844.pdf.

74 *See* Saregama Ltd v. The New Digital Media & Ors. C.S. No. 310 of 2015, Cal HC (India);*See How Does Transferring a Copyright Work?,* MightyRecruiter, (last visited Apr. 21, 2021), https://www.mightyrecruiter.com/recruiter-guide/how-does-transferring-a-copyright-work/.; Also *see Copyright Licenses and Assignments*, Bitlaw (last visited Apr. 20, 2021), https://www.bitlaw.com/copyright/license.html.

75 Omkar Godbole, *Binance-Owned WazirX Launches India's First NFT Platform*, CoinDesk (Apr. 06, 2021), https://www.coindesk.com/binance-owned-wazirx-launches-indias-first-nft-platform#:~:text=Created%20with%20Sketch.,digital%20assets%20and%20earn%20royalties.

76 *See* Benita Fernando, *How a new platform may start the next big trend in the Indian art market — NFTs,*The Indian Express (Apr. 25, 2021), https://indianexpress.com/article/express-sunday-eye/how-a-new-platform-may-start-the-next-big-trend-in-the-indian-art-market-nfts-7287485/.

77 *See* Arathi Ashok, *Economic Rights of Authors under Copyright Law: Some Emerging Judicial Trends*, 15 Journal of Intellectual Property Rights 46, 46-54 (2010).

the law applies with equal force to physical embodiments and those requiring the aid of a machine or a device to perceive. Moreover, the current law only recognizes literary, dramatic, musical work and a computer program for copyright protection.[78] An NFT being merely a cryptographic token that represents a proof of ownership either of the token itself or the work or even the copyright of the work or a combination of any of these is not copyrightable by itself unless a minimal amount of creativity within it is shown along with originality and fixation that forms substructure of any copyrightable work. Therefore, any copyrightable authorship-including creative NFTs such as [Cryptokitties][79] contributed by an author must showcase these characteristics

III. Who can create an NFT?

32 The narrow wordings of section 14 of the Copyright Act have limited even the remote acceptance of the right to create NFT as part of the statutory bundle of rights given to an author. However, an NFT being a purely technological innovation that does not any have an ounce of root to be considered by the framers of the Copyright Act presupposes the existence of a meta legal right that could be associated with the creation of an NFT or any other technological innovation that hinges on the authority of authors to their creation. The meaning of copyright for the purposes of the Copyright Act includes but is not limited to the exclusive right to communicate the work to the public, issue copies that are not already made to the public, make adaptations, as well as translations of the work.[80] The question we should address here would be whether making an NFT could be considered communication of the work to the public? Or to issue copies of the work? Or to make adaptations, or even the translations of the work?

33 To answer, we will emphasize here once again the process involved in the making of an NFT. The creation of an NFT is a very easy process that does not need little to any amount of technical know-how compared to its underlying technology. Any person could make an NFT by first connecting their crypto wallet to the NFT marketplace.[81] The wallet address would probably be the login info in most scenarios so that one won't have to share any other details. After the wallet has been connected, one can move to the "Create" section on the marketplace, then upload their artwork and finalize the process by clicking the right buttons.[82]

34 Interestingly, the issues of copyright take their birth at the point where they upload the work. The uploading in any platform could be through various ways, for example, uploading from the cloud, uploading by connecting the link, uploading from the hard drive, etc.[83] If the work uploaded is an original one or even if it is a copy (with an obvious case of copyright violation) in the absence of specific authorization, infringement of copyright happens as soon as it has been uploaded into the NFT marketplace. This is because although downloading or other private copying is permitted sometimes, once the content has been uploaded for public display (NFT marketplace) by uploading or otherwise offering to share copyright-protected content (without authorization), it remains illegal in almost every jurisdiction.[84]

35 Now assume the person has been authorized to display such by virtue that they bought the article. Now, will there be a copyright violation if that person creates an NFT of the specific piece? We rely on the rights exclusive to the copyright owner as a part of the statutory bundle under section 14. These rights include the right to create adaptations as well

78 *See* The Copyright Act, 1957, No. 14, Acts of Parliament, 1957, **§13** (India).

79 *See* Fitz Tepper, *People have spent over $1M buying virtual cats on the Ethereum blockchain*, TechCrunch (Dec. 04, 2017, 5:18 AM), https://techcrunch.com/2017/12/03/people-have-spent-over-1m-buying-virtual-cats-on-the-ethereum-blockchain/.

80 *See* for e.g., R. G. Ananad v. Delux Fimls and Ors, 1978 AIR SC 1613 (India).

81 *See* Georgia Cogan, *Confused about NFTs? Here's all you need to know*, Creative Bloq (Mar. 24, 2021), https://www.creativebloq.com/features/what-are-nfts#:~:text=Technically%2C%20yes%2C%20everyone%20can%20sell,buys%20the%20piece%20%E2%80%93%20including%20resales.

82 *See* for e.g. *How to Create an NFT*, alchemy (last visited Apr. 25, 2021), https://docs.alchemyapi.io/alchemy/tutorials/how-to-create-an-nft.

83 *See generally Different ways to upload a file?*, Stack Overflow (last visited Apr. 26, 2021), https://stackoverflow.com/questions/31238641/different-ways-to-upload-a-file; Also *see generally 7 Ways to Upload Images to the Internet*, wikiHow (last visited Apr. 17, 2021), https://www.wikihow.com/Upload-Images-to-the-Internet; *See* Alex Atallah, *Create NFTs for Free on OpenSea*, OpenSea blog (Dec. 29, 2020), https://opensea.io/blog/announcements/introducing-the-collection-manager/.

84 S*ee generally* Christian Louboutin Sas v. Nakul Bajaj, 2014 SCC ONLINE DEL 4932 (India); Also *see* Luxottica Group S. P. A. v. Mify Solutions Pvt Ltd., 2018 SCC ONLINE DEL 12307 (India).; *See* Charsur Digital Workstation v. ASV Cyber Solutions Inc, 2016 SCC ONLINE MAD 32741 (India).

as translations of the work.[85] While an argument that the copyrighted work has been translated to the blockchain languages of GO, C++, Java etc. by converting it to an NFT, it would be difficult to comprehend for the prudent mind the argument that by creating an NFT, the creator of NFT has made an adaptation of the original work. The adaptations under copyright are basically a change of format.[86] If an adaptation is made by adding a significant amount of new material, then such work would not be considered as adaptation under the Copyright Act,[87] but in an NFT, no such significant work is added to transform it, rather a blockchain-enabled proof of ownership is created.

F. Recognizing the Right to create an NFT

36 The word right is a blind guide in its own proper field. As noted by Pound, the word right is used in at least five senses. (1) It represents interest as recognised and delimited to secure it through the legal order. (2) It can designate the chief means which the law adopts in order to ensure interests, namely, a recognition in persons, or a conferring upon persons, of specific capacities of influencing the action of others. (3) In another sense, "right" is a capacity of creating, divesting, or altering "rights" in the second sense, and also of creating or altering duties. (4) It can signify a condition of legal immunity from liability for what otherwise would be a breach of duty. (5) Lastly, it can also be used in a purely ethical sense to mean that in the balance of equities, a person should probably have it.[88]

37 When an author creates a work, certain rights flow from it. It could be economic rights, or moral rights or even natural rights. These rights are ascribed with every work of the creator so that the creator can enjoy the benefits of the creation as a reward for the contribution to the public of that creativity. Article 12 of the Berne Convention recognizes authors of literary or artistic works' exclusive right of authorizing adaptations, arrangements and other alterations of their works. This right of an author is a combination of economic, moral and natural rights that allows the author to preserve their integrity of work and have an exclusive say on what to do with it. Even though the Article refrains from laying down what constitutes adaptation, it is agreed that this includes any new form of the substance of the work, marginal cases being left to the courts. India has been a signatory to the Berne Convention since 1928. This is further established under (a) and (c) of section 14 of the Copyright Act that protects the author's exclusive right to create adaptations.

38 In our present scenario based on the above discussions, although the balance of equities that Pound postulates lies in favour of the original copyright holder to claim the right to create an NFT, the copyright owner must have an exclusive right under the copyright framework to claim it in the first place. This is because, as noted in various judgments dealing with copyright infringement in India, there exists no right outside the statute.[89] Since copyright is merely a statutory right in India, the claim that the author has an exclusive right to create an NFT of their work does not hold. For a right to be recognized, it has to be settled through the legal order.[90] In India, such recognition could happen in either of the three ways: the judicial order based on the judiciary's power under the basic structure of the Constitution, through an executive order or through a legislative amendment, representing the people's will.[91] In the absence of such explicit recognition the metaphysical right that every author has for their Creative work to make an NFT will be infringed without any recourse.

39 Now assume, such a right has been granted to the copyright holder, even then certain issues arise. This is because beyond the Copyright domain where the debate of the copyright holder's right to create or to not create NFTs bestrides the programmable nature of NFTs which present new ways for creators to license, monetize and enforce their copyrights. From the copyright holder to the owner of the work and potential NFT buyer, each can be empowered in

85 The Copyright Act, 1957, No. 14, Acts of Parliament, 1957, **§14** (India).

86 *Copyright Law and a Derivative Culture*, SUPREME COURT CASES (last accessed Apr. 19, 2021), www.supremecourtcases.com/index2.php?option=com_content&itemid=1&do_pdf=1&id=19308;*See* Nandita Saikia, *Adaptations, Derivations and Transformations in Copyright Law*, Lawmatters, https://copyright.lawmatters.in/2010/10/adaptations-derivations-and.html.

87 *Id.*

88 ROSCOE POUND, JURISPRUDENCE VOL. 1, 39-163 (West Publishing Co. 1959).

89 *See* for e.g. Time Warner Entertainemnt Company, LP & Ors. v. Columbia Picures Inc. and Ors, 2007 AD DEL 10 577 (India); Also see for e.g., Bristol Myers Squibb Holding Ireland and Ors v. Natco Pharma, CS(COMM) 342/2019 (India).

90 His Holiness Kesavananda Bharati Sripadagalvaru v.State of Kerala and Anr, 1973 AIR SC 1461, **¶1459.**

91 *See* Ashish Bhan & Rohit Rohtagi, *Legal systems in India: Overview*, Thomson Reuters:Practical Law (Mar. 01, 2021), https://uk.practicallaw.thomsonreuters.com/w-017-5278?transitionType=Default&contextData=(sc.Default)&firstPage=true.

Web 3.0 to exert greater control and enjoy more substantial financial participation throughout the copyright's duration. Any area that can reasonably be distilled to "if, then" outcomes and matters of timing that lend themselves well to automated outcomes can benefit significantly in a blockchain atmosphere through the process of automatic reversions, terminations etc., that blockchain smart contracts contribute.[92] The power of NFTs to tokenize copyright interests (including fractional interests), encoded with immutable instructions, would be of great use to the Copyright Office in storing and easier access of copyright records.[93] Therefore, granting such an exclusive statutory right for the copyright holder would mean requiring the copyright holder's permission in every move related to the storing of copyright records in a blockchain, where if the creator of the original work is disinterested in the tokenization then it would mean the storing of multiple data units—one with the traditional mechanism and the other within a blockchain enabled channel for those who are interested in NFTs.

40 Furthermore, sometimes it may happen that the copyright holder might create multiple NFTs of the same asset in different blockchains which is one of the well known mechanisms to hedge against any price deviations that may occur in the volatile market places of NFTs. Assume, if a buyer buys an NFT when there was only one NFT created on that particular artifact and later finds out that the copyright holder has created a different NFT of the same artifact in a different blockchain. Now, this could have potential implication on the price of the NFT that was bought before since there are now, more than one NFT for the same artifact. What recourse does the previous buyer have against this? The next part of the discussion will provide further insight on these scenarios as to how to deal with it.

G. The Way Ahead

41 The emergence of Non-Fungible Token standards to create unique crypto assets presents massive opportunities for creators to leverage digital technology and the Internet in the Web 3.0 world in ways far more empowering than what the Internet appeared to be in the dotcom era of the 90s. Cryptography and digital signatures, combined with non-fungible token standards, offer new opportunities to solve some of the chronic concerns regarding the lack of imbalance of power and profit tilted for centuries in favour of intermediaries. While we are still in the nascent stages of building the crypto infrastructure and have just begun to test the waters in the uncharted seas of white paper promises beyond cryptocurrencies, the possibilities abound to create a new age of digital revolution where the transparent atmosphere with accessible records of data and automated programmes could change the way we perceived many of the traditional functions.

42 However, the future of NFTs in India, especially the creative art-based assets, is haunted by regulatory uncertainty and the narrow wordings of intellectual property laws. The questions regarding copyright protection for the artist for both NFTs as well as original creative works are discussed in this article. Now, it is up to the legislators to make a suitable amendment in the existing law to recognize the rights of copyright holders as part of the statutory bundle of rights under section 14 of the Copyright Act. While, as noted in the previous discussion, recognizing such a right does not come with a bed of roses, many of the shortcomings can be mitigated with either the technology itself or through suitable wordings in the assignment/license/intellectual property transfer (smart) contracts associated with the NFT.

43 The addition of necessary demarcation of rights and liabilities for a creative art buyer with implications of the potential creation of NFT would help the buyer sell the work in an NFT marketplace in the future. Similarly, while a person owns only the NFT rather than the original asset or the copyright ownership in normal scenarios, suitable smart contracts coupled with other legal mechanisms could widen the ambit of NFTs. However, the problem with this approach is that most of the marketplace smart contracts are ready-made. However, if there is a mechanism within the NFT platform to create custom made smart contracts that could draw the line as to the originality of the assets, the rights conferred, royalties, if any etc., then the problems associated within the market regarding intellectual property infringement associated with the sale of NFTs could be brought down.

44 Furthermore, in a situation which we have mentioned in the previous section where the copyright holder might create different NFTs for the same asset; the problems associated with such NFT dizygotic twins can be addressed if the buyer ensures that the smart contract associated with the particular NFT is supplemented with terms and conditions (non executable or otherwise in the same blockchain but forms the crux of relationship between the buyer and the seller) that prohibits or waiver multiple creation of NFT for the same assets by the copyright holder.

92 Tonya M. Evans, Cryptokitties, Cryptography, and Copyright, 47 AIPLA Q. J. 219, 265 (2019)

93 *Id* at 235.

45 Finally, coming into the unauthorized creation of NFTs, it must be noted that the marketplace, even though exploding with various products, suffers hugely from copyright piracy.[94] We could wait for the platform owners to only allow the original works to be uploaded and displayed as well as require necessary copyright authorization rather than violation; however, most policies associated with these platforms are designed for increased usership rather than the protection of the copyright holders. Moreover, the current law does not allow a right to create an NFT as part of the statutory bundle. Thus, the legal recognition of the NFT is necessary to resolve the current copyright issues involved within NFTs. Once this recognition has been granted, most marketplaces will become an authentic platform to buy/sell unique crypto assets. However, law makers must in addition to the recognition of NFT must also look forward for a suitable code of conduct and model rules to contain the growth of fraudulent sites.

H. Conclusion

46 Blockchain and the NFT standards show a substantial promise to offer viable answers to solve the various real world problems that have been surrounding the artifacts market and the copyright offices for a very long time.[95] While the technology is significantly new, like cryptocurrencies the unique NFT tokens have also gained a massive amount of real world traction in India as well as elsewhere.[96] Nevertheless, these speculative markets are surrounded by crypto-pirates and gullible buyers hoping to win fortunes in the volatility. The issues of copyrights in NFT are not a new age problem. Whenever a new technology is born, the intellectual property law has always faced a Freudian dilemma in recognizing their place in the broad framework of rights and duties that forms the bedrock of law.[97]

47 The present article has explored the scope of NFT within the wide framework of Copyright law and ownership. The article has also brought forth and addressed various issues that are surrounding the NFT marketplace. While some of the issues can be solved using the technology itself others require broad legal frameworks and suitable wording under various provisions of the copyright law. The need to recognize the right to create NFT as part of the statutory bundle of rights could be the first step in addressing the major copyright issues that surround the NFT market today. Nonetheless, it will be interesting to see how the regulators, the lawmakers, and various stakeholders will balance their interests in creating the novel NFT framework in India.

94 *See* Kal & Christopher *supra* note 26; Also *see* supra note 34.

95 *See India Shouldn't Throw Out the NFT Baby With the Crypto Bathwater*, The Wire (Apr. 04, 2021),https://thewire.in/tech/india-nft-cryptocurrency-digital-content-royalties-regulation; Also *see generally* Ferdinand Regner Et. Al., NFTs in Pr s in Practice – Non-F actice – Non-Fungible Tokens as Core Component of a Blockchain-based Event Ticketing Application (last visited Apr. 22, 2021), https://core.ac.uk/download/pdf/301384284.pdf

96 Emmanuel Chibuzor Precious, Non Fungible Tokens, the next big thing in the DeFi Ecosystem?, Trust Wallet (Jan. 08, 2021), https://trustwallet.com/blog/non-fungible-tokens-next-big-thing; Also *see* Tribal Scale Inc, *What are NFTs and Why are They Becoming Popular?*, Medium (Mar. 09, 2021), https://medium.com/tribalscale/what-are-nfts-and-why-are-they-becoming-popular-c3ca2c84a4b3.

97 *See* for e.g., *The Digital Dilemma: Intellectual Property in the Information Age*, The National Academies Press (last accessed Apr.04, 2021), https://www.nap.edu/read/9601/chapter/7.

The (Missing) Parody Exception in Italy and its Inconsistency with EU Law

by **Gabriele Spina Ali***

Abstract: The Italian Copyright Statute does not contain a general exception for 'parody, caricature and pastiche' pursuant to Article 5(3k) of the InfoSoc Directive. In spite of this, commentators believe that the case law prior to the Directive sufficiently safeguards parodies against infringement, by granting them the status of autonomous, 'transformative' creations and leveraging on the fundamental freedoms of speech and artistic expression as enshrined in the Italian Constitution. In addition, they have lauded this approach for avoiding downgrading parody from an 'overarching principle' to a narrowly defined 'exception' to copyright protection. The present article criticizes this construct by dissecting and rebuking the related arguments. It emphasizes its inconsistency with the InfoSoc Directive and the recent case law of the Court of Justice of the European Union and submits that, paradoxically, framing parody as a principle leads to more restrictive outcomes than an ad verbum implementation of Article 5(3)(k).

Keywords: Parody; Copyright; Exceptions and Limitations; Three-step test

Recommended citation: Gabriele Spina Ali, The (Missing) Parody Exception in Italy and its Inconsistency with EU Law, 12 (2021) JIPITEC 414para 1

A. Yet another boring contribution on a fun topic

1 It is commonplace that lawyers take professional matters overly seriously, even the most laughable ones. Italian lawyers are no exception to the rule and the debate surrounding parody does confirm to the cliché. Commentators submit that the lack of an explicit exception in the Italian Copyright Statute (ICS) does not undercut the importance of parody in the legal system, nor undermines the freedom to engage into humorous reinterpretations of prior works. Quite on the contrary, it reflects a well-pondered choice: not to relegate parody to a mere 'exception' but to reaffirm its status of overarching principle in the Italian copyright system. In this sense, parody is not a defense-type rule that grants immunity against conduct that would otherwise constitute infringement, but an activity that falls outside the reach of copyright. According to this view, the legitimacy of parodies derives from the basic principles governing the scope of copyright protection and infringement, as well as the fundamental rights of freedom of speech and artistic expression, as enshrined in Articles 21 and 33 of the Italian Constitution.

2 The present article takes issue with this framing and casts doubts over its legitimacy. In particular, it submits that the recent caselaw of the European Court of Justice (CJEU) on the relationship between fundamental rights and copyright exceptions and limitations (E&L), as well as the scope of the exclusive rights of reproduction, distribution and communication to the public, undermine the Italian construct on parody.[1] Under this perspective, the

* Senior Research Fellow MPI, Executive Editor GRUR International Intellectual Property and Competition Law.

1 *Spiegel Online GmbH v Volker Beck* C 516/17, CJEU (2019); *Pelham GmbH and Others v Ralf Hütter and Florian Schneider-Esleben* C476/17, CJEU (2019); *Funke Medien NRW GmbH v*

article hopes to be of interest also for other European jurisdictions, especially those who do not foresee an explicit parody exception in their statutes.[2]

3 The article develops its arguments in the following order. Section B describes the current legal system, citing both the relevant case law and the academic literature. Sections C carries out a critical analysis of the legal construct endorsed by courts and academics, dissecting the arguments that parodies are autonomous creations (C.I), that they do not fall within the right of adaptation (C.II) and criticizing the reference to broad constitutional principles (C.III). Section D addresses the question of the alleged negative effects of implementing an exception at the statutory level, providing further arguments against treating parody as a principle (D.I and D.II). In particular, it submits that an explicit exception carries no risks both in terms of narrowing down the scope of parody (D.III and D.IV) as well as in terms of the application of the three-step test (3ST) (D.V). Section E shortly concludes by reflecting on the gap between the academic theorization of the law and its pragmatic application.

4 As for its limitations, mostly for reasons of space, the article avoids delving into two issues. The first one is the relationship between parody and moral rights, and in particular the right of integrity. This is because according to a common take, parodies do not normally harm the reputation of the author of the first work, insofar as it is prima facie clear that the two works originate from different authors.[3] The second is the balancing between the right to engage in parodies and conflicting interests such as honor, privacy or the principle of nondiscrimination, being the focus of the paper the conflict between parody and the exclusive rights granted to copyright holders.[4]

B. The Legal Framework in Italy and the EU

5 In Italian copyright law, the parliamentary debate on parody dates as far back as 1882, when the appointed committee refused to include parodies among the list of infringing conducts. In 1919, there was a second heated debate on whether parodies constituted derivative elaborations under the control of the author of the parodied work or they fell outside the scope of its exclusive rights. In the end, the advocates of opposite solutions just 'agreed to disagree', and the matter has been left unregulated up to nowadays.[5]

6 Parody received a renewed attention following the enactment of Directive 2001/29/EC (InfoSoc Directive), whose Article 5 contains an *optional* list of E&L to the exclusive rights of reproduction, communication to the public and distribution.[6] As clarified by the CJEU, the list of E&L in Article 5 has exhaustive character, foreclosing any possibility to implement different exceptions beyond the ones enumerated by the provision.[7] Among the relevant exceptions, Article 5(3)(k) allows the use of copyrighted works 'for the purpose of caricature, parody or pastiche'.

7 In *Deckmyn*, the CJEU clarified that these are autonomous concepts of EU law and domestic laws bear no role in clarifying their meaning.[8] The CJEU construed the scope of parody primarily by leveraging on the ordinary meaning of the term in the everyday language, but also on the context of the provision and the objective of the InfoSoc Directive.[9] From these criteria, the Court concluded that the two essential characteristics of parody are to evoke an existing work while being noticeably different from it and to constitute an expression of humor or mockery.[10] No other limiting condition applies to parody, which would not find a solid basis on the above-mentioned interpretative canons. As such, it is irrelevant whether parodies display an

Bundesrepublik Deutschland, C-469/17, CJEU (2019).

2 See for instance the Swedish Act on Copyright in Literary and Artistic Works (Swedish Statute Book, SFS), 1960:729, last amended April 1, 2011.

3 Court of Milan 29 January 1996, Tamaro v Soc. Comix e Soc. P.D.E, *Il Foro Italiano* (1996) 1432; Court of Naples 15 February 2000, De Filippo v Altieri in *Dir. D'autore* (2001) 471; Court of Naples, 15 February 2000, in *Dir. informaz. e informatica* (2001) p. 457.

4 See *Johan Deckmyn et al. v Helena Vandersteen et al.*, C-201/13, CJEU (2014).

5 A. Monti (1996) Case Note to Court of Milan 29 Jan 1996, Tamaro v Soc. Comix e Soc. P.D.E, *Il Foro Italiano,* pp. 1426-8.

6 See Art. 2, 3 and of 4 of Directive 2001/29/EC of The European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (InfoSoc Directive).

7 See Recital 32 of the InfoSoc Directive. See also Spiegel Online at 41; Funke Medien at 56; Pelham at *32.*

8 Deckmyn at 15.

9 Deckmyn at 19.

10 Deckmyn at 20-1.

original character, can be reasonably attributed to a person other than the author of the original work or even mention the source of the parodied work.[11] Unlike other E&L in the Directive, parody is a full-harmonization measure, which leaves Member States no room to maneuver once they decide to implement the exception.[12-13]

8 More recently, Article 17 of the Directive on Copyright in the Digital Single Market (DSM Directive) reiterated that users shall be able to rely on the parody exception when uploading and making available user-generated content on online content-sharing services. In other words, users must be able invoke parody as a defense against takedown measures targeting their derivative content published on online platforms.[14] Marking an important shift from the InfoSoc Directive,[15] the wording of the provision and its context make parody a mandatory exception but *only* for the online activities falling within the scope of the provision.[16]

9 Adopted in December 2021, the legislative decree for the implementation of the DSM in Italy opted for an *ad verbum* implementation of the above-mentioned provision. It allows platform uses to rely on "the exception or limitation" for "the purpose of parody, caricature or pastiche",[17] but does not stipulate an equivalent exception for offline uses. Undoubtedly, this choice adds an additional level of complexity to the legal regulation on parody. Indeed, it is difficult to predict whether it would lead to diverging standards for parody in the offline and online environment, or if the Italian courts will adopt the legal solutions elaborated for the former to the latter.[18]

I. Italian Courts

10 Not without efforts, Italian courts have managed to fill the void left by the legislator. Their definition of parody is similar to the one adopted by the CJEU, even if there are noteworthy differences. According to the case-law, a work qualifies as a parody when, notwithstanding the evident utilization or evocation of a previous one, it shows a creative contribution capable of modifying or overturning the message conveyed by the referenced work, so to achieve a humorous result of any kind.[19-20] This appears a different formulation of the two constitutive elements identified by the CJEU in Deckmyn, i.e. the evocation of pre-existing material and parody's humorous connotation. In spite of this, it seems to require a *quid pluris*: a substantial modification of the message conveyed by the original work, i.e. its *transformation* into something entirely different.

11 For what concerns their regulation, courts have unanimously ruled that parodies do not infringe upon the exclusive rights of copyright holders. This leaves the public at large free to engage into humorous reinterpretations of copyrighted material, without the need to seek approval or compensate the rightsholders of the referenced works. This conclu-

11 Deckmyn at 21.

12 See Deckmyn vis-à-vis Funke Medien at 42-3 and Spiegel Online at 26-7.

13 For some literature see Eleonora Rosati (2015) 'Just a Matter of Laugh? Why the CJEU Decision in Deckmyn is Broader than Parody', *Common Market Law Review* 52(2), 511-30; Daniel Jongsma (2017) 'Parody after Deckmyn - A Comparative Overview of the Approach to Parody under Copyright Law in Belgium, France, Germany and the Netherlands', *IIC* 48(6), 670-674.

14 Article 17(7), Directive 2019/790 on Copyright and Related Rights in the Digital Single Market.

15 See Recital 70, Directive 2019/790; Axel Metzger & Martin Senftleben (2020) Selected Aspects of Implementing Article 17 of the Directive on Copyright in the Digital Single Market into National Law, *European Copyright Society*.

16 Christophe Geiger & Bernd Justin Jütte (2021) 'Towards a Virtuous Legal Framework for Content Moderation by Digital Platforms in the EU? The Commission's Guidance on Article 17 CDSM Directive in the light of the YouTube/Cyando judgement and the AG's Opinion in C-401/19', *European Intellectual Property Review* 43(10), 634-36; Joao Pedro Quintais, Giancarlo Frosio et al. (2020) 'Safeguarding User Freedoms in Implementing Article 17 of the Copyright in the Digital Single Market Directive', JIPITEC 10, 277-282.

17 Art. 102 nonies, par. 2(b), Italian Copyright Statute, as amended by Legislative Decree 8 November 2021, n. 177.

18 See, for instance, Confindustria (2021) 'Position Paper: Recepimento della Direttiva europea n. 790/2019 sul diritto d'autore e sui diritti connessi nel mercato unico nell'ordinamento italiano', pp 14-15, arguing that the new parody exception for works uploaded on content-sharing platforms should not extend to offline uses.

19 Pret. of Rome, 18 November 1966, in *Foro It* 412; Court of Naples 15 February 2000, De Filippo v Altieri in *Dir. D'autore* 2001 457; Court of Milan 29 January 1996, Tamaro v Soc. Comix e Soc. P.D.E, Il Foro Italiano, 1432.

20 The latter requirement has been interpreted as meaning that a parody must achieve a humoristic effect, not being sufficient a mere intention to mock. Federica De Santis (2014) 'Appropriation Art e Diritto D'Autore', PhD Dissertation (University of Milan), p. 111. See also Court of Rome 12 October 2000.

sion leverages on two main arguments, with neither, unsurprisingly, referring to parody as an exception to copyright.

12 According to the first line of reasoning, parodies are not derivative works but fully autonomous creations. This happens because there is no misappropriation of the ideological core of the referenced works, but on the opposite, an overturning of their original meaning.[21] Courts have reinforced this conclusion through an analysis of Article 4 ICS, conferring upon rightsholders the exclusive right of adaptation of their works.[22] They point out that parodies are nothing alike the other forms of elaborations mentioned in that provision, such as translations or cinematographic adaptations. These are mere changes in the medium of communication of the work, but do not concern its message. By contrast, parodies revolutionize the meaning of the referenced work, in other words, they establish a semantic distance with the latter, regardless of the medium used to express them.[23] In addition, some courts have also argued that parodies must not compete commercially with the referenced worked.[24-25] It is, however, unclear whether lack of competition is necessary to prove the semantic distance between the two works or if it constitutes an independent element that courts address when assessing infringement.

13 In this connotation, parody is not an exception because it concerns the delimitation of the scope of copyright protection. Parodies are not derivative works because of their intrinsic difference with the referenced works. To borrow the US terminology, parodies are 'transformative', insofar as they display a new expression, meaning or message that is not traceable in the original work.[26] The case law on appropriation art, i.e. a form of art realized by incorporating previous works to convey a new artistic message, further supports this reading.[27] In this context, courts have ruled out infringement anytime there is a creative transformation of a work into something different, with one ruling explicitly referring to the US fair use doctrine.[28] These judgements thus extend the principles elaborated for parody to any transformative utilization of a work, even when a humoristic intent is missing.[2930] The Italian Supreme Court has indirectly endorsed this line of reasoning, by remarking that the semantic gap between the works is one of the elements to take into account in the assessment of copyright infringement.[31]

14 Notably, Italy is not the only European country to follow this approach. Before the latest amendment to the copyright act introduced a specific parody exception,[32] German courts traditionally dealt with parodies through the application of the 'free use' doctrine (*freie Benutzung*). This principle allowed qualifying a work as an independent creation insofar as it shows sufficient original character so to establish sufficient 'inner distance' from the referenced

21 Court of Naples 27 May 1908, *D'Annunzio v Scarpetta,* in *Foro It.* 1909 n. 18; Pret. of Rome, 18 November 1966, in *Foro It* 412*;* Pret. of Rome, 29 August 1978 in *Dir. Aut.* 1979; Court of Milan 29 January 1996, Tamaro v Soc. Comix e Soc. P.D.E; Court of Naples 15 February 2000, De Filippo v Altieri in *Dir. D'autore* 2001, 471.

22 Article 4 ICS: 'Without prejudice to the rights subsisting in the original work, works of a creative character derived from any such work, such as translations into another language, transformations into any other literary or artistic form, modifications and additions constituting a substantial remodelling of the original work, adaptations, arrangements, abridgements and variations which do not constitute an original work, shall also be protected'. Unofficial translation available at https://www.wipo.int/edocs/lexdocs/laws/en/it/it211en.pdf [Accessed on 10 February 2021].

23 Court of Milan 29 January 1996; Court of Venice, 7 November 2015, Sanguinetti vs Fondazione La Biennale di Venezia and Samson Kabalu.

24 See in particular Court of Naples (1908), Pret. of Rome, 29 August 1978 and Court of Milan 29 January 1996; Court of Milan, 31 May 1999, Warner Chappell Music Italiana S.p.A. c. New Music International S.r.l., Leone Di Lernia, *AIDA*, 2000; Court of Rome, 12 October 2000 in *Dir. Radiodiffusioni*, 2001, p. 67.

25 See Spedicato (2013), pp. 124-5, agreeing on the point.

26 William Fisher (1988) 'Reconstructing the Fair Use Doctrine', *Harvard Law Review* 101(8), p. 1659.

27 See https://www.tate.org.uk/art/art-terms/a/appropriation, [Accessed 03 March 2021].

28 Court of Milan, 14 July 2011, *Giurispr. Comm.* 2013; Court of Venice, 7 November 2015, *Riv. Dir. Ind.* 2018.

29 Court of Milan, 14 July 2011; Court of Venice, 7 November 2015.

30 On the topic see Annapaola Negri-Clementi & Filippo Federici (2017) 'La Salvaguardia del Diritto D'Autore nell'Appropriation Art', *Art & Law* 4, 27-38; see Spedicato (2013), p. 130.

31 See Italian Supreme Court, 19 February 2015, n. 3340 in *AIDA* (2015) 1655; Italian Supreme Court, 26 January 2018, n. 2039 in *AIDA* (2018) 1837. On the topic see, Alberto Musso (2015) 'Il Plagio-Contraffazione Parziale e la Rielaborazione Creativa di Singoli Brani in Altrui Opere Successive: Un Approccio Giuridico in Termini di Funzionalità Estetica', *Lex Mercatoria* 13, p. 60.

32 Act on Copyright and Related Rights, (Urheberrechtsgesetz – UrhG), § 51.

work.[33] Austria, Sweden and the Netherlands have also preferred framing parody under the principles regulating infringement and derivative works.[34]

15 Some have explained the reasoning of the courts by pointing out that, as things stand, the ICS only gave them only two interpretative options.[35] The first one was subsuming parodies under Article 4 to treat them as derivative creations. This would have meant obliging parodists to seek prior authorization and therefore destroying the whole genre, as some courts have pointed out.[36] It should therefore not surprise that courts shied away from this option and embraced the second one, i.e. to treat parodies as fully autonomous creations.[37] This observation however waters downs the *ratio decidendi* of the Courts, describing it more as the result of policy driven considerations than robust legal reasoning.[38]

16 The second line of reasoning is that in the silence of the law, the freedom to engage in parody finds a legal basis in the Italian Constitution and especially in Articles 21 and 33, which guarantee free speech and artistic expression.[39] This is because subjecting parodies to prior consent would unduly curtail the aforementioned rights, which is undesirable and illegitimate in a pluralistic and democratic society. In other words, between the two options of considering parodies as derivative or autonomous creations, the Italian Constitution pushes the interpreter towards the latter, as the most consistent with fundamental rights' doctrines.[40]

II. The legal scholarship

17 Few isolated voices have disagreed with the conclusions of the judiciary, arguing that parodies should be treated as derivative works, at least as long as there is a substantial reproduction of the first work.[41] By contrast, most academics have shared the position of Italian courts.[42] Some have pushed the conclusions of the courts even further. For instance, a few have argued that the freedom to engage in parodies is an expression of the exercise of fundamental rights, thus suggesting a direct application of constitutional provisions, rather than hinging on their radiating effect on copyright law.[43] Others instead

33 Paul Edward Gellller (2010) 'A German Approach to Fair Use: Test Cases for TRIPS Criteria for Copyright Limitations', *Journal of the Copyright Society of the USA* 57, 553-71.

34 Martin Senftleben (2020) 'Flexibility Grace – Partial Reproduction Focus and Closed System Fetishism in CJEU, *Pelham'*, *IIC* 51, 753-60; Martin Senfteleben (2012) 'Quotations, Parody and Fair Use', p 360; J. Rosen (2007) "Copyright and Freedom of Expression in Sweden - Private Law in a Constitutional Context", in Torremans P. (ed) Copyright law: a handbook of contemporary research (Edward Elgar Publishing: Cheltenham), pp 355–372. For a first overview of the implementation of the exception in Europe see Lucie Guibalt, Guido Westkamp et al. (2012) 'Study on the Implementation and Effect in Member States' Laws of Directive 2001/29/EC on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society', [online]. Available at https://dare.uva.nl/search?identifier=200997ce-c8d4-49e9-8fb6-ee874037de9c [Accessed 26 March 2021].

35 Monti (1996) 1426-8

36 Court of Milan 29 January 1996.

37 Monti (1996) 1426-8.

38 In this sense see Vittorio De Sanctis (1990) 'Il Diritto di Satira all'Esame della Pretura di Roma: I Poteri di Riferibilità alla Parodia dell'Opera dell'Ingegno', *Dir. aut.,* 149; Monti (1996), p. 1427; E. Mina (1996) 'Opera Parodistica: Plagio di Opera Letteraria o Autonoma Opera dell'ingegno?', *Diritto Industriale* p. 417.

39 Art 21 of the Italian Constitution: 'Anyone has the right to freely express their thoughts in speech, writing, or any other form of communication'; Art. 33: 'The Republic guarantees the freedom of the arts and sciences, which may be freely taught'. Italian Constitution 1947. Official translation by the Italian Senate. Available at https://www.senato.it/documenti/repository/istituzione/costituzione_inglese.pdf [accessed 30 December 2020].

40 Court of Milan 29 January 1996; Court of Naples 15 February 2000; Court of Milan, 13 September 2004; Court of Venice 7 November 2015.

41 Z.O. Algardi (1978) 'La Tutela dell'Opera dell'Ingegno e il Plagio' (CEDAM: Padova) p. 274; Mina (1996), p. 417; more recently Luca Boggio (2015) 'L'Opera Parodistica tra Proprietà Intellettuale e Diritti della Personalità', *Giurisprudenza Italiana* p. 1143, referring to the primacy of EU law.

42 See for instance Vittorio De Sanctis (1990); Alberto Maria Gambino (2002) 'Le Utilizzazioni Libere: Cronaca, Critica e Parodia', *AIDA* 11, p. 132; Alberto Musso (2008) 'Del Diritto d'Autore sulle Opere dell'Ingegno Letterarie e Artistiche', in *Commentario al Codice Civile Scialoja-Branca* (Zanichelli: Bologna), pp. 43-44; Lorenzo Albertini (2015) 'L'Opera Elaborata e la Questione della sua Titolarità', *Jus Civile* 7, pp. 360-446; Giorgio Spedicato (2018) 'Diritto (o Eccezione?) di Parodia e Libertà d'Espressione' (Persiani: Bologna), p. 95.

43 De Sanctis (1990) 149-51; Vittorio De Sanctis (2002) 'I Soggetti del Diritto d'Autore' (Giuffrè: Milan), pp. 140-1.

suggest that the recontextualization of prior material is sufficient to achieve the semantic distance between the works.[44]

1. Re-conceptualizing parody within the principles governing infringement

18 Some authors have re-conceptualized parodies within a holistic approach to copyright infringement. According to this line of reasoning, infringement does not concern the factual reproduction of copyrighted material but constitutes a multifaceted assessment requiring the balancing of several factors. These include the perception of the work in the eyes of the public, the artistic merit of the work as a standalone creation and the semantic distance between the two works.[45] Some have interpreted the latter requirement as an emphasis on the appropriation of the 'expressive form' of the previous work, i.e. the specific shape or structure through which the author conveys their artistic message.[46] Other possible elements to consider are the amount of work used, the lack of competition between the works and the purpose of the use.[47]

19 In the absence of a legal definition of infringement, some have reinforced this conclusion through systematic considerations. They have found a first normative anchor in Article 2(2) ICS, which protects "musical variations that themselves constitute original works". Under this perspective, the provision would express the wider principle that copyright only covers the parasitic appropriation of previous works and not their transformation into something new and original.[48] However, against this line of reasoning, it is difficult to overlook at the black letter of the law. It is unclear why, if the provision expresses a general principle, the legislator decided to formulate it only in relation to musical works. Furthermore, the relationship between Article 2(2) and 4 ICS remains unexplored, as it is not possible to exclude *a priori* that an original variation does not constitute a derivative elaboration subjected to the consent of the first author.

20 These academics have found a second confirmation in Article 70 ICS, concerning the quotation exception for the purpose of criticisms or review.[49] Indeed, the provision seems to confirm the possibility to reproduce copyrighted material in support of new personal statements,[50] or the principle that no infringement occurs without the appropriation of the 'expressive form' of the previous work.[51] In this sense, parody and quotation would share a common matrix, confirming the freedom to incorporate prior material into a new artistic message, insofar as this does not harm the interest of the rightsholder.[52] Unfortunately, this argument is also not immune from criticism. There is a clear contradiction in elevating quotation to a principle of the ICS when the legislator decided to treat it as an exception. Academics are somewhat aware of this and take issue with the legislative framing of Article 70 in

44 Giorgio Spedicato (2013) 'Opere dell'Arte Appropriativa e Diritto d'Autore', *Giurisp. Comm.* 40(2), p. 123.

45 On the topic see, Paolo Greco & Paolo Vercellone (1974) 'I Diritti sulle Opere dell'Ingegno (UTET: Turin) p. 358; Musso (2015), p. 60; Alessandro Cogo (2016) 'Plagio dell'Opera Musicale', *Giurisprud. It.* 106-8. More vaguely, Vittorio De Sanctis (2003) 'La Protezione delle Opere dell'Ingegno' (Giffrè: Milan) pp. 186-7.

46 Spedicato (2013) p. 121.

47 Spedicato (2013) p. 130, here the inspiration to fair use is evident.

48 Alberto Musso (2008) 'Del Diritto d'Autore sulle Opere dell'Ingegno Letterarie e Artistiche', in *Commentario al Codice Civile Scialoja-Branca* (Zanichelli: Bologna), p. 64; Spedicato (2013), pp. 124-5 and Alessandra Donati (2018) 'Quando L'Artista si Appropria dell'Opera Altrui', *Riv. Dir. Ind.* 67(2), p. 89.

49 Art. 70 ICS: "The abridgment, quotation or reproduction of fragments or parts of a work and their communication to the public for the purpose of criticism or discussion, shall be permitted within the limits justified for such purposes, provided such acts do not conflict with the commercial exploitation of the work; if they are made for teaching or research, the use must have the sole purpose of illustration, and non-commercial purposes". See https://www.wipo.int/edocs/lexdocs/laws/en/it/it211en.pdf [accessed 19 April 2021].

50 Musso (2008) p. 64; Spedicato (2013), pp. 124-5 and Donati (2018), p. 89.

51 Spedicato (2013) pp. 124-5 argues that quotation is permissible because it reproduces copyrighted material to refer to its content/ideas without appropriating the 'expressive form' of the quoted work. See Court of Cassation, 7 March 1997 n. 2089, *Dir. D'Aut.* 1997, 362. However, we do not share this view since: a) if quotations would simply be a matter of referencing content, than courts should reject the exception anytime it would have been possible to engage into a rephrasing of the chosen excerpt. This would make the quotation of scientific or descriptive material impossible; b) there are numerous examples of quotations capturing the aestathic value of the referenced work such as epigraphs, or the incorporations of poetic passages within the one's own text. These should nonetheless being considered licit pursuant Art 70.

52 See Court of Rome 29 September 2008 *AIDA* (2010), 1341.

the ICS.[53] However, if Article 70 truly expressed a general copyright principle, the provision would not be needed in the first place, and reference should be made to the provisions regulating the scope of the exclusive rights rather than its exceptions.[54]

21 Leaving aside the arguments based on Articles 2 and 70 ICS, in short, there are at least three other overriding reasons that *corroborate* the holistic approach to infringement.[55] First, in the absence of a description of 'infringement' in the ICS, if we correctly understand the concept as the violation of the exclusive rights granted to rightsholders, any attempt to draw its contours cannot ignore the definition of the rights that are deemed violated. Accordingly, the violation of the right of reproduction presupposes the 'multiplication' of 'copies' of the work in question.[56] The definition clearly hints that what matters for infringement is the slavish imitation of copyrighted material since the term 'multiplication' stands for the increase in *quantity* or *numbers*,[57] and it therefore suggests that variations in terms of *quality* or *meaning* fall outside the scope of the term. The same goes for the word 'copy', which hints that the right of reproduction protects against *imitations* and not the creative re-elaboration of protected material.[58] Secondly, according to the most recent case law of the Court of Cassation, infringement entails a synthetical assessment, i.e. an overall evaluation of the similarity between the works rather than an analytical comparison of their individual elements.[59] Whereas the reference to doctrines elaborated in the field of trademarks might appear misplaced, here the Court seems to suggest that to assess the similarity between the protected and the infringing works through the eyes of the relevant public. Indeed, it is the latter that purchases the works and who ultimately determines whether they are fungible from a commercial perspective. In this sense, the maxim appears a reiteration of the principle that the lack of economic competition between the works deposes against infringement.[60] Finally, the suggested reading reconnects copyright to the reasons underlying the granting of the exclusive right(s), i.e. a temporary monopoly to incentive the flourishing of arts, science, and culture. Under this perspective, it appears reasonable to deny protection anytime copyright "would stifle the very creativity which that law is designed to foster".[61]

2. The rejection of parody as an exception

22 Established case law sufficiently protects parodists and the legislator should refrain from promulgating a specific exception on the matter.[62] According to this view, an express exception would relegate parody from an overarching principle to a mere exception, which is something to avoid as a matter of principle.[63] There are also pragmatic considerations behind this stance. Commentators fear that the exception approach could open the door towards a restrictive judicial practice, which normally permeates the application of exceptions to IPRs.[64] Likewise, enacting a parody exception would

53 See Spedicato (2013), p. 126.

54 Court of Milan 9 January 1996, refused assimilating parody to quotations.

55 We will see shortly how the judgement of the CJEU in Pelham has shaken this framework.

56 Article 13 ICS: 'The exclusive right of reproduction concerns the multiplication of copies of the work in all or in part, either direct or indirect, temporary or permanent, by any means or in any form, such as copying by hand, printing, lithography, engraving, photography, phonography, cinematography, and any other process of reproduction'.

57 The term has equivalent meaning in Italian and English. See https://www.treccani.it/vocabolario/moltiplicazione/ [accessed 19 April 2021]; https://dictionary.cambridge.org/dictionary/english/multiplication [accessed 19 April 2021]; https://www.merriam-webster.com/dictionary/multiplication [accessed 19 April 2021].

58 The term has equivalent meaning in Italian and English. See https://www.treccani.it/vocabolario/copia2/ [accessed 19 April 2021]. https://www.merriam-webster.com/dictionary/copy; https://dictionary.cambridge.org/dictionary/english/copy, [accessed 19 April 2021].

59 See Italian Supreme Court, 19 February 2015 n. 3340; Italian Supreme Court, 26 January 2018, n. 2039.

60 Please note that this does not entail that the risk of confusion is relevant for the assessment.

61 Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 577 (1994)

62 De Sanctis (2003), p. 220; L.C. Ubertazzi (2012) 'Commentario Breve alla Leggi su Proprietà Intellettuale e Concorrenza' (Cedam: Padova), p. 1512.

63 Gustavo Ghidini (2018) 'Rethinking Intellectual Property: Balancing Conflicts of Interests in the Constitutional Paradigm' (Edward Elgar: Cheltenham), p. 182; Stefania Ercolani (2004) 'Il Diritto d'Autore e i Diritti Connessi. La legge 633/1941 Dopo l'Attuazione della Direttiva 2001/09CE' (UTET: Turin), p. 75; Spedicato (2018) p. 95.

64 Ghidini (2018) 'Rethinking Intellectual Property', p. 182; Gustavo Ghidini (2018) 'Conclusioni' in Quaderni di Alai Italia, p. 183; Spedicato (2018) p. 95.

mean subjecting it to the infamous threestep tests, pursuant to Article 5(5) InfoSoc.[65]

23 Finally, there might also be a perception that the regulation of parody is more a matter of academic debate than pragmatic relevance. In the end, courts have heard cases on parodies in only a dozen of occasions over the past century. This to some extent justifies the preference for a more sophisticated doctrinal construction at the expense of a clear, but academically rougher statutory exception.[66]

C. A critical analysis of the Italian construct on parody

24 Having illustrated the case law on parody and the position of the Italian scholarship on the matter, this section will now provide a critical analysis of the current legal framework. It will question: a) the soundness of considering parodies fully autonomous creations; b) the relevance of the right to adaptation to the regulation of parody, c) the risks of applying constitutional principles and fundamental rights to copyright law.

I. Parodies as fully autonomous creations

25 As seen above, courts have leveraged on the status of parodies as fully autonomous creations to dismiss any infringement proceedings brought against parodists. Even if parodies draw heavily from previous works, they capsize their meaning to such an extent that they fall outside the scope of protection of the works they evoke. In other words, because of existing conceptual and semantic differences, parodies are substantially different from their referenced works and do not fall within the scope of protection of the latter. Two main arguments militate against this construct. The first one hinges on the socalled 'idea-expression dichotomy'. The second and most important one relates to the consistency of the Italian case law with the EU acquis. Finally, there is a question of the utilization of analogy as a (temporary) solution to the lack of specific regulation.

1. The idea-expression dichotomy

26 The idea-expression dichotomy is a defining element of the international copyright system, being enshrined in influential treaties like the TRIPS Agreement and the WIPO Copyright Treaty.[67] At the European level, the Software Directive contains an enunciation thereof,[68] but the dichotomy pervades the whole EU copyright acquis,[69] as well as the Italian legal system.[70] This fundamental principle mandates that copyright protection shall extend to expressions but never to their underlying ideas, therefore excluding procedures, abstract methods or mathematical concepts as such from the scope of the exclusive rights.[71] In other words, copyright protects against the misappropriation of specific expressive forms while leaving free the utilization of generic ideas, including also general plots, artistic styles, or stereotyped characters.[72] In prescribing so, the dichotomy prevents copyright from stagnating creativity by hampering the free flow of ideas.[73]

27 Against this background, the reasoning of Italian courts, or at least some of them, capsizes the relationship between ideas and expressions in the dichotomy: what becomes relevant for infringement is no longer the misappropriation of the expression itself, but of the ideological core therein. In this way, their reasoning defies common logic insofar as it does not provide why the *lack* of appropriation of ideas unexpectedly becomes relevant for the assessment if it is irrelevant for infringement.[74]

65 Ghidini (2018) 'Rethinking Intellectual Property', p. 182; Ghidini (2018) 'Conclusioni' in Quaderni di Alai Italia, p. 96.

66 This emerged from a discussion of the author with some prominent Italian academics in February 2019, in Bologna.

67 Article 9 of the TRIPS Agreement (1995); Article 2 of the WIPO Copyright Treaty (1996).

68 Article 1(2), Directive 2009/24/EC on the Legal Protection of Computer Programs.

69 Roberta Mongillo (2016) 'The Idea-Expression Dichotomy in the US and the EU', *EIPR* 38(12), p. 737.

70 See Giorgio Spedicato (2020) 'Principi di Diritto d'Autore' (Il Mulino: Bologna), p. 41; Marco Saverio Spolidoro (2019) 'I Criteri di Accertamento del Plagio nel Diritto D'Autore', *Riv. Dir. Ind.* 6(1), pp. 584-5. See Italian Supreme Court, 26 January 2018, n. 2039.

71 See for instance WIPO (1978) 'Guide to the Berne Convention', p. 12

72 For a brief recapitulation of the relevant case law in the UK, see Ed Barker and Iona Harding (2012) "Copyright, The Ideas/Expression Dichotomy and Harmonization: Digging Deeper into SAS", *JIPLP* 7(9), 673-9.

73 Mongillo (2016), p. 737.

74 See Monti (1996), p. 1428, emphasizing the weakness on leveraging on the ideological core of parodies. By contrast,

Under this perspective, the choice to leverage on the ideological aspects of parodies is unwise for contradicting a basic tenet of the copyright system.[75]

28 In truth, the above-mentioned holistic approach to infringement does solve the objections based on the dichotomy insofar as it does not blindly emphasize the ideological differences between the two works. Conversely, it fine-tunes the assessment by construing the scope of the exclusive rights in the light of fundamental questions of copyright policy, in particular the necessity to avoid parasitic rent seeking claims and the exercise of private censorship over derivative creativity. Even more importantly, this approach seems consistent with the wording of the ICS insofar as nothing in the statute prevents from carrying out the analysis of infringement by using parameters such as the perception of the interested public or the harm caused to the rightsholder. Despite this, the main problem with this holistic approach now lies in its inconsistency with EU law, as we will see shortly.

2. Inconsistency with EU law

29 Following the most recent judgements of the CJEU, the Italian construct on parody is now an evident deviation from Articles 2, 3, and 4 of the InfoSoc Directive. These constitute measures of full harmonization to be interpreted uniformly throughout the Union.[76] According to the Court, these provisions do not leave room for considerations relating to the meaning and purpose of the use, as well as the lack of harm caused to the rightsholder. As held in *Pelham* in relation to music sampling, the ordinary meaning of 'reproduction' suggests that the only relevant factor for assessing infringement is the objective replication of the copyrighted work or part thereof, and thus even the reproduction of a short sequence of a composition amounts in principle to infringement.[77] As a limit to this finding, the Court held that a reproduction might not amount to infringement when, in exercising the freedom of arts, the user of the sample modifies it "to such a degree that [it] is unrecognizable to the ear in that new work".[78]

30 Despite the Court's statement, it is unclear whether this conclusion is truly the result of a balancing exercise between copyright and fundamental rights. More pragmatically, it seems that no reproduction occurs when it is not possible to recognize in the second work the footprint of the first one.[79] For our purposes, it seems clear that the CJEU's approach, by elevating 'recognizability' as the sole criterion for evaluating infringement, rules out from the assessment any possible consideration as to the semantic/ideological distance between the two works as well the different context in which the borrowed material appears. The emphasis is indeed on the 'factual' reproduction of the first work to be assessed through the eyes of the relevant public.[80] Prominent academics have criticized the reasoning of the CJEU, *inter alia* for writing off the tradition of those member states who followed a holistic approach in assessing infringement. However, they have also pointed out that, as things stand, the teachings of the Court do not leave much room for different interpretations.[81]

31 The CJEU's approach has profound implications for parodies, which by definition establish a strong connection with the referenced works (if not entirely reproduce large parts of it) and thus hardly satisfy the unrecognizability threshold set in *Pelham*. It is therefore clear that the Italian approach is incon-

Spedicato (2013).

75 It must however be noted that foreign courts have also proceeded along similar lines. For instance, in Sweden the Supreme Court has defended the independence of parodies by noting that they serve a different purpose than the original works. Some scholars have however vehemently criticized the judgement, noting that there is little room for the consideration of the purpose of a work in copyright law. See the Swedish Supreme Court in NJA 2005 s. 905. The case is recounted in Lisette Karlsson (2013) 'Copyright and the Parody Problem' (University of Lund: Graduate Thesis), pp. 29-35. Similarly, German courts also used to assess whether parodies subverted the meaning of the original work, at least until they abandoned this line of reasoning in order to comply with the teachings of Deckmyn. See Henrike Maier (2017) 'German Federal Court of Justice Rules on Parody and Free Use', *JIPLP* 12(1), p. 16.

76 See Pelham at 85-6 and Funke Medien at 35-8.

77 See Pelham at 27-30; see also *Infopaq* C 5/08, CJEU (2009) at 57, where the Court held that the reproduction of 11 words constituted infringement.

78 See Pelham at 30-39.

79 To draw a parallel with the US; in this jurisdiction copyright infringement occurs when there is a substantial similarity between the two works, but fundamental rights do not really seem to play any role in this assessment.

80 See also case C-145/10, Painer CJEU (2011), paras. 41–42, 95–99.

81 Senftleben (2020) 759-61; James Parish (2020) 'Sampling and copyright - did the CJEU make the right noises?', *Cambridge Law Journal* 79(1), pp. 32-4; with reference to the AG opinion see Bernd Justin Jütte & João Pedro Quintais (2019) 'Advocate General turns down the music - sampling is not a fundamental right under EU copyright law: Pelham v Hutter', *EIPR* 41(10), 654-657.

sistent EU law. It alters the scope of the exclusive rights granted to the rightsholder and ends up undermining the goal of the InfoSoc Directive to harmonize copyright across the EU.[82] It also violates EU law on the ground that the InfoSoc Directive preempts Member States to implement the corresponding provisions of Berne.[83] This puts Italian courts in a very uncomfortable position, since in the absence of a domestic exception, currently they must either endorse an interpretation that violates EU law or deem parodies as a form of infringement. The following sub-paragraph will show how the recourse to analogy might mitigate this situation.

3. Binary reasoning and analogy

32 For a long time Italian courts seemed stuck in a binary logic, whereby one of the two following options must necessarily hold true: either parodies are autonomous creations or they are derivative works subjected to the consent of the first author.[84] As seen, none of these options is ideal, since the latter unduly restricts free of speech, while the former seems nowadays inconsistent with EU law.

33 However, there are possible ways out of this binary reasoning. A first one is leveraging on the circumstance that the ICS does not explicitly regulate parodies and embark in analogical interpretation of the law. This is the tool expressly devised by the legislator to fill existing gaps in the legal system. It consists of a three-phased process whereby courts must: a) verify the existence of a gap in the legal system; b) identify a legal provision (*analogia legis*) or principle (*analogia iuris*) that regulates an analogous matter and obeys the same rationale;[85] c) check that the identified provision does not have exceptional character or relate to criminal matters.[86] As a tool meant to overcome legislative gaps analogy departs from the ordinary process of interpretation in at least two significant aspects: on one side, it privileges identity of rationales over the linguistic similarity of legal provisions, while on the other it allows courts to resort to general principles instead of specific provisions.

34 In spite of this, the application of analogy to parodies poses several problems, and thus should not surprise that both academics and courts have refrained from taking this path. The first step requires the absence of an applicable legal provision. In this sense, it is possible to undertake an analogical interpretation only as a last resort, when the ordinary means of interpretation leave the matter unregulated or lead to manifestly absurd results.[87] In this sense, analogy entails an historical assessment, insofar as the gap in the legal system and the way to fill it depends on the legal rules applicable at the time of litigation. That is why the first court to adjudicate on parody far back in 1908 had good reasons for not embarking in an analogical interpretation. First, the case revolved around a criminal offense. Secondly, the Court engaged into an analysis of the preparatory works of the then Copyright Act, giving particular emphasis to the 1882 amendment. It concluded that the choice to exclude parody from the list of infringing uses confirmed that parody fell outside the scope of copyright protection. In the analysis of the Court, there was no gap in the legal system but an implicit rule.[88]

35 This line of reasoning does not hold up to nowadays. The last (failed) attempt to regulate parody dates back to 1919, when the legislator decided to leave the matter unregulated and the law has been silent up to nowadays.[89] Until not too long ago, it was the abovedescribed holistic approach to infringement avoided the necessity to appeal to analogy. No gap in the legal system existed as long as courts could resolve the matter by limiting the scope of copyright protection. However, the InfoSoc Directive and its interpretation by CJEU's has created a regulatory void since EU law mandates the considering material reproduction of protected material as the sole element relevant for infringement. There is therefore room to open up to an evolutionary interpretation of the law that leverages on the observation that if the legislator had to confront the matter today, it would have legislated differently, probably by

82 See Recitals 1 and 6 of Directive 2001/29 InfoSoc.

83 See Case *Luksan* C-277/10, CJEU (2012); Mutatis mutandis, see *Football Dataco* Case C-604/10 CJEU (2012) in relation to databases.

84 Monti (1996) 1428.

85 See Art 12(2) of the pre-laws of the Italian Civil Code; Cassazione Civile, 14 February 1994, n. 10699.

86 See Art 14 of the pre-laws of the Italian Civil Code.

87 Court of Cassation, 28 April 1995, n. 4754, in *Giust. Civ. Mass.* 1995, 925; Court of Cassation, 4 February 1985 n. 731, in *Giust. civ. Mass.* 1985, 2.

88 Court of Naples 27 May 1908.

89 Monti (1996) p. 1428.

promulgating an explicit parody exception.[90-91]

36 Another obstacle is the identification of the legal provision to use as a base-reference for regulating parodies. A first problem is motivating why the right to adaptation in Article 4 is not the closest parameter to apply to parodies. Here, the different rationales between parody and other kinds of adaptions might have a role to play in the assessment. As it will be seen shortly, the right of adaptation is meant to extend the reach of copyright to different expressive mediums and not to regulate transformative elaborations. It is also possible to point out that, as a deviation from the idea/expression dichotomy, the right to adaption falls within the prohibition against the analogical application of provisions of exceptional character. Unfortunately, other E&L in the ICS are also unfit reference provisions for parody. First and foremost, because most of them have limiting conditions that would conflict with the teachings of *Deckmyn*.[92] Secondly, because it is controversial whether E&L, being exceptions to a general rule are caught by the prohibition against the analogical utilization of provisions of exceptional character.[93] In the light of the December 2021 ICS amendment, the easiest solution is to rely on the parody exception foreseen for online uses to offline utilizations. Another possibility is appealing to the *analogia iuris* and leveraging on the overarching principle of freedom of expression in Article 21 of the Constitution. A similar solution has for instance been endorsed in relation to the 'right to satire' which normally prevails over the individual right to reputation.[94]

37 Despite this, it is important to stress that analogy must only be a short-term solution to mitigate the impact of the CJEU's case law on the Italian copyright system. Analogy must not become an excuse to postpone legislative intervention on parody for three reasons. First, from a methodological standpoint, analogy by definition is a last resort tool to confront unforeseen circumstances. Second, from an ideological view, analogy confirms the existence of a loophole in the copyright system. Finally, from a pragmatic perspective analogy entails an unnecessary complex regulation of the matter, obliging courts to embark into a multi-layered assessment that can lead to uncertainty and diverging outcomes.

II. The right to adaptation

38 It is also important to clarify the complex relationship between parody and the right to adaptation both at the domestic and international level. Indeed, the argument that parodies are substantially different from the referenced works does not automatically rule out the application of the right of adaptation and the possibility that, therefore, they might infringe upon this right.

1. The right to adaptation at the international level

39 Article 2(3) of the Berne Convention stipulates that "translations, adaptations, arrangements of music and other alterations of a literary or artistic work shall be protected as original works without prejudice to the copyright in the original work", a concept reiterated in Article 12.[95] However, the relationship between the right of adaption and the one of reproduction are a matter of controversy at the domestic, comparative, and international level. Some countries consider the rights of adaptation as a subspecie of the right of reproduction, while other see them as fully independent rights.[96] In any case, the Berne Convention does not seem to

90 On evolutionary interpretation, see Court of Cassation 9 September 2007 n. 17579 and Court of Cassation 7 February 1996 n. 978.

91 Please note that the amendments of the ICS that will follow the implementation of the DSM Directive only concern the online environment and do not take into consideration the impact of the recent CJEU case law on the Italian copyright system.

92 See for instance, Art. 70 ICS on quotation.

93 On the complex topic of what constitutes a provision of exceptional character see Marcello Maria Fracanzani (2003) 'Analogia e Interpretazione Estensiva nell'Ordinamento Giuridico', *Collana Della Libera Università Mediterranea Jean Monnet*. Paola Spada (2018) 'Riflessioni Conclusive', in *Quaderni di Alai Italia*, p. 189, argues in favour of analogy anytime there is no endangerment of the interest of the copyright holder and the exception favors the flourishing and dissemination of creativity. On a similar vein, see Spedicato (2020) p. 198. *Contra* De Sanctis (2003) p. 204 and, most importantly, Court of Cassation 7 March 1997 n. 2089 *Dir. D'Aut.* 1997, 362.

94 Mutatis mutandis, Courts have leveraged on free speech to affirm that the right to satire prevails over reputation. See Court of Cassation, 22 November 2018, n. 30193; Corte of Cassation, 5 February 2014, n. 5499.

95 Article 2(3), Berne Covention; Art. 12: Authors of literary or artistic works shall enjoy the exclusive right of authorizing adaptations, arrangements and other alterations of their works'.

96 See Samuel Ricketson (1987) 'The Berne Convention for the Protection of Literary and Artistic Works' (Kluwer: United Kingdon), p. 389; See Jongsma (2017) pp 668-9.

bind countries to one of these systematic choices.[97] Importantly, the second approach leads to the question of whether the two rights are mutually exclusive, i.e. whether the qualification of a work as an adaptation rules out the application of the rules on the right of reproduction.[98]

40 Under the 'autonomous approach' the two rights clearly serve different purposes. The right of adaptation goes beyond the right of reproduction by granting protection over new expressive elements that are untraceable in the original work.[99] The history of the right to adaptation in the US helps clarifying this point. In 1907, the US Supreme Court held that a perforated roll used to recreate the sound of a musical composition did not infringe upon the copyright on the underlying music. Copyright only protected the particular form of expressions of ideas and the change of medium consequently implied a difference in the expression. Copyright protected against the utilization of the roll to play the music in public, but the distribution of the paper roll was *per se* lawful.[100] This led the US Congress to grant upon authors the exclusive right to transform the work into a different medium. The effects of the amendment was soon felt in courtrooms, with courts concluding that the author of a book enjoyed the exclusive right over its cinematographic dramatization or that making a tridimensional toy out of an animated character would infringe the right of adaptation of the cartoonist.[101] Under this perspective, the right to adaptation is itself an exception to the idea/expression dichotomy, since it grants rightsholders control beyond the original form expression in which their work was first embodied.

41 This excursus also suggests that the rights are not mutually exclusive and *can* overlap in specific cases. In other words, a work might be at the same time an adaptation and a reproduction of a pre-existing creation. Indeed, there would be quite a contradiction in transforming a provision initially devised as *enhancing* the scope of copyright protection beyond the first embodiment of the work into a limitation of the right of reproduction. This reasoning seems especially relevant at the European level, since the InfoSoc Directive does not regulate the right of adaptation. In this context, some have argued that classifying a use as an adaptation does not automatically rules out a violation of the right of reproduction and have consequently proposed a distinction between 'pure' adaptations (e.g. a translation) and those entailing the duplication of protected subject matter. While the former fall outside the scope of the InfoSoc Directive, the same does not hold true for the latter since these encroach upon Article 2 thereof.[102]

2. The right of adaptation in Italy

42 The implicit position of Italian courts and academics is that the assessment of the right of adaptation does not rule out the infringement of different exclusive rights and especially the right of reproduction. As to whether parodies fall within the former, courts have leveraged on a teleological interpretation of the non-exhaustive list of elaborations in Article 4. This hints that the provision only regulates the transposition of a work into a different medium but does not concern transformative elaborations that revolutionize the meaning of the first work.[103-104]

43 Regardless of whether this outcome is correct, this line of reasoning seems methodologically flawed. It tries to secondguess the extent of the non-exhaustive list of adaptations in the provision beyond non-exemplified cases.[105] However, it is possible to argue otherwise that the inherent function of a non-exhaustive list is to clarify which cases unambiguously fall within the literal scope of a provision, while leaving to the courts the evaluation of unstated cases. In carrying out this task, courts should not depart from the ordinary canons of interpretation and, first among them, the ordinary meaning of legislative text. Against this background, it is striking that courts did not investigate whether the concept of parody falls within the ordinary

97 Silke Von Lewinski (2008) 'International Copyright Law and Policy' (Oxford University Press: Oxford), p. 143.

98 In this sense Ercolani (2004), p. 75; and Senftleben (2020).

99 Paul Goldstein (1983) 'Derivative Rights and Derivative Works in Copyright" (1983) *J. Copyright Society' USA* 30, p. 217

100 See White-Smith Music Publishing Co. v. Apollo Co. 209 US 1 (1908).

101 See Amy B. Cohen (1990) 'Copyright Law and the Myth of Objectivity: The Idea-Expression Dichotomy', *Indiana Law Journal* 66(1), p. 201-4 and the case law cited therein.

102 Rosati (2014) p. 21.

103 This seems in particular the reasoning of the Court of Milan 29 January 1996.

104 In the literature see, Emanuele Santoro (1967) 'Brevi Osservazioni in Tema di Parodia', *Il Diritto d'Autore*, p. 1-15; Alberto Musso (2009) 'Diritto d'Autore sulle Opere dell'Ingegno, Letterarie e Artistiche' in Scialoja e Branca (eds) Commentario del Codice Civile (Zanichelli: Bologna), p. 43.

105 According to Giacomo Guglielmetti (1996) 'Case note on Court of Milan', 29 January 1996, *AIDA* p 677, there is no valid reason to exclude parodies from the reach of Art. 4.

meaning of "creative elaboration of the work", i.e. the very definition offered by Article 4. Instead, they entirely skipped this fundamental phase of the interpretative process, to jump to a systematic conceptualization of the list of adaptations in the provision. In doing so, they privileged a systematic interpretation over a literary one and this seems a questionable hermeneutical choice.[106] Instead courts should have emphasized the ambiguity of the term 'elaborazione' (elaboration), and *then* indulge into an analysis of the context and history of the provision. For instance, some dictionaries define 'elaborations' or 'to elaborate' as the act of expanding or developing a content, which suggest that the term presupposes a certain degree of conceptual identity between the original work and its elaboration.[107] This definition is strikingly different from 'rielaborare' (re-elaborate), which does not simply stand for elaborate for a second time but 'to elaborate through different criteria and for different purposes'.[108-109]

III. The impact of constitutional principles on the copyright act

44 The argument that subjecting parodies to prior authorization would curtail the constitutional freedoms of speech and artistic expressions is undoubtedly compelling. Nevertheless, there are both formal and substantive reasons against invoking constitutional provisions to rule on parody.

45 The first objection relates to the complex and unsolved question of the direct applicability of constitutional provisions to civil proceedings between private parties. While it is impossible to delve into this matter here, we share the stance that courts should not apply abstract constitutional principles to interpret ordinary statutes regulating horizontal relationships between individuals.[110] The Constitution is a standard to evaluate the legitimacy of secondary legislation, so to impose a limit over the discretion of lawmakers, who cannot violate constitutional principles and the fundamental rights embed therein. Reasoning otherwise despoils the Constitutional Court of its institutional function and therefore overhauls the architecture of the Italian constitutional order for what concerns the competence of different judicial bodies. This solution can also lead to unpredictable or altogether discretionary outcomes, insofar as courts rely on abstract and undefined legal principles that are not fit to settle concrete cases.[111-112]

46 The caselaw on parody confirms these concerns. Courts have referenced only some of the constitutional rights relevant in the matter. As well known, free speech can be limited by countervailing rights and interests, including intellectual property. This is of particular relevance considering that IP finds a constitutional basis on several fundamental rights, including the promotion of art and the protection of both property and labor,[113] values that all militate in favor of the plaintiff.[114] In reality, it is possible to reframe this criticism under a wider observation: the disregard for the principle of proportionality. This

106 Please consider that the "ordinary meaning" of the law and 'the intention of the legislator' are the two main canons of interpretation in the Italian legal system, pursuant to Art. 12 of the "pre-laws" of the Italian Civil Code.

107 See for instance Vocabolario Treccani: 'To develop or carry out a project or a work through a careful coordination and transformation of its basic elements until the attainment of the intended result'. Available at https://www.treccani.it/vocabolario/rielaborare/ [accessed 21 April]. Translated by the author. Similarly, Cambridge Dictionary, https://dictionary.cambridge.org/dictionary/english/elaboration [accessed 21 April].

108 Vocabolario Treccani: https://www.treccani.it/vocabolario/rielaborare/ [accessed 21 April].

109 Another problematic feature is the possible difference of scope between the right of adaptation as construed by Italian courts and Arts. 2(3) and 12 of the Berne Convention. The latter seem to treat any 'alteration' of the work as falling within the scope of the right of adaptation, including original ones such as parodies. See See WIPO (1978) 'Guide to the Berne Convention for the Protection of Literary and Artistic Works', pp. 77; Ricketson (1987) p. 398; Sam Ricketson & Jane Ginsburg (2005) 'International Copyright and Neighboring Rights. The Berne Convention and Beyond', I, (Oxford University Press: Oxford), at 11.34; Von Lewinski (2008), p. 143.

110 A notable example of 'concrete' rather than abstract constitutional prescription is Art. 31 of the Italian Constitution. The provision prescribes that the employee is entitled to a fair remuneration. See Giovanni D'Amico (2016) 'Problemi (e limiti) dell'Applicazione Diretta dei Principi Costituzionali nei Rapporti di Diritto Privato (in Particolare nei Rapporti Contrattuali)', *GiustiziaCivile.com* 3 [online]. Available at https://giustiziacivile.com/giustizia-civile-riv-trim/problemi-e-limiti-dellapplicazione-diretta-dei-principi-costituzionali-nei#testo-8 [Accessed on 18 February 2021].

111 D'Amico (2016); Federica Mannella (2010) 'Giudice Comune e Costituzione: Il Problema dell'Applicazione Diretta del Testo Costituzionale', *Federalismi.it* 24, 1-23.

112 For instance, in Germany before the question was referred to the CJEU in Pelham, it was the Constitutional Court to elucidate the relationship between sampling and fundamental rights. See *Metall Auf Metall*, 31 May 2016.

113 See Constitutional Court, 6 April 1995 n. 108, *AIDA* 1995, 297.

114 Spedicato (2013), p. 124; Guglielmetti (1996), pp. 677-8.

is the standard tool to adjudicate the legitimacy of a provision limiting fundamental rights. In short, proportionality consists of ascertaining whether a) the limiting provision obeys a legitimate interest, b) no less restrictive measure is available to safeguard the interest pursued by the law, and c) the measure does not disproportionally exceed what is needed to pursue the interest in question.[115] A proportionality assessment pushes towards concluding that whereas the ICS aims at protecting property, extending its scope to parodies is neither necessary nor proportionate with the goal of the statute, insofar as parodies do not harm the moral or economic interest of rightsholders. In these regards, the application of a proportionality test from the Constitutional Court could lead to a *de facto* amendment of the ICS: the declaration of its unconstitutionality insofar as it does not foresee an exception for parody. The Constitutional Court is not new to this kind of creative judgement, having in the past deemed a statute unconstitutional for what it does not stipulate, rather than for its explicit provisions.[116]

IV. Summary of key results

47 The above discussion tried to debunk the main arguments in support of treating parody as a principle relating to infringement. It submitted that considering parodies as autonomous, non-infringing creations by leveraging on the conceptual and semantic differences between the works creates important frictions with some of the cornerstone principles of copyright law, is methodologically flawed and, most importantly, is nowadays inconsistent with EU law. By contrast, it is *in principle* possible to agree with the finding that parodies do not violate the right to adaption, even though the reasoning of the courts in this regard seems hermeneutically skewed, which also seems to apply to a constitutionally oriented interpretation of the ICS.

D. Declassing parody from a principle to an exception: Legal problems and false assumptions

48 Having dissected the case law on parody, it is now time to turn the attention to the claim that implementing a statutory exception would amount to downgrading parody from an overarching principle to a mere defense against infringement and that this would inevitably stifle creativity by providing more restrictive rules for parodists. A first counter-argument against the downgrading narrative relies on common logic: an exception would be an *addition* to the principles on copyright scope and infringement and not a downgrading. Pragmatically, it would offer parodists a double layer of protection against infringement claims. This is of particular importance, considering that defenses leveraging on the scope of protection and on E&L have different contours and one might succeed where the other fails. The Netherlands and, more recently, Germany have for instance followed this route, providing for an exception in addition to the rules on the scope of protection.[117] In any case, the connotation of parody as a principle remains ambiguous and different objections arise depending on whether we qualify parody as a copyright or human rights principle.[118]

I. Parody as a principle of copyright law

49 Under the first angle, parody concerns the limits to the scope of copyright protection.[119] As seen earlier on, the main problem with this approach relates to its compatibility with EU law. An ancillary consideration relates to the thin line between exceptions and limitations. Traditionally, while limitations delineate the scope of copyright, exceptions are defense-type rules that grant immunity against conducts that would otherwise constitute infringement.[120] This difference entails pragmatic consequences such as the burden of proof, which for defenses falls entirely

115 See for instance the former President of the Italian Court of Cassation, Giovanni Mammone (2018) 'The Relationship between the Constitutional Courts and the Supreme Courts - The Italian Experience' [online]. Available at www.cortedicassazione.it/cassazione-resources/resources/cms/documents/relazione_Rete_Presidenti_Corti_UE-Karlsrhue_2018.pdf [Accessed 18 February 2021].

116 See for instance, Danilo Diaco, 'Le Tipologie Decisorie della Corte Costituzionale attraverso gli Scritti della Dottrina', Corte Costituzionale: Quaderno Processuale del Diritto di Studi' [online]. Available at https://www.cortecostituzionale.it/documenti/convegni_seminari/STU%20296.pdf [Accessed 21 January 2021]. See for instance Constitutional Court, 5 May 1988, n. 501.

117 See Jongsma (2017); Senftleben (2012); See German Copyright Act, § 23(1) and § 51.

118 See Lorenzo Albertini (2015) 'L'Opera Elaborata e la Questione della sua Titolarità', *Jus Civile* 7, p. 364.

119 In this sense, Musso (2015), 60.

120 Annette Kur (2011) 'Limitations and Exceptions under The Three-Step Test - How Much Room to Walk the Middle Ground?' in Kur (ed) Intellectual property in a fair world trade system (Edward Elgar Publishing: Cheltenham), p. 212; Spedicato (2020) p. 191.

upon defendants, and the tendency to construe exceptions more narrowly than exclusions.[121]

50 However, both the TRIPS and the InfoSoc Directive refer to the two concepts interchangeably and the same applies to the ICS. In any case, at the European level exceptions and limitations share a common legal regime, including the application of the 3ST.[122] Some academics have argued that the E&L in the InfoSoc Directive represent either internal limitations of the exclusive rights or the expression of heterogeneous rights and interests of users or both of these options.[123] For instance, while it is better to conceptualize the exception for temporary, technologydictated reproductions as an internal limitation of the right of reproduction, the exceptions for public libraries or to the benefit of people with a disability pursue reasons of policy welfare alien to the copyright system.[124] Against this background, the parody exception might be an expression of both internal and external interests, even though the CJEU case law seems to favor the second understanding. At any rate, qualifying parody as a limitation does not rule out Article 5 InfoSoc Directive.

II. Parody as a constitutional principle

51 The necessity not to downgrade parody from a constitutional principle to ordinary law is perhaps a reference to the so-called hierarchy of legal sources, which sees constitutional provisions at the top of the ranking. The hierarchy is one of the tools to solve the conflicts between different legal rules. It also ensures that the legislative power does not encroach upon citizens' fundamental rights and overarching constitutional principles. Under this perspective, the hierarchy has no role to play in relation to parody as an exception to copyright, insofar as this would not be in conflict with the Constitution and that both the rule (copyright) and the exception (parody) enjoy equal ranking.

52 Alternatively, the rejection of the exception approach might be an attempt to emphasize the nature of parody as a 'fundamental right', finding its *raison d'être* in the ontological value of the human being. By contrast, an exception is a mere defense against infringement and obeys contingent reasons of public policy. However, this line of reasoning seems now obsolete and is being progressively replaced by a new approach that sees E&L as a concretization of constitutional principles rather than their downgrading. In this sense, E&L specify the mode of application of fundamental rights, sparing the courts the hurdle of relying on broad, abstract and ambiguous principles. Moreover, they also set the boundaries for the application of the exceptions, allowing the legislator to strike the proper balance between the interests of the involved parties.[125]

1. E&L and constitutional rights: Indications from the EU

53 The EU legislator clearly endorses this latter understanding of the relationship between E&L and fundamental rights. For instance, the Directives on Trade Secret and Copyright in the Digital Single Market both describe E&L as the preferred tool to balance the two sets of rights.[126] A statement of this kind is missing in the InfoSoc Directive, which is contemporary to the EU Charter of Fundamental Rights and precedes the following constitutionalization trend of EU IP law. This has not refrained the CJEU from portraying E&L as the weapon of choice of the EU legislator in balancing IP and fundamental rights.[127] The Court has leveraged on the linkage between the two sets of rules to push for a broader interpretation of E&L, within the boundaries imposed by the InfoSoc Directive. The CJEU has reinforced this conclusion by pointing out that E&L are not mere defenses against infringement but that they grant fullfledged rights

121 Kur (2011), p. 212.

122 See Article 13 of the TRIPS Agreement (1995); Art. 5 of Directive 2001/29 (InfoSoc) and Art 71^{nonies} ICS.

123 See Maurizio Borghi (2020) 'Exceptions as Users' Rights in EU Copyright Law', CIPPM / Jean Monnet Working Papers No. 06-2020, p. 79.

124 See Arts. 5(2)(c) and 5(3)(b) InfoSoc Directive.

125 See also the German Federal Supreme Court in Germania 3 at 19-23 in Elizabeth Adeney and Christoph Antons (2013) 'The Germania 3 Decision Translated: The Quotation Exception before the German Constitutional Court', *EIPR* 35(11) 646-657, where the Court interpreted the quotation exception in the light of the Constitution. Jan Nordemann & Viktoria Kraetzig, 'The German Bundesgerichtshof changes its concept of parody following CJEU Deckmyn v. Vrijheidsfonds/ Vandersteen', Kluwer Copyright Blog http://copyrightblog.kluweriplaw.com/2016/11/03/the-german-bundesgerichtshof-changes-its-concept-of-parody-following-cjeu-deckmyn-v-vrijheidsfonds-vandersteen/ [Accessed 3 February 2021].

126 See Recital 19 and Article 5 of Directive 2016/943; see Recital 70 and Arts. 17(7) and 17(10) of Directive 2019/790.

127 Spiegel Online at 43; Funke Medien at 55-58 and 64.

to their beneficiaries.[128-129] This rhetoric opens the door to a proportionality assessment, whereby in applying E&L courts must also ensure the respect of fundamental rights.[130] Another salient point is that the CJEU has forbidden Member States to rely on their constitutions to introduce new E&L beyond the exhaustive list foreseen in Article 5 InfoSoc. Reasoning otherwise would inevitably endanger the effectiveness of the Directive in relation to its objective of harmonizing copyright across Europe.[131]

54 To recapitulate, it is possible to draw two intertwined principles from the CJEU case law. First, domestic rules, even of constitutional ranking, cannot undermine the effectiveness of EU law and the harmonizing push of the InfoSoc Directive.[132] Secondly, the devised mechanism to curtail the scope of the exclusive rights vis-à-vis fundamental ones is the list of E&L contained in Article 5 InfoSoc, with all its limits and faults.[133] Thus, it is not possible to rely on the constitution to impose external constraints on copyright beyond what foreseen by that provision.[134] These principles bind both governments and courts. The former can exercise some discretion in the implementation of E&L in national law, as long as the related measure does not constitute a case of full harmonization and they comply within the limits set in the InfoSoc Directive.[135] The latter should ensure that their interpretation of E&L does not conflict with fundamental rights, in line with the tradition of their legal system. However, national courts remain bound by the black letter of the provision and its objective.[136]

55 Against this background, the position of Italy on parody does not introduce a new exception beyond what foreseen in the InfoSoc Directive, since the instrument expressly contemplates 'parody, caricature and pastiche' in Article 5(3)(k). Nevertheless, it overhauls the architecture of the InfoSoc directive. Indeed, it relies on the Constitution as a way to bypass the prism of Article 5 and to circumvent the (alleged) restrictive effect of that provision. This approach is clearly inconsistent with EU law as recently interpreted by the CJEU.

2. Systematic considerations

56 A last observation rests on systematic analysis. Whereas courts and academics have stressed the status of parody as an overarching principle, their reasoning does not extend to another important freespeech related exception: quotation. Not only does the ICS codify an explicit exception but it also provides for an overly restrictive regulation, e.g. by allowing quotations only for non-commercial teaching and scientific research purposes.[137] The regulation of quotation goes beyond the minimum requirements prescribed by the InfoSoc Directive and the Berne Convention.[138] This different treatment is puzzling, now even more in the light of the latest DSM Copyright Directive. The latter portrays both parody and quotation as equally important for the free flow of ideas, qualifying both of them as mandatory exceptions for content uploaded on content sharing platforms.[139]

III. Restrictive interpretation

57 The concern that a statutory exception would lead to a narrow interpretation of parody seems to be an exaggeration—in principle, because the CJEU has clarified that there is no obligation to interpret E&L narrowly, at least when fundamental rights are involved. From a pragmatic standpoint, this is because the Italian approach paradoxically leads to more stringent results than relying on the corresponding InfoSoc exception.

128 Spiegel Online at 50 and Funke Medien at 70.

129 See also De Sanctis (2003) p. 218

130 Spiegel Online at 59 Funke Medien at 76.

131 Spiegel Online at 40-7: Funke Medien at 53-64.

132 Spiegel Online at 47; Funke Medien at 30.

133 Spiegel Online at 43-5; Funke Medien at 42-58.

134 For some literature see: T. Snijders and S. van Deursen (2019) 'The Road Not Taken – the CJEU Sheds Light on the Role of Fundamental Rights in the European Copyright Framework – a Case Note on the Pelham, Spiegel Online and Funke Medien Decisions', *IIC* 50(9), p. 1189; BJ Jutte (2019) 'CJEU Permits Sampling of Phonograms under a de minimis Rule and the Quotation Exception' *JIPLP* 14(11) p. 828; Christoph Geiger and Elena Izyumenko (2020) 'The Constitutionalisation of Intellectual Property Law in the EU and the Funke Medien, Pelham and Spiegel Online Decisions of the CJEU: Progress, but Still Some Way to Go!', *IIC* 51(3), pp. 282-289.

135 Spiegel Online 30-39; Funke Medien at 42-54.

136 Spiegel Online 31-9, 50-9; Funke Medien at 68-76.

137 Article, 70 ICS.

138 See Article 5(3)(d) of the InfoSoc Directive; see Article 10(1) Berne Convention.

139 See Article 17(7), Directive 2019/970.

1. Restrictive interpretation of E&L

58 It is true that, according to settled case law, the CJEU normally engages in a narrow interpretation of the provisions of a directive that derogate from a general principle established therein.[140] In IP-related instruments, the CJEU even reinforces this approach by venturing into teleological interpretations, whereby the Court emphasizes that EU legislators intended to grant a high level of protection to rightsholders.[141] Italian courts have endorsed the same principle, deeming exclusivity as the norm and exceptions as narrowly crafted defenses derogating therefrom.[142]

59 Despite this, the restrictive interpretation of E&L is not an obligated route. In both the EU and Italy, systematic and teleological interpretations, from which the principle of the narrow reading of exceptions descends, are ancillary to black letter interpretation. Only when the literary meaning of a provision is unclear or leads to absurd or unreasonable results should courts engage in systematic and teleological considerations.[143] This is evident in *Deckmyn*, where the CJEU explicitly discarded a restrictive reading of the parody exception by ruling that Member States could not impose on parody other limitations beyond the ones deriving from the everyday meaning of the provision.[144] As such, parodies do not have to possess an original character of their own, display noticeable differences from the original or mention the source of the parodied work. A domestic statute providing for these or any other additional requirements is inconsistent with EU law.[145] In this case, the ordinary meaning of the law also guaranteed the need for harmonized regulation across Europe, which might be endangered in case of differing implementations.

60 Furthermore, the CJEU has counterbalanced the push towards a narrow interpretation of E&L by assigning them the status of full-fledged rights.[146] This means that they are not subordinate to the exclusive rights of copyright holders, but that both claims stand equal and courts must balance them properly. Academics have also endorsed this reading. They have emphasized that construing E&L as rights better captures their fundamental role in copyright statutes, reflects the importance of users and their contribution in the copyright ecosystem and leads to a more liberal interpretation of exceptions.[147] In this way, E&L also gain a positive connotation by imposing a duty not to interfere with the use of a work covered by an exception.[148]

IV. Parody as a principle: more restrictive than as an exception?

1. Requirements to qualify a work as a parody

61 The concerns over the potential narrow reading of an exception lose credibility once we compare the Italian construct with the teachings of *Deckmyn*. It is indeed possible to trace in the domestic case law at least three additional restrictive requirements. These are: a) the absence of competition between the twoworks,[149-150] b) the need for parodies to show original character on their own,[151] and c) the necessity

140 See *Kapper* C-476/01, CJEU (2004) at 72; *Commission* v *Spain* C36/05, CJEU (2006) at 31; *Infopaq International* C5/08, CJEU (2009) at 57; *ACI Adam BV and Others v Stichting de Thuiskopie*, C435/12 CJEU (2014) at 23.

141 See *SGAE,* C-306/05 CJEU (2006), Opinion of the AG Sharpston, 26 and the Judgment, 26. See also *ITV Broadcasting* C-607/11, CJEU (2013) at 20.

142 Constitutional Court, 6 April 1995 n. 108; Court of Cassation, 7 March 1997 n. 2089, *Dir. D'Aut.* 1997, 362; Court of Appeal of Milan 21 March 2000, *AIDA* 2000, 930.

143 Giulio Itycovich (2009) 'The Interpretation of Community Law by The European Court of Justice', *German Law Journal* 10(5), pp. 550-554; Marcella Favale, Martin Kretschmer, and Paul C. Torremans (2016) 'Is there an EU Copyright Jurisprudence? An Empirical Analysis of the Workings of the European Court of Justice', *Modern Law Review* 79(1), pp. 31-75.

144 See Deckmyn at 22.

145 See Deckmyn at 21.

146 *Technische Universität Darmstadt v Eugen Ulmer*, C-117/13 (2014) at 43-44; Spiegel Online at 50-56; Funke Medien at 70-76.

147 Guy Pessach (2011) 'Reverse Exclusion in Copyright Law – Reconfiguring Users' Rights' (2011), Available at SSRN: https://ssrn.com/abstract=1813082 (last accessed 28 July 2020), p. 4.

148 See Maurizio Borghi (2020) 'Exceptions as Users' Rights in EU Copyright Law', *CIPPM Jean Monnet Working Papers*, No. 06-2020, p. 2.

149 See in particular Court of Naples (1908), Pret. of Rome, 29 August 1978 and Court of Milan 29 January 1996; Court of Milan, 31 May 1999, Warner Chappell Music Italiana S.p.A. c. New Music International S.r.l., Leone Di Lernia, *AIDA* (2000).

150 See Boggio (2015) p 1144, suggesting that this requirement is inconsistent with EU law.

151 See Pret. of Rome, 29 August 1978 and Court of Milan 29 January 1996; Court of Milan, 31 May 1999.

to overturn the meaning of the referenced work, or at least to establish a semantic distance between the two works.[152] Some have even hinted that the latter entails ascertaining whether the parody achieves the intended humoristic result, being the mere intent to mock insufficient.[153] All these requirements violate the principles expressed in *Deckmyn*, by providing for an overly restrictive regulation of the exception.[154] They might also perplex the application of the law, insofar as the assessment of whether a work achieves a humorous result is inherently subjective.[155]

62 By contrast, Italian courts have not endorsed the so-called 'necessity test', i.e. the evaluation of the proportionality between the amount of the borrowed work and its role in achieving the intended humorous effect.[156] On their side, academics distinguish between genuine parodies in which the amount of the reproduced work is immaterial for the assessment and bad faith attempts of disguising infringement through minor elaborations of the work.[157][158] However, qualifying parody as an exception would most likely lead to the same outcome.[159] This seems confirmed both by the wording of Article 5(3)(k) as well as by systematic considerations. In particular, it is noteworthy that unlike other E&L in the provision, parody does not require the use of the work to be limited to the extent required by the specific purpose.[160]

63 A comparative analysis confirms that subsuming parodies under the principles relating to the scope of protection leads to more restrictive results than an exception. In Germany, the application of the 'free use' doctrine to parodies led courts to require them to be 'antithetical' to the referenced work. Consequently, the humoristic intent had to be directed against the referenced work itself (target parody) but not towards a third work, person or topic (weapon parody). The German Supreme Court has now modified its approach to allow also for weapon parody, to conform to the principles of *Deckmyn*. This marks an evolution of the legal concept of parody in a more liberal sense.[161] Other restrictive requirements applied by foreign courts include necessity tests, the need for parodies to be original, the absence of confusion between the two works and the absence of the intention to obtain a competitive advantage.[162-163]

2. The hard case of parodies of musical works

64 A complex case concerns composite works made of separable copyrightable elements, and especially songs consisting of lyrics and music. The dilemma

152 Pret. of Rome, 18 November 1966; Court of Naples 15 February 2000; Court of Milan 29 January 1996.

153 Guglielmetti (1996), p. 677; De Santis (2014), p. 111; Alessandra Donati (2018) 'Quando L'Artista si Appropria dell'Opera Altrui', *Riv. Dir. Ind.* 67(2), p. 93. This seem confirmed by Court of Rome, 12 October 2000.

154 See also Jongsma (2017), pp. 652-82; Please note that according to Rosati (2015) 'Just a Matter of Laugh?', the CJEU did not clarify whether parody must achieve a humorous result or if an intention to mock suffice for the assessment.

155 In this sense, the argument against assessing the humoristic result of a parody is analogous to the one against assessing the aesthetic value of a copyrighted work: if courts must not become the arbitrators of what is art, then they should not equally become the ones of what is humor.

156 See for instance Court of Naples, 27 May 1908 and Court of Milan 29 January 1996.

157 Monti (1996), p. 1430; Spolidoro (2019), p. 591; *contra* Guglielmetti (1996) p. 687.

158 In the Netherlands, necessity tests have led to restrictive outcomes. See Senftleben (2012) pp 361-64.

159 See for instance Opinion of Advocate General Cruz Villalón, Deckmyn C-201/13 at 50-56.

160 See for instance Article 5(3)(a) and 5(3)(d), respectively on teaching and quotation.

161 See German Federal Supreme 'Auf fett getrimmt' 28 July 2016, I ZR 9/15. For commentary, Jan Nordemann & Viktoria Kraetzig, 'The German Bundesgerichtshof changes its concept of parody following CJEU Deckmyn v. Vrijheidsfonds/Vandersteen', Kluwer Copyright Blog http://copyrightblog.kluweriplaw.com/2016/11/03/the-german-bundesgerichtshof-changes-its-concept-of-parody-following-cjeu-deckmyn-v-vrijheidsfonds-vandersteen/ [Accessed 3 February 2021]; Henrike Maier (2017) 'German Federal Court of Justice Rules on Parody and Free Use', *JIPLP* 12(1), pp. 16-7.

162 See for instance Senftleben (2012) 'Quotation, Parody, and Fair Use', p. 362; and Jongma (2017), pp. 655-64, and the case law cited therein.

163 In Spain the same restrictive outcomes depends on a narrow legislative drafting of the parody exception. Art. 39 of the IP Act prescribes: 'The parody of a work made available to the public shall not be deemed a transformation that requires the author's consent, provided that it involves no risk of confusion with that work and does no harm to the original work or the author thereof'. On the topic see Mario Sol Muntañola (2005) 'El Régimen Jurídico de la Parodia' (Marcial Pons: Madrid). The same goes for France and Belgium, see Jongma (2017) 655-64.

is whether the overturning effect or the semantic distance must exist in relation to all the elements of the parodied work or only to some of them. Unsurprisingly, this scenario has led to conflicting rulings. Some courts have affirmed that parodists cannot reproduce the melody of a song if they only replace its lyrics, attaching a greater value to the melodic element of a song over its literary part. This is because it is impossible to deny that the two works are in competition if they are identical in terms of melody and arrangements.[164] Other courts have opined otherwise, concluding that the replacement of the lyrics suffices to overturn the meaning of the parodied work.[165] Commentators have praised the latter approach. They have emphasized that the former would *de facto* impede parodying songs and pointed out that the ICS qualifies songs as 'composite works', characterizing music and lyrics as inseparable esthetic elements.[166] In other words, the matter depends on whether the different components of the music must be perceived as autonomous entities or mere facets of a single unity, an indivisible creation.[167]

65 However, this argument does not bring us very far. It is incapable of dealing with synchronizations of autonomous works, which might have separate esthetic value and belong to different rightsholders. Cinematographic works, for example, frequently incorporate preexisting musical tracks and popular songs as background music.[168-169] In these cases, it is difficult to argue that parodies of audiovisual works ridicule background music if their irony only targets the visual component of the work or other features such as its characters, dialogues, or plot. Even the holistic approach to infringement endorsed in the literature does not lead to optimal results. Indeed, if there is any good reason to affirm that the act of synchronization has transformative character then the same reasoning should hold true for the first music synchronization into the later parodied work. Either both synchronizations create an entirely new message or they do not. In fact, the latter seems most likely: it makes little sense to engage into a semantic analysis of musical appropriations, since, apart from the lyrics, music is a form of nonconceptual art. On the same vein, an analysis of infringement in terms of economic harm to the rightsholder leads to equally unsatisfactory outcomes. It is well-known that synchronization licenses are both a common and significant revenue stream in the music sector.[170] In this sense, under an economic perspective, it might appear unclear why if the first author is obliged to bear the cost of a synchronization license, the posterior parodist is exempted from bearing this financial burden.

66 The reality is that parodists reproduce background music in order to better evoke the parodied work and not as an object of their irony, but it is difficult for the doctrines elaborated by courts and academics to come to terms with this reality. In this sense, the Italian construct seems to undermine or, at least, create inconsistencies with commonly accepted principles on copyright and music licensing. By contrast, an exception greatly simplifies the assessment: background music falls within the concept of parody because it is a necessary element to achieve the humorous result intended by the parodist, being any speculation on concepts such as 'semantic meaning', 'transformative use' or 'competitive harm' irrelevant.

V. Parody and the three-step tests

67 The three-step test (3ST) requires E&L to copyright to comply with three cumulative conditions. These are: a) the E&L shall only be applied in certain special cases; b) it must not conflict with a normal exploitation of the work or other subject-matter and c) it must not unreasonably prejudice the legitimate interests of the rightsholder.[171] There is a common fear that the 3ST unduly limits the operability of E&L,[172] which is one of the reasons why the Italian legislator should shy away from framing parody as an exception.[173] This sub-section illustrates why these

164 Court of Milan, 31 May 1999 in *Annali It. Dir. Autore*, 2000, 687

165 Court of Rome, 12 October 2000.

166 Musso (2015) p. 60.

167 Luis Gimeno (1997) 'Parody of Songs: a Spanish Case and an International Perspective', *Entertainment Law Review* 8(1), p. 20

168 See Gimeno (1997), p. 20

169 See for instance 'Porklips Now' (parody of 'Apocalypse Now'), which starts by reproducing the famous track 'The End' by The Doors. Available at https://www.youtube.com/watch?v=Yt93DVyjSZE [Accessed 22 April 2021].

170 See B. Klein and LM Meier (2017) 'In Sync? Music Supervisors, Music Placement Practices and Industrial Change'. In: M. Mera, R. Sadoff and B. Winters (eds.) The Routledge Companion to Screen Music and Sound (Routledge, Abingdon, UK) pp. 281-290.

171 See Article 5(5) of the Infosoc Directive; Article 13 TRIPS Agreement (1995); Article 9(2) of the Berne Convention.

172 See among the many Reto Hilty (2010) 'Declaration on the Three-step Test: Where Do We Go From Here?', *JPITEC* 83-6.

173 Ghidini (2018) 'Rethinking Intellectual Property'; Ghidini (2018) 'Conclusioni' in *Quaderni di Alai Italia*, p. 183.

concerns are largely misplaced. First, it submits that, in principle, the 3ST has no bearing on parodies and secondly, it shows how parodies normally satisfy the test.

1. The addressees of the Three-Step Test

68 The signatories of international IP treaties devised the 3ST as a counterweight to the scope of the exclusive rights. The test provided a legal basis to promulgate exceptions to copyright protection, within certain normative boundaries. As such, the function of the 3ST was to enable rather than limit E&L.[174]

69 In this context, there is little doubt that the addressees of the test are national legislators as the subjects of international treaty law.[175] It was the insertion of the 3ST in the InfoSoc Directive that perplexed the matter at the EU level. It is indeed unclear whether the Directive obliges member states to transpose the 3ST into national law or whether the test only curtails the margin of discretion of member states when introducing E&L. Depending on the answer to this first enquiry, two further questions arise. If the first solution holds true, it is unclear whether national courts should apply the test even in the absence of a corresponding domestic provision. Conversely, the second solution leads to the question whether national courts must dis-apply national law when it is clear that a domestic exception violates the 3ST. Commentators normally group the two questions together under the umbrella problem of whether the test bounds national courts during the application of E&L, and we will follow this approach for reasons of conciseness.[176]

70 In the past, the CJEU has offered ambiguous indications on this matter. In some judgements, it ruled that the 3ST is relevant only during the implementation phase of the InfoSoc Directive, that it does not affect the scope of E&L and that if a conduct unequivocally falls within an exception it automatically satisfies the test.[177] In other rulings, the CJEU seemed to invite national courts to assess whether the conduct of the defendant satisfy the requirements of the test.[178-179] Member States are divided between those who refused to implement the text into their national law and those who, in a way or the other, have done so.[180] This is not surprising, since the topic of the direct applicability of directives is among the more complex and ambiguous of EU law and has perplexed experts for years.[181]

71 On their side, while academics emphasize that the direct applicability of the 3ST becomes an additional control mechanism on already narrowly drafted E&L, thus bearing a nefarious impact on the fundamental rights that E&L are meant to safeguard,[182] they disagree on the direct applicability of the 3ST. In more detail, two main arguments militate in favor of the applicability of the 3ST by domestic courts. The first one is that Article 5(5) by using the word "apply" seems to refer to the judicial application of the test.[183] However, Recital 44 links the *application* of E&L to

174 Christoph Geiger, Martin Senftelben & Daniel Gervais (2014) 'The Three-Step Test Revisited: How to Use the Test's Flexibility in National Copyright Law', *Am. U. Int'l L. Rev.* 29(3), 593.

175 Geiger (2014) 593-4.

176 On the topic, see Richard Arnold & Eleonora Rosati (2015) 'Are National Courts the Addressees of the Three-step test?', *Journal of Intellectual Property and Practice* 10(10), 741-44; Eleonora Rosati (2014) 'Copyright in the EU: In search of (In) flexibilities', *JIPLP* 9(7), 585-88. They argue that domestic courts should disapply national law found inconsistent with the 3ST.

177 See *Copydan Båndkopi v Nokia Danmark A/S,* C463/12 CJEU (2015) at 90;*Infopaq International A/S v Danske Dagblades Forening,* C302/10 CJEU (2012) at 55-7; ACI Adam (2014) at 25.

178 See *Football Association Premier League Ltd et al. v Murphy et al.*, Joined Cases C403/08 and C429/08 CJEU (2011) at 181; *Public Relations Consultants Association Ltd v Newspaper Licensing Agency Ltd and Others,* C360/13, CJEU (2014) at 53-63.

179 For a more exhaustive analysis of the CJEU's case law, please see Arnold & Rosati (2015).

180 See Christoph Geiger (2007) 'The Role of the Three-Step Test in the Adaptation of Copyright Law to the Information Society', e-Copyright Bulletin, pp. 13-4.

181 Lorenzo Squintaini & Justin Lindeboom (2019) 'The Normative Impact of Invoking Directives: Casting Light on Direct Effect and the Elusive Distinction between Obligations and Mere Adverse Repercussions', *Yearbook of European Law* 38(1), 18-72; Arguing against the direct applicability, Daniël Jongsma (2020) 'The Nature and Content of the Three-step Test in EU Copyright Law: A Reappraisal' in Eleonora Rosati (ed) Handbook of European Copyright Law (Routledge).

182 Geiger et al (2014); Christoph Geiger (2006) 'The Three-Step-Test, a Threat to a Balanced Copyright Law?' *IIC* 37(6), p. 683; Martin Senftleben (2010) 'Bridging the Differences between Copyright's Legal Traditions – The Emerging EC Fair Use Doctrine', p. 529; Griffithis (2009), p. 3.

183 Christoph Geiger (2006) 'The Three-Step-Test, a Threat to a Balanced Copyright Law?', *IIC* 37(6), p. 690; more generally K.J. Koelman (2006) 'Fixing the Three-Step Test', *EIPR*, p. 40; Cohen H. Jehoram, 'Restrictions on Copyright and Their Abuse', EIPR, 2005, p. 364; Gustavo Ghidini (2018) 'Conclusioni' in *Quaderni di Alai Italia*, p. 183.

the obligations deriving from the international copyright framework, which in turn exclusively bind national legislators.[184] Others have also noted that the wording of the 3ST in the InfoSoc differs from the more restrictive one adopted in the Database and Software directives, which explicitly stipulate that exceptions to the rights conferred therein may not be 'interpreted' inconsistently with the test.[185] Finally, it cannot be excluded that the Article 5(5) is directed to the judicial application of the test by the CJEU. This reading has gained consensus in the literature and finds support in some recent rulings.[186] These considerations seem indeed to suggest that the expression 'shall be applied' has far from a clear connotation or decisive value. The second argument in favor of the 3ST direct applicability leverages on the observation that, since the EU legislator has already gauged the *abstract* compatibility of the E&L in Article 5 with the 3ST, it would be redundant to require domestic governments to duplicate this assessment.[187] However, this argument is now outdated due to the most recent developments of the CJEU. As we will see shortly, these suggest that for some of the E&L in Article 5(3) the assessment as to the compatibility between an exception and the 3ST is a prerogative of national legislators. Conversely, the case against the direct applicability of the test by national courts seems to leverage on more solid arguments. These include the context of the provision,[188] its history,[189] and the overarching principle of EU law that in the absence of a specific implementation directives are not applicable *contra legem* to the horizontal relations between individuals.[190-191]

72 Furthermore, even if a reading of this kind has not been advanced yet in the literature, it can be possible to reach a middle ground between the above extremes.[192] In particular, the most recent CJEU case law seems to invite the reconceptualization of the whole discussion by drawing on the fundamental distinction between E&L constituting a measure of full-harmonization and those which do not qualify as such. The distinction demands a case-by-case assessment, taking into account factors such as the wording, context, and history of the relevant provision.[193] Full-harmonization measures limit the leeway of Member States to a 'take it or leave it' decision, binding them to the wording of the InfoSoc Directive and the scope of the exception.[194] In these cases, the EU legislator has already struck a balance between the countervailing interests of rightsholders and users and this balancing shall apply uniformly throughout the Union. It is also safe to argue that the 3ST is mostly irrelevant for fully harmonized E&L. Indeed, on one side the EU legislator has already evaluated the conformity between the exception and the 3ST. On the other, an application of the test by domestic courts could lead to conflicting results and hamper the objective of copyright harmonization across the EU. Thus, for fully harmonized E&L, it would seem that if the act of the defendants fulfils the conditions for the application of the exception, then they automatically fulfil the three prongs of the test.[195]

73 The matter is more complicated in relation to E&L that do not constitute measures of full harmonization, quotation being a notable example.[196] In this case, Member States enjoy some room to maneuver in defining the scope of E&L. However, the InfoSoc Directive circumscribes this leeway in several

184 Recital 44 of the InfoSoc Directive: "When applying the exceptions and limitations provided for in this Directive, they should be exercised in accordance with international obligations. Such exceptions and limitations may not be applied in a way which prejudices the legitimate interests of the rightholder or which conflicts with the normal exploitation of his work or other subject-matter".

185 Griffith (2009); See M. Hart (2002) 'The Copyright in the Information Society Directive: an Overview', *EIPR* 58.

186 Jongsma (2020); see also *Stichting Brein v Jack Frederik Wullems* C-527/15, CJEU (2017) at 63; Spedicato (2020) p. 196.

187 Christoph Geiger (2006) 'The Three-Step-Test, a Threat to a Balanced Copyright Law?', *IIC* 37(6), p. 690.

188 Recital 44 in the Preamble to the InfoSoc Directive.

189 Proposal for a European Parliament and Council Directive on the harmonization of certain aspects of copyright and related rights in the Information Society (Brussels, 10 December 1997, COM(97) 628 Final), p. 32.

190 See *OSA – Ochranný svaz autorský pro práva k dílům hudebním o.s. V Léčebné lázně Mariánské Lázně a.s.,* C351/12, CJEU (2014). 43-5. See also Squintaini & Lindeboom (2019).

191 See Jongsma (2020).

192 The analysis of this middle-ground approach will require further research and, for reasons of conciseness, we will only sketch it here.

193 Spiegel Online at 25-29; Funke Medien 40-44.

194 See Deckmyn and Panier; See also Raquel Xalabarder (2016) 'The Role of the CJEU in Harmonizing EU Copyright Law', *IIC* 47, 636.

195 We borrow the wording of Infopaq II at 55-57.

196 Spiegel Online at 28; Funke Medien at 42.

ways. These include the need to fulfil all the requirements set for the relevant exception, not to compromise the objectives of the Directive and to comply with the 3ST.[197] This leads to the question of what are the consequences of a *prima facie* 3ST-incompliant domestic implementation. If it is impossible to reconcile domestic law and the 3ST, then the prohibition against the application of directives in horizontal relationships *contra legem* must be upheld.[198] By contrast, when the letter of the law allows for alternative interpretations, of which only some are inconsistent with the 3ST, the domestic court should adopt the interpretation most consistent with the test. This solution reconciles conflicting legal principles. On one side, it respects the prohibition against the application of directives *contra legem*, since it invites courts to interpret rather than disapply domestic statutes. On the other, it respects the necessity to "consider the whole body of rules of national law and to interpret them, so far as possible, in the light of the wording and purpose of the directive in order to achieve an outcome consistent with the objective pursued by the directive".[199]

74 Whereas this selective application of the 3ST in relation to only partially harmonized E&L will have to find a confirmation in future research and judicial practice, it is possible to see how the above three options play out in relation to parody. It is clear that if we conceive the 3ST as exclusively directed to legislators, it will have no bearing on the judicial application of parody. The only risk would lie in the choice to subject a parody exception to the 3ST or framing the latter as a general clause applying to all the E&L of the ICS. However, this does not seem an obligation under the InfoSoc Directive and the ICS seems to confirm this understanding.[200]

75 The same holds true under the middle-ground approach, i.e. the selective application of the 3ST to the E&L in Article 5. Indeed, parody constitutes a measure of full harmonization and as long as a state reproduces the wording of Article 5(3)k the conditions of the 3ST are automatically fulfilled. Moreover, the everyday meaning of the terms 'parody, caricature and pastiche' is sufficiently clear to clarify the scope of the exception and not even the CJEU has relied on the 3ST to construe the scope of the provision.[201] The CJEU has only emphasized the need for national courts to strike a fair balance between the interests of rightsholders and users.[202] This requirement seems close to a proportionality assessment meant to strike a balance between IP and other fundamental rights.[203] Interestingly, the German Supreme Court has also stressed the role of the 3ST as yardstick for the interpretation of E&L in relation to quotation, but has refrained from doing so in relation to parodies.[204]

76 As such, the 3ST becomes a threat to parody only under the understanding that courts must apply it in relation to all the E&L implemented in domestic statutes. However, it must be noted that the ICS rejects this approach, instead opting for a selective implementation of the test limited to only some specific E&L. Among these, Article 70 stipulates that E&L must comply with the 3ST "when applied to protected works or other subject-matter made available to the public in such a way that members of the public may access them in a time and from a place individually chosen by them".[205] Under this perspective, there seems to be a contradiction in advocating against an explicit parody exception in order to escape the reach of 3ST while prescribing for such a wide application thereof in relation to individually accessible works. Shall Italy ever implement a parody exception, it is Article 70 that constitutes the real threat to the free speech of parodists. Furthermore, the provision could also produce erratic results, for instance by subjecting 'on-demand' parodies to the 3ST, while providing for a more liberal application of the exception in other cases.

2. Application of the 3ST to parody

77 The precise criteria for applying the 3ST are not fully crystallized at the international and EU level and important ambiguities remain both as to the scope of each step and the relationship with one another.[206] However, it is possible to extract some

197 Spiegel Online at 38-9; Funke Medien at 45-53.

198 *OSA* at 45.

199 *OSA* at 44.

200 See below.

201 *Deckmyn.*

202 *Deckmyn* at 25-30.

203 *See* Christoph Geiger & Bernd Justin Jütte (2021) "Platform Liability under Art. 17 of the Copyright in the Digital Single Market Directive, Automated Filtering and Fundamental Rights: An Impossible Match', *GRUR International* 70(6); see partially in this sense Jongsma (2017) 675-6.

204 Please compare Federal Supreme Court, Meilensteine der Psychologie' 28 November 2013 – I ZR 76/12 and 'Reformistischer Aufbruch II', 30 April 2020 – I ZR 228/15 against 'Auf fett getrimmt' 28 July 2016.

205 Article 70 ICS.

206 Jongsma (2020) *ibid.*

common trends, hinting that the 3ST has a limited impact on parody.

78 As for the first step, an exception is 'clearly defined' when it has an 'individual and limited application or purpose', so to 'guarantee a sufficient level of legal certainty'. It must also target a limited number of beneficiaries and be invoked in specific and exceptional circumstances.[207-208] It is therefore hard to doubt that the expressions 'parody, caricature and pastiche' do not meet the requirement, since the meanings of these words are clearly defined and the exception applies to the specific circumstance of the humoristic re-elaboration of a work.

79 The expression 'normal exploitation' in the second step has been interpreted by the WTO appellate bodies as encompassing all utilizations that presently generate significant or tangible income, as well as those likely to generate income in the future,[209] and that are a normal consequence of enforcing IPRs.[210] The provision therefore excludes uses from which rightsholders do not normally receive compensation.[211] The CJEU endorses a similar understanding. It has laconically concluded that a use conflicts with the normal exploitation when it significantly reduces the volume of lawful transactions for the rightsholder.[212-213] In the context of patent exceptions, the WTO appellate bodies argued that 'normal exploitations' are the ones that are essential to achieve the underlying policy goals of IPRs,[214] and some have suggested extending this reasoning to copyright cases.[215] All these principles seem to rule out that parodies violate the second step. On one side, copyright holders do not normally embark in humorous reinterpretations of their own work and regarding other parodies "do not enter into economic competition with nonexempted uses".[216-217]

80 Despite this, there might be exceptional cases of parodies competing with the rightsholders' original works and these might be particularly difficult to adjudicate. For instance, Disney and Lucas Films normally engage into mockeries of their own characters in merchandising articles, especially apparel.[218] In these cases, the commercial harm caused to the rightsholder might be significant, insofar as merchandise constitutes a valuable revenue stream. This might be particularly relevant if courts understand the requirement of normal exploitation as having an economic rather than legal connotation, i.e. in terms of economic harm to the rightsholder.[219] However, even in this case, the 3ST does not lead to diverging outcomes from the

207 On the application of the first step, see Report of the WTO Panel, United States – Section 110(5) of the US Copyright Act, para. 6.62, WT/DS160/R (June 15, 2000); in the EU see *Public Relations Consultants Association* (PRCA) Case C-360/13, CJEU (2014) at 75-6.

208 Christoph Geiger, Martin Senftelben and Daniel Gervais (2014) 'The Three-Step Test Revisited: How to Use the Test's Flexibility in National Copyright Law', *Am. U. Int'l L. Rev.* 29(3), 593; Annette Kur (2009) 'Of Oceans Islands and Inland Water - How Much Room for Exceptions and Limitations Under the Three-Step Test?', *Richmond Journal of Global law and Business* 8(3), 314-5; Martin Senftleben (2006) 'Towards a Horizontal Standard for Limiting Intellectual Property Rights? – WTO Panel Reports Shed Light on the Three-Step Test in Copyright Law and Related Tests in Patent and Trademark Law', *IIC* 4, 414-8.

209 See Report of the WTO Panel, US at 6.180.

210 See Report of the Panel, Canada – Patent Protection of Pharmaceutical Products: Complaint by the European Communities and Their Member States, para. 7.69, WT/DS114/R (Mar. 17, 2000) at 7.38.

211 Senftelben (2006) 425.

212 *ACI Adam and Others*, C-435/12 (2014) at 39; *Stichting Brein* (2017) at 70.

213 In Germany the Federal Supreme Court has held that the step entails whether 'the use in question enters into direct competition with the conventional use, i.e. that there is an interference in the primary exploitation'. See Federal Supreme Court, 'Reformistischer Aufbruch II', 30 April 2020 – I ZR 228/15 at 72 and 'Meilensteine der Psychologie' 28 November 2013 – I ZR 76/12 at 50-2.

214 Report of the Panel, Canada at. 7.69, WT/DS114/R (Mar. 17, 2000).

215 See Geiger et al (2014) 594-600, Kur (2009) 318-20; Senftleben (2006) 421-428.

216 WTO Panel, US at 6.181. This is also the conclusion of the Commercial Court of Barcelona, 22 May 2019, arguing that a parody of a well-known character met the requirements of the 3ST.

217 Gambino (2002) 'Le Utilizzazioni Libere: Cronaca, Critica e Parodia', *AIDA*, pp. 127-134. This seems also confirmed by an empirical study on parody on YouTube K. Erickson (2013) 'Evaluating the Impact of Parody on the Exploitation of Copyright Works: An Empirical Study of Music Video Content on YouTube', Project Report – UK Intellectual Property Office.

218 Just browse Disney's official shop https://www.shopdisney.com/franchises/star-wars/clothing/ [Accessed 3 March 2021].

219 See for instance Senftelben (2006) p. 427-8; economic parameters were also a factor in WTO Panel, US at 6.206-6.219.

Italian approach, insofar as courts have deemed the lack of competition between the two works one of the requirements to treat parodies as autonomous creations.[220]

81 The last step entails two requirements. First, the interest claimed by the right-holder must be legitimate. This means to have a basis in the law, public policy, or social norms, which pushes courts to take into account both economic and non-economic interests.[221] In this regard, parodies normally do not encroach upon any legitimate interest of the copyright holder. This might be true insofar as the latter does not suffer any economic damages and its claims rather appear an attempt to exercise a form of censorship, a behavior that should not encounter the favor of the law in a democratic state.[222] The second requirement is even more relevant for parodies. It suggests that a certain amount of prejudice can be justified as 'reasonable', taking into account factors such as the economic harm caused to the rightsholder,[223] and the importance of the countervailing public interest in the free exploitation of the work.[224] This explains why the third step is sometimes associated with a proportionality assessment, in which courts have to gauge and balance conflicting interest, through criteria such as necessity, suitability and proportionality.[225] This reading strongly militates in favor of parodies, insofar as the prejudice caused to the rightsholder is justified by the overriding interest of safeguarding freedom of expression, while the harm caused to the rightsholder normally has little significance from an economic perspective.

VI. Summary of key results

82 The above exposition has proved that the legal scholarship has put a wrong emphasis on the status of parody as an overarching principle of the Italian legal system. First, because this construction contravenes the EU copyright law as interpreted by the CJEU, which clearly described E&L as the only legitimate tool to introduce the desired degree of flexibility into the copyright system. Secondly, because the assumption that a statutory exception would lead to an intransigent legal regime is erroneous: there is no legal principle obliging courts to interpret exceptions narrowly and, on a deeper look, even the infamous 3ST has no role to play on the matter. Conversely, it is the systematization of parody as a principle relating to infringement that paradoxically subjects parody to stricter legal requirements. The main reason for this is rather evident: while Article 5(3)(k) just requires parody to be the expression of humor, adjudicating whether a parody is a fully autonomous work requires a complex and delicate assessment, which includes considerations as to the semantic distance between the two works or the lack of economic competition among them. Furthermore, parody as a principle is incapable of effectively dealing with some hardline cases, and in particular music synchronization.

E. Conclusion

83 The tension between the pragmatic implications of the law and its dogmatic conceptualization is an old and everlasting one. Undoubtedly, it is the task of academics to refine legal theories both to guide courts and legislators and to deepen our understanding of the legal system, at least if we believe that knowledge has inherent value.[226] However, doctrinal over-conceptualization also comes with serious risks, such as overlooking the actual outcomes of the proposed constructs and neglecting the needs of the addressees of legal provisions. In Italy, the choice not to implement a parody exception has undoubtedly rested upon ideological reasons, such as portraying copyright as a principle-based system based upon solid freespeech foundations. What was lost amidst these ideological crusades was the sight of the pragmatic implications of the law: that parody as a principle leads to more restrictive outcomes than as an exception. Against this background, the implementation of the DSM directive not only seems like another lost opportunity to enact a generalized parody exception, but as anticipated, unnecessarily adds complexity to the system by potentially differentiating between the online and offline environment.

220 See in particular Pret. of Rome, 29 August 1978 and Court of Milan 29 January 1996, 1431.

221 See for instance Senftelben (2006) p. 433; WTO Panel, US at 6.224.

222 Arjun Gosh (2013) 'Censorship through Copyright: From Print to Digital Media', *Social Scientist* 41 (1/2) 51-68.

223 WTO Panel, US at 6.229; in the EU see PRCA at 61.

224 Geiger et al (2014), 596; Kur (2009) 322-4.

225 Jongsma (2020); in Germany see Federal Supreme Court, 'Reformistischer Aufbruch II at 73 and Meilensteine der Psychologie at 56.

226 In the latter sense, Michel Vivant (2021) "Thinking IP: A Game of the Mind", GRUR International 70(3), 213-4.

This result is very hard to justify, both under a doctrinal and pragmatic perspective.

Framing links and the prohibition of formalities

by **Maurice Schellekens***

Abstract: The Berne Convention of 1886 prohibits subjecting foreign copyright holders to formalities that control the enjoyment and exercise of their rights. This has given an important impetus to the 'international' protection of copyrights. This century, there is increasing attention for the drawbacks of a prohibition of formalities. Formalities may make it more difficult to clear rights because they limit possibilities to make the registration of rights mandatory or to find solutions for the use of orphaned works. In its recent decision in VG Bild-Kunst case, the CJEU has arguably introduced a new formality. A copyright holder who wants to exercise control over hyperlinks and framing links to their work, has to use effective technological protection measures to clarify for which public they seek to make their work available on the internet. The reason for requiring technology is to make it easier for those making links to know what links are allowed and which ones are not. However, if foreign copyright holders can invoke the prohibition of formalities and can enforce their rights against makers of links, even if they did not use technology, the goal of more clarity on permitted uses would not be achieved. This article investigates how the old prohibition of formalities relates to the proposed new uses of technology.

Keywords: Berne Convention; prohibition of formalities; hyperlinks; framing links; implied consent; Communication to the Public

Recommended citation: Maurice Schellekens, Framing links and the prohibition of formalities, 12 (2021) JIPITEC 439 para 1

A. Introduction

1 The Berne Convention of 1886 contains a prohibition of formalities. The prohibition ensures that authors outside their country of origin can enjoy and exercise their copyright, without having to comply with formalities. This has given an important boost to copyright protection on an international scale. The TRIPs agreement and the WIPO Copyright Treaty have further extended the prohibition of formalities. Even at the time the Berne Convention was drafted and during its first revisions, it was known that formalities can have positive effects too. For example, registration of a work or a copyright notice can alert the public to the existence of a copyright and thus can create more clarity about the status of a work. Nowadays, the subject matter of copyright has expanded, and the informational function of formalities has not lost its relevance. In the VG Bild-Kunst case, the CJEU conditioned the right to forbid hyperlinks to a work on the use of effective technical protection measures by the copyright holder.[1] The rationale is to create more certainty for those who seek to create hyperlinks to works. This article investigates how this new use of formalities relates to the old prohibition and how the decision sits within the field of tensions between unencumbered protection of copyrights outside the country of origin and the informational needs of

* Assistant Professor, Tilburg Law School.

1 CJEU 9 March 2021, Case C-392/19, ECLI:EU:C:2021:181, VG Bild-Kunst v Stiftung Preußischer Kulturbesitz, available at: <https://curia.europa.eu/juris/document/document.jsf;jsessionid=D63604B1A42C29CE0C30A-5996886F3E6?text=&docid=238661&pageIndex=0&d-lang=EN&mode=lst&dir=&occ=first&part=1&cid=9602731> Nelisa de Bruin, 'Door middel van framing opnemen van werk op website is mededeling aan publiek wanneer er maatregelen tegen framing zijn getroffen' (IEPT20210309, HvJEU, VG Bild-Kunst v SPK, 17 March 2021) <https://www.boek9.nl/items/iept20210309-hvjeu-vg-bild-kunst-v-spk > accessed 21 July 2021.

the public where it concerns information about the management of copyrights.

2 The first section after this introduction will briefly explain the VG Bild-Kunst case and place it in the context of the court's caselaw on hyperlinks. The second sections will address the question how the court's latest decision relates to the prohibition of formalities.

B. The VG Bild-Kunst ruling

3 Collective management organization (hereinafter CMO) VG Bild-Kunst negotiated with Stiftung Preußischer Kulturbesitz (hereinafter SPK) which is the operator of the website of the Deutsche Digitale Bibliothek (hereinafter DDB) about a license allowing the latter to display on its website(s) works of authors that are represented by VG Bild-Kunst.[2] VG Bild-Kunst insisted that SPK take effective technical protection measures (hereinafter TPMs) to prevent third parties from framing the works displayed on DDB's website and wanted to see a condition to that effect included in the license agreement between the parties. SPK disagreed and demanded that the CMO grant a license without the disputed condition. Litigation before German courts reached the Federal Court of Justice. In order to properly assess whether VG Bild-Kunst's demand for TPMs was objectively justified, the Federal Court of Justice asked the CJEU the following question for preliminary assessment: "Does the embedding of a work – which is available on a freely accessible website with the consent of the right holder – in the website of a third party by way of framing constitute communication to the public of that work within the meaning of Article 3(1) of Directive 2001/29 where it circumvents protection measures against framing adopted or imposed by the right holder?"

4 In its earlier case law, the CJEU had already decided that a public hyperlink to a work is only a communication to the public if the link serves a new public.[3] This holds not just for clickable links, but also for so-called framing links where webcontent is shown inside the frame of another website.[4] A new public is a public not contemplated by the rightsholder when he gave permission for the website on which the work is placed (and to which a link points). This is for example the case where a work is behind a paywall and the link circumvents the paywall. Hence, a new public can be a public that is not served by the original website, such as non-paying visitors in the example above. The facts of the VG Bild-Kunst case were particular in the sense that they concerned a situation where technology did not limit directly who could visit the original website, but the requested technology would only control what links could be made to the website. It only controlled who could see a work framed within a third party website. The technology left unaffected who can see the work directly on the original website of DDB (which might be anybody on the internet). The CJEU decided that also in this case the public excluded via the technology (i.e. the public that would have seen works framed in a third party website) counts as not contemplated by the copyright holder and therefore as a new public.[5] Hence, the CJEU answered the question of the Federal Court of Justice affirmatively.

5 With its ruling, the court gave a new dimension to how it conceives a new public. Apparently, a new public is not simply an issue of a nose-count or an analysis who could technically have had access to a work. The newness of a public may also be dependent on the context within which a member of the public has access to a work. A rightsholder may contemplate access via a certain website (for example Deutscher Digitaler Bibliothekenverband) and exclude access via framing links on other websites, even though anybody can directly access the work on the first mentioned website. This adds a new dimension to what the court decided in the Svensson case where it still found (at 26 and 27):

> *26 The public targeted by the initial communication consisted of all potential visitors to the site concerned, since, given that access to the works on that site was not subject to any restrictive measures, all Internet users could therefore have free access to them.*
>
> *27 In those circumstances, it must be held that, where all the users of another site to whom the works at issue have been communicated by means of a clickable link could access those works directly on the site on which they were initially communicated, without the involvement of the manager of that other site, the users of the site managed by the latter must be deemed to be potential recipients of the initial communication and, therefore, as being part of the public taken into account by the copyright holders when they authorised the initial communication.*

6 In case a copyright holder has taken measures to prevent framing however, the court finds that the nose-count-approach to a new public to 'be incompatible with his or her exclusive and inexhaustible right to authorise or prohibit any communication

2 C-392/19, VG Bild-Kunst v Stiftung Preußischer Kulturbesitz, at 11.

3 CJEU 13 February 2014, C-466/12, ECLI:EU:C:2014:76, Nils Svensson, Sten Sjögren, Madelaine Sahlman, and Pia Gadd v Retriever Sverige AB, at 24-28.

4 CJEU 21 October 2014, C-348/13, BestWater International GmbH v Michael Mebes, and Stefan Potsch, at 17-19.

5 C-392/19, VG Bild-Kunst v Stiftung Preußischer Kulturbesitz, at 41, 42.

to the public of his or her work'.[6] From the perspective that the right to communication to the public must not be hollowed out, the ruling is justified. It does however add yet another layer of complication to the application of copyright law to the phenomenon of hyperlinking.

7 To make the application of this part of copyright law easier in practice, the court decided that the copyright holder can only make known which public he contemplates through the use of effective technological protection measures (hereinafter TPMs). Hence, it is apparently not sufficient to put a provision in the Terms-of-Use of the website stating that framing is not permitted or words of similar meaning. They have to use effective technical protection measures to prevent framing.[7] In practice, this means either limiting access to the website or limiting the links that can be made. The court gives the following reasons for requiring effective TPMs:

> *46. It must be made clear that, in order to ensure legal certainty and the smooth functioning of the internet, the copyright holder cannot be allowed to limit his or her consent by means other than effective technological measures, within the meaning of Article 6(1) and (3) of Directive 2001/29 (see, in that regard, judgment of 23 January 2014, Nintendo and Others, C-355/12, EU:C:2014:25, paragraphs 24, 25 and 27). In the absence of such measures, it might prove difficult, particularly for individual users, to ascertain whether that right holder intended to oppose the framing of his or her works. To do so might prove even more difficult when that work is subject to sub-licences (see, by analogy, judgment of 8 September 2016, GS Media, C-160/15, EU:C:2016:644, paragraph 46).*
>
> *49. Admittedly, it cannot be forgotten that hyperlinks, whether they are used in connection with the technique of framing or not, contribute to the smooth operation of the Internet, which is of particular importance to freedom of expression and information, enshrined in Article 11 of the Charter, as well as to the exchange of opinions and information on the Internet, which is characterised by the availability of incalculable amounts of information (judgment of 29 July 2019, Spiegel Online, C-516/17, EU:C:2019:625, paragraph 81 and the case-law cited).*

8 From the perspective that makers of framing links need to know what public a copyright holder contemplated, the requirement to use TPMs can be applauded.

9 On the basis of the court's ruling, one may wonder whether the technical measures are perhaps required in more situations: not just for controlling framing links, but for all hyperlinks. The reason to demand effective technological protection measures (legal certainty, smooth functioning of the internet) certainly points in that direction. The uncertainty faced by potential makers of links is the same, whether it concerns framing links or clickable links. The rationale (i.e., difficulty of ascertaining the rightsholder's intentions) also points in this direction. Moreover, the court seeks to hold the rules around linking technology neutral.[8]

10 At the same time, the desired clarity is achieved only with limitations. An internet user making a link cannot blindly trust the presence or absence of TPMs. Works can be and often are placed on the internet without permission of the rightsholder, and then the absence (or even presence) of TPMs obviously does not provide any information about the intentions of the rightsholder.

11 The ruling also does not make clear what counts as effective technical protection measures. Sometimes the TPM only consists of machine readable text that others respect on the basis of a broadly shared technical convention. For example, with a robots.txt file a website owner can indicate that a site may not be indexed by a search engine. Search engines usually respect the message conveyed by a robots.txt file. However, the text file does not physically prevent indexing. In that respect, it may not be effective.

12 Furthermore, the clarity of the intentions of the copyright holder may be compromised if a copyright holder's expression in words about their intentions deviate from the 'message' conveyed by technology. If the text of the ruling is taken by its literal meaning, it suggests that a copyright holder's clear expressions of their intentions in words should be ignored, if not backed up by TPMs. So, terms-of-use of a website that clearly address the copyrights in works present on the website and disallow links should thus be ignored, if no TPMs to that effect are in place. The same holds for provided licenses. That is at least remarkable, because the court also stresses a copyright holder's exclusive and inexhaustible right to authorize or prohibit any communication to the public.[9] It will be interesting to see whether this is going to be further qualified in future case law.

13 Foreign copyright holder's may find in the prohibition of formalities, both in the Berne Convention and in

6 C-392/19, VG Bild-Kunst v Stiftung Preußischer Kulturbesitz, at 50.

7 Alexander Ross, 'VG Bild-Kunst v SPK - putting the illegality back into being framed, Case Comment', (2021) 32(5) Ent. L.R. 149, 150: 'It appears from the decision that (absent the introduction of such measures by the rights holder) a simple contractual bar on framing by the copyright owner would not be enough—it seems that the relevant licence would have to expressly require the licensee to introduce "effective technological measures" to prevent framing.'

8 C-466/12, Svensson, at 29.

9 C-392/19, VG Bild-Kunst v Stiftung Preußischer Kulturbesitz, at 50.

the WIPO Copyright Treaty, a first instrument to test this aspect of the court's ruling. The court did not address the compatibility of its decision with the prohibition of formalities.

C. Prohibition of formalities

14 Under the Berne Convention, foreign authors may not be subjected to formalities that affect the existence and enforcement of rights. Formalities relating to the existence of rights refer to 'everything which must be complied with in order to ensure that the rights of the author with regard to their work may come into existence.'[10] Examples of this include registration, deposit of copies, payment of fees or the making of declarations. Likewise, formalities relating to the enforcement refer to everything that must be complied with to bring court proceedings to enforce the copyright. According to article 5(2) BC, the enjoyment and the exercise of the author's rights shall not be subject to any formality. The term 'exercise' of rights in the Berne Convention means enforcement.[11]

I. Is requiring effective TPMs to limit the contemplated public a formality?

15 According to the decision in VG-Bild-Kunst, a rightsholder can only invokes their right to communication to the public against the maker of a hyperlink, if it serves a new public. A new public is defined as a public not contemplated by the copyright holder when they gave permission for the original communication of the work on the website to which the hyperlink points. To preserve the possibility to act against hyperlinks, the copyright holder must mark a potential public as not contemplated by them. Theoretically, a public can be excluded by using effective TPMs, by demanding that licensees take such technical measures or by excluding a public in words, for example in a contract, website terms-of-use or the like. The latter option has been whittled down by the latest decision of the court, as was mentioned in the previous section.

16 To see what exactly the formality is in a hyperlinking case, we have to revisit the observation made in the previous section that a rightsholder may delimit a public either by limiting the public of the original website or by specifically addressing hyperlinks (as in the VG Bild-Kunst case). In the first mentioned cases, a copyright holder may place their work on a website behind a paywall, because this is the way to exploit their work. It is now the responsibility of the maker of a hyperlink to this work to respect the paywall or to ask for permission for a hyperlink. The copyright holder does not need to do anything to ensure that that any non-paying audience is considered a new public, other than what they did to delimit the public of their original website. So in this case, the paywall is simply a decision of the copyright holder to exercise their right in a certain way.

17 However, if the copyright holder wants to set specific rules for hyperlinking (e.g. no hotlinking or framing forbidden, but other links are fine) then the copyright holder has to take measures specifically targeting hyperlinks. Given that the copyright holder has to do something to preserve their right, this raises the question whether the requirement to use TPMs amounts to a forbidden formality in the sense of article 5(2) BC. In some blogs, it is suggested that this is indeed so.[12]

18 First, a declaration, either in words or through the use of effective TPMs, is of the type of activities that are typically caught by the concept of formalities as meant in the BC and WCT.[13]

19 Second, we need to analyze whether the formality affects the existence or scope of the right ('enjoyment' in terms of the Berne Convention) or conditions its enforcement ('exercise' in terms of the Berne Convention). The requirement of TPMs does not affect the procedural means that a foreign copyright holder has at their disposal to enforce a right.

10 Federal Council programme, art. 2: Actes 1884, 43. See also S. Ricketson and J.C. Ginsburg, International Copyright and Neighbouring Rights. The Berne Convention and beyond, Volume I, (second edition OUP, 2006) 323.

11 S. Ricketson and J.C. Ginsburg, International Copyright and Neighbouring Rights. The Berne Convention and beyond, Volume I, (second edition OUP, 2006), 6-104, p. 325.

12 Eleonora Rosati, 'CJEU rules that linking can be restricted by contract, though only by using effective technological measures' (IPKat 2021) <https://ipkitten.blogspot.com/2021/03/cjeu-rules-that-linking-can-be.html> accessed 14 June 2021, under 'Comment' and Giulia Priora, 'The CJEU's take on unauthorized framing of online content: (only) if technologically precluded, then prohibited, Court of Justice of the European Union, 9 March 2021, Case C-392/19, VG Bild-Kunst v Stiftung Preußischer Kulturbesitz (VG Bild-Kunst)' (Medialaws 9 April 2021) < https://www.medialaws.eu/the-cjeus-take-on-unauthorized-framing-of-online-content-only-if-technologically-precluded-then-prohibited/ > accessed 21 July 2021, at 5.2.

13 S. Ricketson and J.C. Ginsburg, International Copyright and Neighbouring Rights. The Berne Convention and beyond, Volume I, (second edition OUP, 2006), 1-19, p. 18.

Therefore, the analysis below focuses on formalities that condition the 'enjoyment' of a right.

20 Could the existence or scope of the right be affected by the formality? For the formality to affect existence or scope, this would mean that a hyperlink serving a contemplated public (i.e. a public the copyright holder failed to exclude) is outside the scope of the right of communication to the public. The following part of the ruling in VG Bild-Kunst supports this proposition. In rule 36 of its decision, the court states:

> *'[...] it is apparent from the Court's case-law that, provided that the technical means used by the technique of framing are the same as those previously used to communicate the protected work to the public on the original website, namely the Internet, that communication does not satisfy the condition of being made to a new public and, since that communication accordingly does not fall within the scope of a communication 'to the public', within the meaning of Article 3(1) of Directive 2001/29, the authorisation of the copyright holders is not required for such a communication [...]'*

21 Apparently, in the absence of a new public, the making of a hyperlink falls outside the scope of a communication to the public. This reading is further supported in rule 32 where the court holds:

> *'In order to be classified as a 'communication to the public', a protected work must further be communicated using specific technical means, different from those previously used or, failing that, to a new public, that is to say, to a public that was not already taken into account by the copyright holder when he or she authorised the initial communication of his or her work to the public (judgment of 19 December 2019, Nederlands Uitgeversverbond and Groep Algemene Uitgevers, C-263/18, EU:C:2019:1111, paragraph 70 and the case-law cited).'*

22 Hence, if the technical means are the same (hyperlink is the same means) and the public is contemplated and thus not new there is no communication to the public. It seems that the copyright holder is required to perform a formality, viz. to mark a public as not contemplated, in order to prevent that a hyperlink serving this public falls outside the scope of the right of communication to the public. Therein, it would affect the scope of the right.

II. Is it a forbidden formality?

23 The BC gives foreign authors certain substantive minimum rights and it grants them protection under the assimilation principle. Does the requirement of TPMs take away minimum rights? In particular, one may ask whether the right of communication to the public as meant in the BC encompasses hyperlinking. If it wouldn't, it may be possible to argue that formalities are allowed since they fall outside the framework of the BC. In order to analyze this, we must look beyond the BC, in particular to the WIPO Copyright Treaty (hereinafter WCT). According to article 3 WCT, signatories must apply the articles 1 to 21 of the BC mutatis mutandis to the protection provided for in the WCT. This includes the prohibition of formalities of article 5(2) BC. Article 8 WCT brings the right of making a work available to the public explicitly under the right of communication to the public. The WCT prescribes that signatories must ensure that authors 'enjoy the exclusive right of authorizing any communication to the public of their works, by wire or wireless means, including the making available to the public of their works in such a way that members of the public may access these works from a place and at a time individually chosen by them'. This does not yet explicitly say that hyperlinking is covered, but it brings the right of communication to the public at least within the digital realm. But even if it cannot be established with certainty whether hyperlinking falls within the right of making available to the public as mentioned in the WCT, it may still not be beyond the reach of the formalities prohibition. On the basis of a historic interpretation, Ginsburg rejects the view that the prohibition of formalities does not see to rights extending beyond Berne minima.[14] Strict adherence to well-established minimum rights would make the prohibition of formalities a toothless instrument. The whole idea of Berne+ rights is a misnomer according to Ginsburg.

24 However, the issue may be moot in light of the fact that a foreign author in an EU Member State may invoke the assimilation principle. Under this principle, they have a right of communication to the public that can be invoked against makers of hyperlinks, since foreign national copyright law of an EU Member State grants this right. The foreign author may not have taken technical measures against framing nor any other measures, such as a rejection of framing in the ToU of the website. Could they invoke the prohibition of formalities to enforce their right of communication to the public against the maker of a framing link? That would be unlikely if you interpret the assimilation principle purely as a non-discrimination principle. Then the foreign author would be able to invoke the right only on the same terms as a national author. However, this would take away the effect of the prohibition of formalities. For a foreign copyright holder, it is more difficult to comply with formalities than it is for a national author.[15] Given the rationale of the

14 Jane C. Ginsburg, 'Berne-Forbidden Formalities and Mass Digitization' (2016) 96 B. U. L. Rev. 745 < https://scholarship.law.columbia.edu/faculty_scholarship/691/> accessed 7 July 2021, p.763-764. This includes rights covering ground that could be subject to Berne-permissible exceptions.

15 See S. Ricketson and J.C. Ginsburg, International Copyright

BC to enable and facilitate copyright protection outside the country of origin, this approach must be rejected. Analyzing the issue from the perspective of the Vienna Convention on the law of treaties, van Gompel arrives at the same conclusion in his dissertation.[16] It is more convincing to interpret the assimilation principle as granting 'the rights which their respective laws do now or may hereafter grant to their nationals'. The foreign copyright holder is able to invoke the right to communication to the public as a right granted to national authors and ignore the formalities on the basis of the prohibition. He would thus be able to demand action against the maker of a framing link.

25 The preliminary result is that foreign authors may invoke a right to Communication to the public in European Member States without having taken TPMs. This would undermine the certainty the CJEU seeks to create for makers of hyperlinks: every foreign author could invoke the right to communication to the public without TPMs. This gives reason to analyze whether there are ways to avoid this result. A first approach may be to see whether the Berne Convention and the WCT would arrive at a different result if hyperlinking in certain situations is seen as an exception to the right to communication to the public.

1. Hyperlinking as an exception to the right to Communication to the public

26 Article 10bis(1) BC may give a possibility to introduce a formality that also binds foreign copyright holders. The first sentence of the provision reads:

> *'(1) It shall be a matter for legislation in the countries of the Union to permit the reproduction by the press, the broadcasting or the communication to the public by wire of articles published in newspapers or periodicals on current economic, political or religious topics, and of broadcast works of the same character, in cases in which the reproduction, broadcasting or such communication thereof is not expressly reserved.'*

27 This provision gives the possibility to introduce an exception for the benefit of the press, however with a possibility for the copyright holder to expressly reserve the mentioned rights, in which case the exception obviously isn't available. Possibly, the route via an exception provides a model that can be used in other situations too, to introduce a formality that is not forbidden. The idea would be that national law introduces an exception, e.g. an exception to the right to communication to the public allowing beneficiaries of the exception to make framing links. The assimilation principle would give a foreign author only the right as reduced by the exception and in order to bar a claim of the foreign copyright holder grounded in minimum rights, the exception must be Berne and WCT compatible, i.e. it must pass the 3-step test. Therefore, the reasoning is that compliance with the formality – such as taking effective TPMs against framing – would broaden the rights of the foreign author beyond what he can claim on the basis of the Berne Convention and the WCT. Employing TPMs would allow the copyright holder to forbid framing links as communications to a new public. Because compliance with the formality would give supra-treaty rights and because the BC apparently sanctions such a construction in article 10bis(1), be it in a different context, the formality would be allowed and can be invoked against foreign authors.

28 This argumentation is however controversial. Ginsburg argues that article 10bis(1) BC is a lex specialis that does not lend itself for a generalization.[17] It has to be said that article 10bis(1) BC is a formality written directly in the Berne Convention. That is obviously not the case for any other exception, such as an exception for framing or hyperlinks. Van Gompel sees more room for the argumentation, but sees the first step of the three step test – only in special cases – as a bottleneck that strongly reduces practical usability.[18] Moreover, it is unclear how the third step in the three step test – not prejudicial to the justified interests of the author – should be applied. Can you argue that the copyright holder does not suffer prejudice because they can take any prejudice away by complying with the formality? Or is this creating a cloud of dust to hide that you make a minimum right subject to a formality? This route to arrive at a permitted formality is therefore far from sure.

29 Moreover, the CJEU does not think about hyperlinking in terms of an exception. Hyperlinking is in the view of the CJEU under circumstances possible without seeking prior permission from the copyright holder either because it falls outside the

and Neighbouring Rights. The Berne Convention and beyond, Volume I, (second edition OUP, 2006), section 6.85.

16 Stef van Gompel, Formalities in copyright law—an analysis of their history, rationales and possible future (Wolters Kluwer, Information Law Series, 2011) 179–93. Available at: < https://dare.uva.nl/search?identifier=2f611291-951b-4781-9559-fc64158902d0>, p. 150.

17 Jane C. Ginsburg, 'Berne-Forbidden Formalities and Mass Digitization' (2016) 96 B. U. L. Rev. 745, 759 < https://scholarship.law.columbia.edu/faculty_scholarship/691/> accessed 7 July 2021.

18 Stef van Gompel, Formalities in copyright law—an analysis of their history, rationales and possible future (Wolters Kluwer, Information Law Series, 2011) 172 <https://dare.uva.nl/search?identifier=2f611291-951b-4781-9559-fc64158902d0> accessed 21 July 2021.

right of communication to the public, or because permission is implied because of the way in which the copyright holder has allowed the work to be placed on the internet. The CJEU is not completely clear about this, but it did not create an exception for hyperlinking.

30 In conclusion, the route inspired by article 10bis(1) BC is uncertain for the time being. Given that the CJEU does not think about hyperlinking in terms of an exception, it is also not a plausible option.

31 If an EU court would deny enjoyment or exercise (i.e. enforcement) of the right on the ground that a limitation of the contemplated public was not rendered in effective TPMs, this has the appearance of a forbidden formality.

2. How the required use of TPMs may not be a forbidden formality

32 The CJEU leaves room to see a hyperlink to a contemplated public in two ways. As indicated above, such a hyperlink can be seen as something that 'does not fall within the scope of a communication 'to the public'' so that 'authorisation of the copyright holders is not required for such a communication' (at 36). However, in the same decision you can also read: 'by making his or her work freely accessible to the public or by authorising the provision of such access, the right holder envisaged from the outset all internet users as the public and accordingly consented to third parties themselves undertaking acts of communication of that work.' (at 37). At the end of the quotation the court does not say 'communication to the public' but merely speaks of 'communication'. However, given that the court also speaks about consent it leaves open room for seeing the making of a link to a contemplated public as a communication to the public, or at least as being part of more encompassing communication to the public, such as the initial placement of the work on the public internet by the copyright holder or with their permission. It may be that the exact doctrinal categorization does not matter for the question the court sought to answer in its decision. With a view to the prohibition of formalities however, it does make a difference. In the view that a link to a contemplated public is outside the scope of the right, the formality (use of an effective TPM or demanding that a licensee uses such tech) controls the scope of the right. Then it becomes difficult to argue how it is not a forbidden formality.

33 If it is however seen as a communication to the public for which the author has given permission, then it is much easier to argue that TPMs are a permissible formality that can also be upheld against foreign copyright holders. The prohibition of formalities does not see to the exercise of rights (the term 'exercise' here not being understood as enforcement). If a country requires that an exclusive license can only be given in writing for example, such is not a forbidden formality.

34 This solution to the problem of the forbidden formalities, is reminiscent of the decision the German Federal Supreme Court reached in a copyright case about Google's use of thumbnails of images for its Image Search service.[19] Google's use of the thumbnails could not be justified under statutory copyright exceptions. The Federal Supreme Court found a solution in the assumption of an implied consent. By placing the images on the public internet without TPMs the rightsholder consented to inclusion of the images' thumbnails in image search services. Nonetheless the route of the implied consent raised questions that were resolved in sometimes less, sometimes more satisfactory ways.[20] By choosing the route of the implied consent instead of the implied license, the court avoided the mandatory interpretation of licenses that only those use rights are licensed that are specified explicitly. Implied consent merely takes away the unlawfulness of the use of the images. Furthermore, the route of the implied consent raises the question of how to deal with the situation that a rightsholder in words explicitly declares that they do not allow the works to be included in a search engine (or in framing links, as in the VG Bild-Kunst case), but fails to use technical means to that effect. Such a statement may be ignored if it is clearly a contradictory statement by the rightsholder.[21] This implies that there have to be strong reasons to view the consent as it emanates from the non-use of TPMs as the declaration that objectively may be understood as intended. These reasons can be found in an economic argumentation, viz. that the rightsholder using TPMs appears to be the cheapest-cost-avoider. Below an economic argumentation in the context of the mandatory use of TPMs to fend off

19 German Federal Supreme Court (Vorschaubilder) (I ZR 69/08) April 29, 2010 (BGH (Ger)). See also BERBERICH, "Die urheberrechtliche Zulässigkeit von Thumbnails bei der Suche nach Bildern im Internet", 2005 MultiMedia und Recht (MMR) 145, at 147,148.

20 Matthias Leistner, 'The German Federal Supreme Court's judgment on Google's Image Search - a topical example of the "limitations" of the European approach to exceptions and limitations' (2011) IIC 42(4), 417-442. Spindler, "Bildersuchmaschinen, Schranken und konkludente Einwilligung im Urheberrecht - Besprechung der BGH-Entscheidung "Vorschaubilder"", 2010 GRUR 785.

21 Spindler, "Bildersuchmaschinen, Schranken und konkludente Einwilligung im Urheberrecht - Besprechung der BGH-Entscheidung "Vorschaubilder"", 2010 GRUR 785, 790.

framing links will be elaborated. Other issues have not been resolved or at least far from satisfactorily. These included situations where images have been placed on the internet by others than the rightsholder and without his consent.[22] In such case there cannot be an implicit consent to the benefit of Image Search Services. Furthermore, might there be situations in which a compensation to the rightsholder for the use of their images is justified, the route of the implied consent makes this extremely difficult.[23] It is clear that implied consent is far from ideal solution to lacking statutory exceptions (as in the Google Image Search case) or to a conflict with the prohibition of formalities in international copyright law. In the latter context, Samuelson raises the question whether seeing the failure to use TPMs as permission is not overly formalistic.[24] The result comes close to a situation in which the enjoyment of the right to communication to the public has been reduced.

35 Even though an implied license is not an ideal solution, there are good economic arguments to embrace it. Hyperlinks constitute a clear social added value as is recognized by the court:[25]

> *'[...] it cannot be forgotten that hyperlinks, whether they are used in connection with the technique of framing or not, contribute to the smooth operation of the Internet, which is of particular importance to freedom of expression and information, enshrined in Article 11 of the Charter, as well as to the exchange of opinions and information on the Internet, which is characterised by the availability of incalculable amounts of information (judgment of 29 July 2019, Spiegel Online, C-516/17, EU:C:2019:625, paragraph 81 and the case-law cited).'*

36 In itself, this does not mean that hyperlinks could not be subjected to a right of communication to the public or that the copyright holder should be limited in the exercise of his right. The latter may only be justified if the transaction cost of exercising the right in the same way as with respect to other (non-hyperlink) communications to the public is so high that it takes away for a substantial part the social benefit of hyperlinks. Apparently, the court thinks that this is the case:[26]

> *'It must be made clear that, in order to ensure legal certainty and the smooth functioning of the internet, the copyright holder cannot be allowed to limit his or her consent by means other than effective technological measures, within the meaning of Article 6(1) and (3) of Directive 2001/29 (see, in that regard, judgment of 23 January 2014, Nintendo and Others, C-355/12, EU:C:2014:25, paragraphs 24, 25 and 27). In the absence of such measures, it might prove difficult, particularly for individual users, to ascertain whether that right holder intended to oppose the framing of his or her works. To do so might prove even more difficult when that work is subject to sub-licences (see, by analogy, judgment of 8 September 2016, GS Media, C-160/15, EU:C:2016:644, paragraph 46).'*

37 So, the 'formality' of using technical means serves to communicate how the copyright holder exercises their right. Already, in the discussion leading up to the BC and its revisions, it was understood that formalities have a valuable communicative function (be it that it was conceived of in terms of putting the public on notice about a copyright). Apparently, the holder of a copyright is here the cheapest cost avoider.

38 Copyright law and especial the law concerning the right to communication to the public as applied to hyperlinks has in the last few years become more complicated. At the same time, it is important that copyright law can at least in a basic form be applied by laymen. After all, with digital technology, copyright law has entered everybody's world. In that respect, it is helpful that a legal reality is not too far removed from the physical (or at least digital) reality. To make copyright more 'what you see is what you get'.

39 This also fits in with the idea to give formalities a bigger role in copyright, an idea that is at least in academic circles gaining traction, be it more in the context of solving the problem of the growing body of orphan works.[27]

22 Matthias Leistner, 'The German Federal Supreme Court's judgment on Google's Image Search - a topical example of the "limitations" of the European approach to exceptions and limitations' (2011) IIC 42(4), 417-442, at 433-434.

23 Matthias Leistner, 'The German Federal Supreme Court's judgment on Google's Image Search - a topical example of the "limitations" of the European approach to exceptions and limitations' (2011) IIC 42(4), 417-442, at 431-432.

24 Jane C. Ginsburg, 'Berne-Forbidden Formalities and Mass Digitization' (2016) 96 B. U. L. Rev. 745, 774 < https://scholarship.law.columbia.edu/faculty_scholarship/691/ > accessed 7 July 2021. Ginsburg 2016 asks the same question in her article about her analogous solution for orphaned works.

25 VG Bild-Kunst at 49.

26 VG Bild-Kunst at 46.

27 Jane C. Ginsburg, 'Berne-Forbidden Formalities and Mass Digitization' (2016) 96 B. U. L. Rev. 745 < https://scholarship.law.columbia.edu/faculty_scholarship/691/> accessed 7 July 2021, Gompel, Stef van, 'Copyright Formalities in the Internet Age: Filters of Protection or Facilitators of Licensing' (2013) 28 Berkeley Technology Law Journal 1425 (2013) < https://ssrn.com/abstract=2420312 > accessed 21 July 2021, M. R. F. Senftleben, 'How to Overcome the Normal Exploitation Obstacle: Opt-Out Formalities, Embargo Periods, and the International Three-Step Test', 2014(1) Berkeley Technology Law Journal 1-19 < https://research.vu.nl/ws/files/1032636/Normal%20Exploitation%20

40 All this does not take away that there are challenges. Technology may not allow for the formulation of such fine-grained conditions as those rendered in natural language. For the time being, it is for example difficult to have a machine distinguish between commercial and other websites. In this sense, the ruling of the court lays a burden on the shoulders of the holders of copyrights: not using TPMs implies consent, and to change this situation, only TPMs can be used.

41 Another challenge is that it makes copyright enforcement more complicated. Copyright holders from EU member states may get used to the idea that TPMs need to be used, if control over linking is desired. For copyright holders outside Europe, the requirement to use TPMs may come as a surprise if they want to enforce their right of communication to the public against a hyper- or framing link. However, technical measures against framing are uniform and can be taken from any country and they can also be introduced after a work has been brought online.

D. Conclusion

42 With its decision in the VG Bild-Kunst case, the CJEU reconfirmed that a copyright holder can only invoke their right to communication to the public against makers of hyperlinks that were not contemplated by them. The new element is that the copyright holder can only mark a public as not contemplated by using effective TPMs. This allows potential makers of links to ascertain easily whether the rightsholder allows linking. It is important that copyright law – which nowadays applies to almost anybody, not just professional parties – remains relatively simple in its daily application. That here technology is the prescribed means to express contemplated uses of the work contributes to this goal.

43 The analysis undertaken in this article shows that contrary to some comments an obligation to use TPMs can be compatible with the prohibition of formalities, as laid down in the Berne Convention and later extended in the WCT. Therefore, it is necessary that the CJEU brings more doctrinal clarity in the reason why a copyright holder cannot forbid hyperlinking to a contemplated public. If this reason is that a hyperlink is a contemplated part of the original publication on the internet for which already permission has been given, then formally the requirement to exclude a new public with TPMs is compliant with the prohibition of formalities. Maybe this result will not please everybody. However, in my view there are enough reasons to embrace this result.

Obstacle.pdf > accessed 21 July 2021, Christopher Jon Sprigman, 'Berne's Vanishing Ban on Formalities' (2013) Vol. 28, No. 3 Berkeley Technology Law Journal, < https://ssrn.com/abstract=2407015> accessed 21 July 2021.

Responsible Vulnerability Disclosure under the NIS 2.0 Proposal

by **Sandra Schmitz and Stefan Schiffner***

Abstract: Both, the NIS Directive and the GDPR introduce breach reporting obligations. In particular, in the case of the GDPR this might include an obligation to go public about an incident. These legal obligations might be in conflict with good/common practice of responsible vulnerability disclosure. This paper briefly outlines reporting duties under NISD and GDPR and maps these to hypothetical scenarios where informing end users about cyber incidents might lead to uncontrolled vulnerability disclosure. In that view, this paper analyses whether the latest proposal for a NIS Directive 2.0 strikes the right balance between the need for swift reporting and the need to investigate a vulnerability when introducing a 'coordinated vulnerability disclosure'.

Keywords: Cybersecurity; NIS Directive; GDPR; Vulnerability; Disclosure

Recommended citation: Sandra Schmitz and Stefan Schiffner, Responsible Vulnerability Disclosure under the NIS 2.0 Proposal, 12 (2021) JIPITEC 447 para 1

A. Introduction

1 A central element of EU cybersecurity legislation is the reporting of security breaches.[1] In this line, the General Data Protection Regulation (GDPR)[2] introduced reporting obligations for data controllers based on the assumption that security challenges and relevant mitigation measures can be better identified if data breaches are communicated to public authorities. Similarly, the first horizontal cybersecurity instrument, the NIS Directive (NISD)[3], introduced reporting obligations for operators of essential services (OESs) and digital service providers (DSPs) under its scope. While it may seem that the reporting obligations are a mere duplication of legal obligations, tempting entities to report only to one authority, the obligations co-exist without prejudice. Accordingly, one incident may be reported to two separate regulators under different reporting schemes and notably with different objectives (GDPR: protection of personal data; NISD: protection of underlying infrastructure). Though such double reporting is not restricted to the NISD and GDPR, the example of these two instruments perfectly highlights one potentially 'dangerous' con-

* SnT, University of Luxembourg, sandra.schmitz@uni.lu; stefan.schiffner@uni.lu.

1 NIS Cooperation Group, *Annual Report NIS Directive Incidents 2019* (Publication 03/2020) 2.

2 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/ 1.

3 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L 194/1.

sequence: early public disclosure of a vulnerability that challenges the effectiveness of the incident response.[4] In December 2020, the European Commission published a proposal for a new NIS Directive ('NIS 2.0 proposal')[5], which inter alia introduces a so called 'coordinated vulnerability disclosure' and addresses the need to balance swift reporting and in-depth analysis of vulnerabilities.

2 This paper briefly outlines the reporting schemes under the NISD and GDPR before the flaws of existing legislation in relation to controlled vulnerability disclosure are analysed. We will then critically evaluate how the NIS 2.0 proposal addresses the identified concerns.

B. EU Incident Reporting Schemes

3 Incident reporting obligations are not restricted to the NISD and GDPR. A number of further legal instruments also require the reporting of security incidents, such as: Directive (EU) 2018/1972 (EECC)[6], Regulation (EU) No 910/2014 (eIDAS Regulation)[7], Directive (EU) 2015/2366 (PSD2 Directive)[8]. While the NISD introduces a cross-sectoral cybersecurity incident reporting scheme, the aforementioned instruments have a limited, sectoral scope of application. Simplified, they provide for an obligation to notify (security) incidents having an actual adverse effect[9] on the security of network and information systems of essential services or digital services (NISD), electronic communications networks or services (EECC), trust services (eIDAS Regulation), and payment-related services (PSD2). The common aim is to understand (cyber-)security threats and identify vulnerabilities. In terms of simplification, we focus on incident reporting under NISD and GDPR, since the mandatory public disclosure of certain data breaches under GDPR challenges the effectiveness of a NIS incident response in general.

I. Incident Reporting under the NIS Directive

4 The NISD establishes an incident reporting framework covering the notification of significant incidents as well as requiring the implementation of security measures. As regards the obligation to report an incident, i.e. "any event having an actual adverse effect on the security of" NIS[10], the NISD differentiates between operators of essential services (OESs)[11] and digital service providers (DSPs)[12]. Member States shall ensure that OESs and DSPs notify, "without undue delay", the National Competent Authority (NCA)[13] or the computer security incident

4 See S Schmitz and S Schiffner, 'Don't tell them now (or at all)-End user notification duties under NIS Directive and GDPR' (2021) 35:2 International Review of Law, Computers & Technology 101-115.

5 European Commission, 'Proposal for a Directive of the European Parliament and of the Council on measure for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148' COM(2020) 823 final.

6 Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code [2018] OJ L 321/36.

7 Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L 257/73.

8 Directive (EU) of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [2015] OJ L 337/35.

9 The definitions of 'incidents' vary slightly, and the PSD2 distinguishes between security incidents (as malicious actions) and operational incidents.

10 Art 4(7) NISD.

11 An OES is a public or private entity within one of the sectors enlisted in Annex II, which meets the criteria laid down in art. 5(2) NISD. These criteria are inter alia whether the entity provides a service that is essential for the maintenance of critical societal and/or economic activities, and an incident would have significant disruptive effects on the provision of that service. This resembles the definition of "critical infrastructure" in Art. 2(1) ECI Directive (Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection [2008] OJ L 345/75) with the difference that only entities depending on NIS may qualify as OESs, and thus fall within the scope of the NISD. Member States are tasked with the identification of OES on a national basis.

12 Annex III to the NISD lists as DSPs within the scope of the NISD only three types of services: online marketplaces, online search engines, and cloud computing services. Providers of digital services have to self-determine whether they o er services of a type listed in Annex III of the NISD in order to fall within the scope of application.

13 The NISD provides for great flexibility either to implement a centralised or decentralised approach for designation of

response team (CSIRT)[14] of incidents having a significant impact on the continuity of the essential services they provide (in case of an OES), or incidents having a substantial impact on the provision of a digital service (in case of a DSP).[15] The NISD does not foresee mandatory notification of the individuals concerned by a security incident.[16] After consultation with the notifying entity, the NCA or the CSIRT may inform the public about individual incidents where public awareness is necessary in order to prevent an incident or to deal with an ongoing incident, or in the case of a DSP disclosure of the incident that is otherwise in the public interest.[17] As the NISD is a Directive, results that must be achieved are laid down, but Member States are free to decide how to achieve these aims. The amount of leeway as to the exact rules to be adopted may result in varying determination of what constitutes a "significant impact" or "undue delay". Notification requirements may not only vary depending on the Member State but also within sectors. Only with regard to DSPs, the determination of substantial impact has been harmonised by Commission Implementing Regulation (EU) 2018/151[18], which specifies the relevant factors to be taken into account.[19] The different level of harmonisation for treatment of OESs and DSPs is directly linked to the different services provided (with OES directly linked to physical infrastructure) and also respects that Member States are tasked with the identification of national OES.[20] Supervision of OESs and DSPs at national level may be centralised[21] or decentralised[22], resulting in a variety of National Competent Authorities (NCAs).

competences at national level: A slight majority of Member States opted to designate a single NCA, others designated several sectoral NCAs. Spain, for instance, employs a decentralised approach where the competent authority de-pends on whether the operator concerned is an OES or DSP); the same applies to the UK, where the NCA for OESs further depends on the sector concerned.

14 According to art. 9 NISD, Member States shall designate one or more CSIRTs, which may be established within a NCA and must be responsible for risk and incident handling.

15 See art 14(3) NISD as regards OES, and art 16(3) as regards DSP.

16 Arts 14(6) and 16(6) NISD.

17 Ibid.

18 Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems and of the parameters for determining whether an incident has a substantial impact [2018] OJ L26/48.

19 An incident is to be considered substantial if e.g. more than 100,000 users have been affected or the damage caused exceeds EUR 1,000,000, see art 4 Commission Implementing Regulation (EU) 2018/151.

II. Data Breach Reporting under the GDPR

5 Articles 33 and 34 GDPR require data controllers to notify a personal data breach to the supervisory authority, i.e. the Data Protection Authority (DPA), within 72 hours after becoming aware of it and communicate the personal data breach to the data subject without undue delay. As a 'Regulation', the GDPR has binding legal force throughout every Member State and is directly applicable. The GDPR defines a 'personal data breach' as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".[23] Reporting of data breaches to the competent DPA is not necessary where the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.[24] The same applies where the controller has taken steps to ensure that the high risk posed to individuals' rights and freedoms is no longer likely to materialise.[25] Where notification of the DPA cannot be achieved within 72 hrs, information may be provided in phases without undue further delay.[26] In contrast to the NISD, data controllers must also communicate a breach to the

20 Cf. Recital 57 NISD.

21 Member States that applied a centralised approach are inter alia: Austria, Belgium, France, and Germany.

22 Member States that applied a decentralised approach are inter alia: Czechia, Luxembourg, the Netherlands, and Poland.

23 Art 4(12) GDPR.

24 Art 33(1) GDPR. The exemption from the general reporting duty requires a predictive risk assessment from the perspective of an objective bystander, see Maria Wilhelm, 'Art. 33, marginal no. 9' in: Gernot Sydow (ed), *Europäische Datenschutzgrundverordnung, Handkommentar* (2nd edn, Nomos 2018). On conditions where notification is not required cf. Article 29 Working Party, *Guidelines on Personal Data Breach Notification under Regulation 2016/679 (wp250rev.01)* (2018) 18 et seq.

25 Art 34(3)(b) GDPR.

26 Art 33(4) GDPR.

affected individual without undue delay if there is a 'high risk' for the rights and freedoms of the affected individual.[27] This notice allows the controller to inform about the risks and advise individuals on how to protect themselves from the potential consequences of the breach.[28] Where direct communication to the individuals concerned would involve disproportionate effort, Article 34(3)(c) GDPR permits public communication. No guidance is provided as to when a delay is 'undue'; Recital 86 refers to "as soon as reasonably feasible". From a privacy perspective, this may be as soon as the data controller has determined that the prerequisites for notification foreseen in Article 34 GDPR are fulfilled. Since recital 86 also appeals for "close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities", the determination of 'undue delay' depends as well on the guidance provided by the national authorities involved.[29]

III. Interplay of the Reporting Schemes and the Potential Risk of Early Vulnerability

6 A *lex specialis* provision within the NISD foresees that where a sector-specific union act foresees security or notification requirements of at least equivalent effect, these provisions shall prevail.[30] The same applies regarding pre-existing sector-specific legislation, namely, the reporting schemes of the Telecoms Framework (now: EECC) and the eIDAS Regulation.

7 The GDPR does not constitute a l*ex specialis* to the NISD as it does not regulate the notification of a significant disruption to the provision of NIS but introduces a notification obligation where personal data is at stake. Breaches of personal data are problems in and of themselves, but a breach may indicate a vulnerability in the underlying security regime.[31] Thus, although the notification obligations are very similar, they are no duplications, and do not exclude one another.[32] While from a legal perspective, it is possible to differentiate between incidents falling under the GDPR and such falling under the NISD, in practice, most security incidents will involve some sort of personal data, meaning that the data controller will have to report these incidents to the NISD NCA and the DPA. Cooperation of these authorities in the sense of co-ordination and information-sharing is only recommended under the NISD and the GDPR framework ('should'/'shall' cooperate) when dealing with an incident/data breach. They operate independently. The lack of formal cooperation may result in different advice by the NIS NCA and competent DPA to the reporting entity surrounding public disclosure of an incident. From a privacy perspective, the DPA may request instant information of the data subjects concerned, although the entity concerned has a basic interest in delaying notification to investigate an attack. In terms of delaying notification of the data subject, recital 86 GDPR requires that guidance be respected when provided by the DPA or by other relevant authorities such as law-enforcement authorities. This may suggest that guidance by a NIS NCA to delay going public may justify a delay in notifying data subjects. However, since the operative provisions of the GDPR do not require cooperation and information-sharing by the DPAs and NIS NCAs, the initiation of such cooperation may in the worst case lay at the hand of the reporting entity. The fact that cooperation is only mentioned in a recital requires to recall the nature of recitals: The recitals of an EU legal act are not in themselves legally binding in the same way that the operative articles are. In principle, recitals "state concisely the reasons for the main provisions of the enacting terms of the act".[33] The function of recitals as an interpretative legal tool has been developed in the case law of the CJEU to resolve ambiguities where an operative provision is not clear[34] or to help to explain the purpose and intent behind a normative instrument.[35] Obviously, recital 86 goes further than explaining purpose or intent, or the reasons for Article 34 GDPR, when it appeals for "close cooperation with" authorities when determining the lawfulness of a deviation from the

27 Art 34 GDPR; see also Recital 86. On how to assess risk and high risk see Article 29 Working Part (n 24) 22 et seq.

28 Recital 86.

29 Mario Martini, 'Art. 34 DS-GVO, marginal no. 44' in B Paal and D Pauly (eds), *Beck'sche Kompakt-Kommentare, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz* (2rd ed Beck 2021).

30 Art. 1(7) NISD.

31 European Data Protection Board, *Guidelines 01/2021 on Examples regarding Data Breach Notification* (Version 1.0, 2021) 6.

32 Cf. Art. 1(3) NISD.

33 European Union, *Joint Practical Guide of the European Parliament, the Council and the Commission for Persons Involved in the Drafting of European Union Legislation* (2nd ed Publications Office of the European Union 2015) 32. By stating the reasons on which a legal act is based, recitals give effect to Art. 296 TFEU.

34 See T Klimas and J Vaiciukaite, 'The Law of Recitals in European Community Legislation' [2008] ILSA Journal of International & Comparative Law 61, 86 with further references.

35 Cf. case C-173/99 *BECTU* EU:C:2001:356, paras. 37-39.

obligation to inform "without undue delay". Other than the operative provisions of the GDPR, recital 86 further recognises that "the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication". Considering that early disclosure of an incident may interfere with the containment and recovery of an incident, it seems that the GDPR recognises this risk as a reason for delay. When the recital uses the notion 'may' instead of 'must' in relation to the justification for more time, it remains unclear which "need to implement appropriate measures against continuing or similar breaches" justifies a delay.[36] Also, the justification seems to be restricted to an ongoing attack (and 'similar breaches'), which leads to the further question as to when an attack is still ongoing. An attack may be terminated, but the fixture of a vulnerability may be ongoing. Therefore, an entity may have a keen interest in further delaying the notification of data subjects opposed to what the GDPR requires. Considering that there are also scenarios, where the same incident is notified by two different entities to two different authorities (for instance where a DSP reports an incident to the NIS NCA, and the data controller (using a service provided by the DSP) to the competent DPA under the GDPR), there is a likelihood that an early disclosure to the public by the data controller hampers the incident response of the DSP. Instead of specifying when delay is not 'undue', the legislator limits its focus on legitimate suspension of notification in the following recitals on law enforcement interests. Accordingly, recital 88 GDPR sets forth that in setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, such rules and procedures should "take into account the legitimate interests of law enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach". In that line, the guidance on personal data breach notification issued by the Article 29 WP[37] solely addresses interests of law enforcement authorities as justifying delay. Consequently, early disclosure is primarily considered as potentially hampering criminal investigations. As of date, little attention is paid to the interests of the entity encountering a security incident. One reason for this may be the fact, that national case law in which fines have been imposed upon data controllers primarily relate to failures in implementing technical and organisational measures to ensure secure processing, right to access or right to erasure.[38] Many of the cases outlined in the EDPB 2019 annual report highlighted a lack of proper technical and organisational measures for ensuring data protection that resulted in data breaches without an outside attack.[39]

8 The question remains as to which legal consequences a data controller faces when—in order to not hamper their containment and recovery strategy—they delay notification of data subjects concerned of a data breach. Pursuant to Art. 82 (1) GDPR, they will be liable for the damage caused by the suspended or delayed notification of the subject.[40] Accordingly, this liability is limited to damage that occurs from the point of time where a delay is considered undue. The DPA may use its investigative and corrective powers (Article 58 GDPR), and, once an infringement of the obligation under Article 34 GDPR is established, may issue an administrative fine of up to EUR 10 million, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.[41] When deciding whether to impose an administrative fine and deciding on the amount of the fine due regard has to be given to a number of factors enshrined in Article 83 (2) GDPR. These factors include inter alia actions taken to mitigate the damage suffered by data subjects (lit. c), the degree of cooperation with the supervisory authority to remedy the infringement and mitigate the possible adverse effects of the infringement (lit. f), and to what extent the controller notified the infringement to the controller (lit. h). Article 83 (2) GDPR also provides for a catch-all element when "any other mitigating factor" needs to be taken into consideration, which must—in light of the aforementioned factors—also include the containment and recovery of an incident to identify an attacker, vulnerability or certain modus operandi. It remains to be seen how much weight national DPAs attribute to an effective NIS response—either

36 The same applies to the questions which law enforcement interests may justify a delay, however, law enforcement authorities are more likely to provide guidance. There is a clear need to concretise justifications from the side of DPAs, see Mario Martini, 'Art. 34 DS-GVO, marginal no. 45' in B Paal and D Pauly (eds), *Beck'sche Kompakt-Kommentare, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz* (2rd ed Beck 2021).

37 Article 29 Working Party (n 24) 1.

38 Confer chapter 6 on supervisory authority activities in 2019 in European Data Protection Board, *2019 Annual Report, Working Together for Stronger Rights* (2020).

39 Ibid.

40 Mario Martini, 'Art. 34 DS-GVO, marginal no. 7' in B Paal and D Pauly (eds), *Beck'sche Kompakt-Kommentare, Datenschutz-Grundverordnung, Bundesdatenschutzgesetz* (2rd ed Beck 2021). This view is not undisputed: according to *Reif* (Yvette Reif, 'Art. 34 DS-GVO, marginal no. 18' in Peter Gola (ed), *DS-GVO, Datenschutz-Grundverordnung VO (EU) 2016/679, Kommentar* (2nd ed Beck 2018)) a suspended or delayed notification only triggers claims for damages under general tort law.

41 Art. 82 (4) lit a GDPR.

as a justification or at least as an important factor when deciding upon and setting the amount of a fine.

IV. Interim Summary

9 At a first glance, the aforementioned lack of mandatory cooperation may account for an early incident disclosure. Where the DPA treats an incident independently from the NIS NCA, privacy may prevail over an investigation into the roots and causes of an incident from a technical perspective. As DPAs advise on when data subjects should be notified, an entity may feel obliged to disclose an incident instantly, whereas from a cybersecurity perspective delay is required. This theoretical risk is rooted in the different aims of the legal instruments. The GDPR concerns the protection of personal data and publicity of a data breach should put the data subjects concerned in a position to mitigate immediate risks of damage. Guidance on data breach notification by the EDPB European Data Protection Board[42] thus solely focuses on the data protection position and addresses issues in relation to the timing of notification from a mere privacy viewpoint. Other than protecting the rights and freedoms of a natural person, publicity of incidents under the NISD aims at (re-)establishing information security, i.e. confidentiality, integrity and availability of NIS. As a consequence, the individual affected by a mere security incident may only be informed of the incident, where public awareness is necessary in order to prevent an incident, to deal with an ongoing incident, or limited to DSPs, disclosure is in the public interest.[43] Recital 86 GDPR addresses the dilemma of early disclosure by recognising that "the need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication". The wording of the justification suggests that it should be limited to continuing and ongoing data breaches; it does not encompass ongoing security incidents as such. Hence, it would for instance fall short in an incident which incidentally compromised consumer data, but leads to an ongoing attack targeted at other vital systems of the OES or DSP.[44] However, since the justification is 'only' part of the recital, this supports the interpretation of 'undue delay' in the operating provision, but does not provide legally binding limits to the scope of Article 34 GDPR. Also, mitigation of an incident and an effective NIS response are factors to be considered when deciding upon the imposition of an administrative fine for infringing Article 34 GDPR.

C. Responsible Disclosure

10 In the light of the above, the following section analyses two relevant examples discussed by the EDPB in its guidelines 01/2021[45] with regard to their potential for harm in the case of premature public incident disclosure. As aforementioned, legal reporting duties, in particular public disclosure, might conflict with the professional ethical standards of IT-Security staff. However, this conflict might appear larger than it is due to a general overestimation of what can be learned from reporting an incident about the mechanics of a vulnerability.

11 **Incidents aren't Vulnerabilities – Definitions.** A vulnerability is a set of conditions that allows the violation of a security (or privacy) policy. Such conditions might be created by software flaws, configuration mistakes and other human errors of operators, or unexpected conditions of the environment a system runs in. Exploits are software that exploit vulnerabilities for some effect (even be it only to demonstrate the existence of vulnerabilities). Malware is some software that is designed with malicious intent. It might or might not make use of exploits or vulnerabilities. An incident from a technical perspective is any successful or attempted violation of a security or privacy policy. It might involve vulnerabilities, exploits malware, or none of these concepts.[46] Lastly, a patch is a piece of software that is designed to improve an IT system by modifying its software or data.

12 **Controlled (or Responsible) Vulnerability Disclosure** is a process that allows IT vendors and finders of vulnerabilities to cooperatively find solutions that reduce the risk associated with public vulnerabilities;[47] I.e., a researcher (finder) who discovered a flaw in a system, informs the developer (vendors, providers) of a system about a flaw and potential fixes. This allows the developer to take mitigation measures (patches, traffic monitoring, blocking) to eliminate or reduce the risk that the vulnerability is used by an attacker. Only then the vulnerability is published. Controlled vulnerability

42 European Data Protection Board (n 31), or Article 29 Working Party, (n 24).

43 cf. Articles 14(6) and 16(7) NISD.

44 Schmitz and Schiffner (n 4) 110.

45 European Data Protection Board (n 31).

46 Allen D Householder et al, 'The CERT ® Guide to Coordinated Vulnerability Disclosure' [2017] (August) Technical Report Cmu/Sei-2017-Sr-022 <https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf> last accessed 26 August 2021.

47 Cf. ISO/IEC 29147.

disclosure is detailing out this process, in particular how to act if developers are not willing or not able to react accordingly. This type of disclosure may eventually result in the suspension of going public about an incident in order to elaborate the appropriate containment strategy including vulnerability fixtures.

I. Case Analysis.

13 In its Guidelines 01/2021 the EDPB outlines 18 fictional cases that shall support and guide data controllers and processors to better understand reporting obligations under the GDPR. Two of these exemplary cases will be analysed that demonstrate risks of being in conflict with general controlled vulnerability disclosure guidelines. Due to the sample cases being of a very general nature, further details have been added by the authors to highlight potential conflicts.

14 Since the issue of hampering investigations by early disclosure in particular arises in ransomware and data exfiltration attacks, the subsequent analysis focuses on these attacks. Attacks of this kind are largely based on software vulnerabilities as opposed to human error, natural disaster or traditional crime.

15 **Ransomware Attacks.** Ransomware is a type of malware attack which attacks the availability of data of the victim in order to extort money from the victim.

16 EDPB Case no. 03: "The information system of a hospital/healthcare centre was exposed to a ransomware attack and a significant proportion of its data was encrypted by the attacker. The company is using the expertise of an external cybersecurity company to monitor their network. Logs tracing all data flows leaving the company (including outbound email) are available. After analysing the logs and the data the other detection systems have collected the internal investigation aided by the cybersecurity company determined that the perpetrator only encrypted the data without exfiltrating it. The logs show no outward data flow in the timeframe of the attack. The personal data affected by the breach relates to the employees and patients, which represented thousands of individuals. Backups were available in an electronic form. Most of the data was restored but this operation lasted 2 working days and led to major delays in treating the patients with surgery cancelled / postponed, and to a lowering the level of service due to the unavailability of the systems." The EDPB concludes that this sort of attack might lead to reporting obligations to the general public if a sever interruption of the service for many customers is observed and the involved data amounts to special categories of data.[48]

17 The case seems to be inspired by a Ransomware attack which largely effected the NHS[49] in 2017.[50] It needs to be pointed out that the malware WannaCry[51] was epidemic. Hence, it was most likely not targeted at the NHS as such. Its large spread was possible since it was based on the so called EternalBlue exploit which made use of the vulnerability CVE-2017-014.[52] This exploit targeted a certain implementation of Microsoft's smb protocol.[53] Although a related vulnerability a patch was available, many systems remained unpatched.[54]

18 Beside the direct effect of the attack, the large spread of the malware also demonstrated the vast number of unpatched systems and in particular the vast number of systems which are likely hard to patch due to legacy system support. In such a case, one might advise against informing the general public immediately to avoid copycat attacks.[55] In simple terms, publicity should be avoided until a patch for

48 ibid.

49 UK national health service (https://www.nhs.uk).

50 Acronis iGmbH, 'Case study the NHS cyber attack' (Acronis) <https://www.acronis.com/en-us/articles/nhs-cyber-attack/> last accessed 26 August 2021.

51 Kaspersky, 'What is WannaCry ransomware?' (Kaspersky Resource Center) <https://www.kaspersky.com/resource-center/threats/ransomware-wannacry> last accessed 26 August 2021.

52 For more on the vulnerability, see National Cybersecurity FFRDC, CVE-2017-0144m (Mitre Corporation) <https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2017-0144> last accessed 26 August 2021.

53 For more on the current revision and previous versions of the Microsoft server message block (SMB) protocol, see Microsoft, 'Server Message Block (SMB) Protocol' (Microsoft) <https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-smb/f210069c-7086-4dc2-885e-861d837df688> last accessed 26 August 2021.

54 It has to be noted that not patching is not always neglect: often systems in production stay unpatched for longer since system owners need time to investigate if the patch is compatible with specialised equipment.

55 A delay needs to consider that due to high impact of some observed infections, controlled disclosure may not even be possible.

the software vulnerability is released in order to prevent further personal data to be interfered with.

19 In contrast to this, is EDPB Case no. 04: "The server of a public transportation company was exposed to a ransomware attack and its data was encrypted. According to the findings of the internal investigation the perpetrator not only encrypted the data, but also exfiltrated it. The type of breached data was the personal data of clients and employees, and of the several thousand people using the services of the company (e.g., buying tickets online). Beyond basic identity data, identity card numbers and financial data such as credit card details are involved in the breach. A backup database existed, but it was also encrypted by the attacker."

20 Assuming, contra to Case no. 3, that no public knowledge of the mechanics of the attack can be derived nor was the underlying malware as widespread or at least would not expose vulnerabilities in widespread systems, informing the general public is unlikely to trigger more attacks. However, the leaked information poses high risks for the affected individuals, so it is advisable to inform victims and the public as soon as possible.

II. Protection Goal Conflict GDPR – NISD

21 Extending the EDPB's fictional cases magnifies the root cause of the conflict among GDPR and NISD with regard to incident reporting, namely, the different protection goals. On one hand, the NISD aims at the protection of the underlying (vital) infrastructure. That is, its focus is on availability, though confidentiality and integrity might be needed to ensure the former. Further, the NISD operates under the assumption that OESs and DSPs use similar systems for their operation. That means in turn, knowledge of an incident might help to uncover ongoing incidents with other providers. Lastly, the analysis of incidents might unveil vulnerabilities that are shared with other providers. In short, incident reporting aims at the discovery of large-scale attacks and identification of underlying vulnerabilities in order to allow coordinated incidence response (short term) and an improved level of cyber security/ preparedness (long term). On the other hand, the GDPR aims at the protection of users' rights with focus on confidentiality (of the users' data). Here, incident reporting to the DPAs has the same aims as reporting under the NISD. However, regarding the duty to inform affected users, it goes further: it shall allow users to take personal mitigation actions, e.g., changing passwords, blocking payment cards etc. and thereby, prevent the harm from materialising.

D. Vulnerability Disclosure under the NIS 2.0 Proposal

22 With the COVID-19 pandemic, the foreseen revision of the NISD gained momentum. Following an accelerated review of the NISD, the European Commission adopted a proposal for a revised NISD on 16 December 2020 ('Proposal for NIS 2.0')[56], although the first report of the Directive was only due in May 2021. This clearly shows the commitment of the European Commission to increase cyber resilience. While the NISD set up cooperation mechanisms between Member States, the NIS 2.0 proposal aims to strengthen and extend cooperation, as well as exploit synergies.

I. The Operative Provisions on Coordinated Vulnerability Disclosure and Cooperation Mechanisms in the NIS 2.0 Proposal

23 Remedying the causes of NIS vulnerabilities is identified as an important factor in reducing cybersecurity risks. The proposal recognises that the reporting entities are often third parties relying on a particular ICT product or service, and thus, the manufacturer or provider of ICT products or services should also receive vulnerability information. In that regard, the NIS 2.0 proposal introduces a framework for coordinated vulnerability disclosure[57] and requires Member States to designate CSIRTs to act as trusted intermediaries and facilitate the interaction between the reporting entities and the manufacturers or providers of ICT products and services.[58] Coordinated vulnerability disclosure, as described in the proposal, specifies a structured process through which vulnerabilities are reported in a manner allowing the diagnosis and remedy of the vulnerability before vulnerable information is disclosed to third parties or to the general public. Where entities become aware of an incident, they are required to submit an initial notification without undue delay and not later than 24 hours, followed by a final report not later than one month after.[59] While the initial notification is limited to the information strictly necessary to make the competent authorities aware of the incident and allow the reporting entity to seek assistance, the final report must contain a (i)

56 European Commission (n 5).

57 Art 6(1) NIS 2.0 Proposal.

58 Recital 29 NIS 2.0 Proposal.

59 Art 20(4) NIS 2.0 Proposal.

detailed description of the incident, its severity and impact; (ii) the type of threat or root cause that likely triggered the incident; (iii) applied and ongoing mitigation measures. This two-stage approach is similar to the reporting in stages under the GDPR, where information may be provided in phases if full notification of the DPA cannot be achieved within 72 hrs.

24 The aim of the two-stage approach becomes clear in the recitals: the reporting entity's resources should not be diverted from activities related to incident handling, which should be prioritised.[60] Coordinated vulnerability disclosure also takes into account coordination between the reporting entity and the manufacturers or providers of ICT products and services as regards the timing of remediation and publication of vulnerabilities.[61] The role of the CSIRT as the coordinator in that process should include the identification and contact of further entities concerned, support of reporting entities including negotiations with regard to disclosure timelines, and the management of vulnerabilities that affect multiple organisations (so called multi-party vulnerability disclosure).[62] ENISA is required to develop and maintain a European vulnerability registry for the discovered vulnerabilities.[63] Although cooperation under the NIS 2.0 proposal is still attached to cross-border incidents, there is a clear request to strengthen information sharing of national authorities,[64] e.g. by establishing cooperation rules between the NIS NCAs and DPAs to deal with infringements related to personal data.[65] However, cooperation of NIS NCAs and DPAs as required in Article 32 NIS 2.0 Proposal focuses on NCAs notifying DPAs when they have an indication of a personal data breach infringement by important or essential services (prieviously known as OES and DSP) of the security and notification obligations enshrined in Articles 18 and 20. Since NCAs are obliged to notify indications of a personal data breach to the DPA 'within a reasonable period of time',[66] yet another timeframe is introduced, adding to the complexity of determining 'undue delay' under GDPR and suggesting that the NCA may withhold information where the data controller would be obliged to notify the DPA 'without undue delay'.[67]

II. Strengthening Coordination, but Laxity Towards Responsible Disclosure?

25 While at first glance, the introduction of a coordinated vulnerability disclosure suggests a strengthening of control in the sense of responsible disclosure—i.e. it respects the interest of an entity to delay information of the public—this may not be the case. It is merely that the Proposal lays down a two-stage approach to incident reporting to strike a balance between, on the one hand, swift reporting to NCAs that helps mitigating the potential spread of incidents and allows entities to seek support, and, on the other hand, detailed reporting that draws valuable lessons from individual incidents and improves over time the resilience to cyber threats of individual companies and entire sectors.[68]

26 The clear commitment to put the incident response ahead of detailed reporting, does not eliminate the conflict with swift reporting to data subjects under GDPR since this remains predominantly an issue of GDPR compliance and does not concern obligations under the NISD. The delay granted for detailed reporting may tempt entities even more to depart from the 'without undue delay' reporting to individuals under the GDPR. The reporting in phases of a NIS incident to NIS NCAs may become the default reporting mechanism in light of prioritizing the incident response. As publicity may hamper an incident response, data controllers may give priority to the technical incident response over informing data subjects. Even when Article 20(1) and (2) NIS 2.0 Proposal introduce a GDPR-like obligation to inform service recipients of incidents that are inter alia likely to adversely affect the provision of that service 'without undue delay', the ratio of the NISD remains an effective incident response. Accordingly, this third-party notification is only required 'where appropriate', suggesting that this is only necessary where measures are available to the service recipients to mitigate the resulting risk

60 Recital 55 NIS 2.0 Proposal.

61 Recital 28 NIS 2.0 Proposal.

62 Recital 29 NIS 2.0 Proposal.

63 Art 6(2) NIS 2.0 Proposal.

64 Art 26(1) NIS 2.0 Proposal.

65 Recital 77 NIS 2.0 Proposal.

66 Art. 32(1) NIS 2.0 Proposal.

67 The EDPS suggests changing the wording of the Proposal to 'without undue delay' in order to enable DPAs to perform effectively their tasks, European Data Protection Supervisor, *Opinion 5/2021 on the Cybersecurity Strategy and the NIS 2.0 Directive* (11 March 2021), 17.

68 cf. Recital 55 NIS 2.0 Proposal.

themselves,[69] and where incident publicity does not interfere with effective incident response in a whole.

27 During the consultation process various stakeholders[70] addressed a necessity to align reporting authorities, thresholds, timeframes and penalties in EU legislation to eliminate "persisting redundancies in terms of incident reporting and double notification requirements under different legal regimes".[71] The proposal suggests that for the purposes of simplifying the reporting of security incidents, Member States should establish a single entry point for all notifications required under NISD and also under other Union law such as the GDPR.[72] Whether a single entry point may alleviate issues in relation to early disclosure to the public in form of individual data subjects remains to be seen as a single entry point does not mean that notified authorities will treat a reported incident in the same way. A single entry point for reporting to regulators is also not related to obligations to inform the public. However, there was also no necessity from the legislator to address this issue in the NIS 2.0 proposal since the risk of early disclosure is merely an issue of GDPR compliance. As long as the GDPR does not address the containment and recovery of an incident along with further interests such as law enforcement as a justification to delay notification of data subjects, the conflict persists. The sole conflict that the NIS 2.0 Proposal eliminates are the legal consequences for non-compliance under the GDPR and NIS instrument: Article 32(2) NIS 2.0 Proposal clarifies that where a DPA imposes an administrative fine, a NCA shall not impose an administrative fine for the same infringement. Again, failure to comply with notification obligations towards the regulatory authority, and failure to comply with the notification obligation towards the data subject/service recipient are different infringements. An entity that informs the DPA and NCA of a security incident involving personal data but does not inform the data subject without undue delay to deal with an incident is potentially subject to legal sanction under the GDPR.

28 In sum, the coordinated vulnerability disclosure and strengthening of cooperation do not provide a solid framework for responsible disclosure since every data controller has the sword of Damocles hanging over their head in the form of mandatory disclosure of data breaches to data subjects without undue delay.

E. Conclusion

29 Reporting obligations under NISD and GDPR are neither redundant nor conflicting at large, but stem from the different goals of the respective legislation. However, in detail, these protection goals might be conflicting, and accordingly, reporting under one instrument might undermine protection efforts under the other regime. In particular, premature notification of users (and by this the general public) might lead to adverse effects with regard to cybersecurity, i.e., the reported incident under GDPR might lead to uncontrolled vulnerability disclosure. This in turn might expose other entities and services to risks since they did not have the head start to patch vulnerabilities as they would have had under a controlled disclosure regime. It is creditable that the NISD 2.0 proposal acknowledges the concept of controlled disclosure. However, without matching obligations within the GDPR, this might cause further conflicts: the GDPR might require informing users while under the NISD 2.0 Proposal, NCAs may advice controlled disclosure, which in practice can only be effective if information is held back from the general public to allow time to patch systems. The conflict is not trivial due to protection goals that might be in competition. In order to trade off the interests of OESs, DSPs and data subjects, NCAs and DPAs need to collaborate. However, such collaboration is currently not mandatory under EU law. The conflict could also be alleviated if the normative provisions of the GDPR are aligned and provide for a precise justification for delaying information of data subjects in the case of contravening interests of law enforcement, or interests of the data controller concerned in responding adequately to the incident.

Acknowledgment

The research for this article was funded by the Luxembourg National Research Fund (FNR) C18/IS/12639666/EnCaViBS/Cole, https://www.fnr.lu/projects/the-eu-nis-directive-enhancing-cybersecurity-across-vital-business-sectors-encavibs/.

69 Cf. Recital 52 NIS 2.0 Proposal.

70 Inter alia Microsoft, bitkom, Digitaleurope.

71 See e.g. Sebastian Artz, 'Position Paper "Roadmap NIS-Review Bitkom Views Concerning the Combined Evaluation Roadmap / Inception Impact Assessment' (*Bitkom,* 13 August 2020) <https://www.bitkom.org/sites/default/files/2020-08/bitkom_positionpaper_nis_roadmap_final_200813.pdf> last accessed 26 August 2021; and European Banking Authority, 'Guidelines on major incident reporting under Directive (EU) 2015/2366 (PSD2)' Final Report (*EBA*, 27 July 2017) <https://www.eba.europa.eu/documents/10180/1914076/Guidelines+on+incident+reporting+under+PSD2+%28EBA-GL-2017-10%29.pdf/3902c3db-c86d-40b7-b875-dd50eec87657> last accessed 26 August 2021.

72 Recital 56 NIS 2.0 Proposal.

Transborder Transfer of Personal Data in Turkish Personal Data Protection Law

by **Sevde Pelen***

Abstract: Transborder data transfer is a challenging matter in Turkey, as well as in other countries and the EU. The most common problem is dealing with this issue detached from today's global economic system and with a prohibitive approach. Since 6698 numbered Law on Personal Data Protection entered into force in Turkey in 2016, the transborder transfer of personal data has become one of the most difficult subjects of legal compliance projects carried out with companies. There are many reasons for this, such as the problems experienced in the full and accurate perception of personal data, introduction of a new legislation in Turkey for data protection through the Law on Personal Data Protection, the fact that this field can be handled detached from today's global economic system, the ambiguity of some provisions and the vague matters. Within the scope of this article, the provisions regarding the transborder transfer of personal data in Turkish law and the developments in practice since the Law on Personal Data Protection entered into force are examined. Thus, it is aimed towards those who would like to follow the relevant legislation and practice in Turkey. For this purpose, in Chapter B, the relevant legislation in Turkish law and the Council of Europe conventions and protocols that interact with both Turkish and EU law are examined. In Chapter C, transborder transfer of personal data practice in Turkey is examined in the light of Personal Data Protection Board decisions.

Keywords: Turkish Law on Personal Data Protection; personal data protection; transborder transfer; Turkish law

Recommended citation: Sevde Pelen, Transborder Transfer of Personal Data in Turkish Personal Data Protection Law, 12 (2021) JIPITEC 458 para 1

A. Introduction

1 Since 6698 numbered Law on Personal Data Protection ("PDP Law") entered into force on 24 March 2016, the transborder transfer of personal data has been a challenging and confusing issue in Turkey. Due to the size of this confusion, the transborder transfer of personal data has become one of the most difficult subjects of the PDP Law compliance projects carried out with companies. While lawyers aim to eliminate all the legal risks and establish the order required by the current system, these efforts are criticized by company executives as incompatible with today's global economic system. In addition, it is characterized as the product of an extremely idealistic approach that is disconnected from reality and can cause serious loss of customers and income. With regard to the transborder transfer of personal data, where the aforementioned two attitudes are in conflict, company executives started to choose between the risk of loss of customers and income, and the risk of administrative fines.

2 The Personal Data Protection Authority seeks to establish a balance between the right to protect personal data and the data-based economy in the PDP Law[1] and the doctrine emphasizes it's importance.[2]

* Sevde Pelen, Istanbul Bar Association.

1 Personal Data Protection Authority, '100 Soruda Kişisel Verilerin Korunması Kanunu (Law on Personal Data Protection in 100 Questions)' <https://kvkk.gov.tr/SharedFolderServer/CMSFiles/7d5b0a2f-e0ea-41e0-bf0b-bc9e43dfb57a.pdf> accessed 17 April 2020.

2 Berna Akçalı Gür, 'Uluslararası Hukuk ve AB Hukuku Boyutuyla Kişisel Verilerin Yurt Dışına Aktarılması (Transborder

Nevertheless, it is not always easy to establish this balance in practice. As the outcome of this controversial situation, the decision of the Personal Data Protection Board regarding Amazon Turkey[3] is of great importance for companies transferring personal data from Turkey to third countries. At the time this decision was taken, there were some expectations and criticism arising from this controversial situation. Besides, the authorization process of Amazon Turkey's undertakings regarding legality of its transborder transfers had not been concluded. Despite this, the Personal Data Protection Board imposed a large amount of administrative fines on Amazon Turkey, that were based on various violations including transborder transfer of personal data.[4]

3 The transborder transfer of personal data turned into a risky phenomenon in Turkey due to several reasons. For instance, there is misunderstanding and misperception of personal data and its protection because the PDP Law is new legislation in Turkey. Furthermore, this field can be handled detached from today's global economic system. Additionally, some provisions of the PDP Law are ambiguous, and there are vague matters.

4 One of the most significant matters in this field, which is commonly overlooked, is that the fourth industrial revolution, known as Industry 4.0 or the digital revolution, has been experienced in the history of humanity.[5] As a result of this digital revolution, the network society has been formed and the data economy has emerged.[6] Today's global economy is closely linked to transborder data transfers especially due to digital trade.[7] Statistical and detailed reports reveal the speed of digitalization of the world and the boosting effect of global data flows and their importance in the global economy.[8] Moreover, the Covid-19 pandemic has caused the speed of digitalization in the world to increase exponentially and humanity to move to a new phase.[9] Therefore, personal data are now considered crucial raw materials of the global economy.[10]

5 Due to the lack of harmonized global rules on personal data protection, the transborder data flows especially through social networks, search engines, cloud computing, etc. can cause several business, technology, and security challenges.[11] All these developments put increasing pressure on regulatory systems.[12] As a result, it is generally accepted that law cannot keep up with the speed of technology, but

Transfer of Personal Data with the Dimension of International Law and EU Law)' (2019) 25 (2) Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, 850.

3 27.02.2020 dated and 2020/173 numbered decision of Personal Data Protection Board <https://www.kvkk.gov.tr/Icerik/6739/2020-173> accessed 23 April 2021.

4 For more detailed information on this decision see "Board decision on Amazon Turkey" titled chapter C.III.

5 Gediz Kocabaş, *KVKK'da Yer Alan Kurum ve Kavramların TMK ve Kıta Avrupası Hukuk Sistemi Kapsamında Değerlendirilmesi (Evaluation of Authorities and Terms in the PDP Law within the Scope of Turkish Civil Code and Continental European Legal System)* in Leyla Keser Berber and Ali Cem Bilgili (eds), *Güncel Gelişmeler Işığında Kişisel Verilerin Korunması Hukuku (Law on Protection of Personal Data in the Light of Current Developments)* (On İki Levha Yayınları 2020) 83.

6 Mehmet Bedii Kaya, *Kişisel Verilerin İşlenmesi ve Korunması Arasındaki Denge (Balance between Processing and Protecting Personal Data)* in Leyla Keser Berber and Ali Cem Bilgili (eds), *Güncel Gelişmeler Işığında Kişisel Verilerin Korunması Hukuku (Law on Protection of Personal Data in the Light of Current Developments)*, (On İki Levha Yayınları 2020) 33, 34.

7 Svetlana Yakovleva/Kristina Irion, 'Pitching Trade Against Privacy: Reconciling EU Governance of Personal Data Flows with External Trade' (2020) 10 (3) International Data Privacy Law 201.

8 IDC, 'The Digitization of the World: From Edge to Core' (2018) 2-26 <https://resources.moredirect.com/white-papers/idc-report-the-digitization-of-the-world-from-edge-to-core> accessed 10 April 2021; McKinsey & Company, 'Digital Globalization: The New Era of Global Flows' (2016) 1-41 <https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20globalization%20The%20new%20era%20of%20global%20flows/MGI-Digital-globalization-Full-report.ashx> accessed 10 April 2021.

9 McKinsey & Company, 'How Covid-19 Has Pushed Companies over the Technology Tipping Point—And Transformed Business Forever' (2020) <https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever#> accessed 10 April 2021; International Telecommunication Union, 'Economic Impact of Covid-19 on Digital Infrastructure' (2020) 3-6 <https://www.itu.int/en/ITU-D/Conferences/GSR/2020/Documents/GSR-20_Impact-COVID-19-on-digital-economy_DiscussionPaper.pdf> accessed 10 April 2021.

10 Christopher Kuner, 'Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future' (2011) 187 OECD Digital Economy Papers 1, 10.

11 Rolf H. Weber, 'Transborder Data Transfers: Concepts, Regulatory Approaches and New Legislative Initiatives' (2013) 3 (2) International Data Privacy Law, 117, 118.

12 Christopher Kuner, 'Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future' (2011) 187 OECD Digital Economy Papers 1, 8.

as Christopher Kuner emphasizes, the key question is how we can speed up the conversion of legal thinking and knowledge into appropriate legal principles and rules.[13] It should be noted that the data ecosystem is undergoing tremendous changes all over the world, and in this context, laws that provide for the protection of personal data, including the General Data Protection Regulation (GDPR), which many countries take as a point of reference[14], are criticized for failing to protect the data subjects.[15] As some of these difficulties are global, it is important to closely follow up examples and developments in the world and to discuss how to reach more effective and balanced results by criticizing legislation and practice.

6 Within the scope of this article, the legislation and practice in Turkish law in the scope of transborder transfer of personal data are examined. In this context, in chapter B, the relevant legislation in Turkish law and the Council of Europe (CoE) conventions and protocols that interact with both Turkish and EU law are examined. In chapter C, the practice of transborder data transfer in Turkey is examined in the light of Personal Data Protection Board decisions.

B. Legislation, Conventions and Protocols

7 The legislation on the protection of personal data in Turkish law is based on EU law. Moreover, CoE conventions and protocols are of special importance due to the membership of Turkey to the CoE and the CoE's aim of creating internationally accepted, uniform norms that go beyond the borders of the EU in the field of personal data protection.

8 In this chapter, the transborder transfer of personal data shall be examined limited to the legislation in Turkey and conventions and protocols of the CoE, that have direct effect on Turkish law.

13 Christopher Kuner et al, 'The (data privacy) law hasn't even checked in when technology takes off' (2014) 4 (3) International Data Privacy Law, 175, 176.

14 European Commission, 'Digital Single Market – Communication on Exchanging and Protecting Personal Data in a Globalised World Questions and Answers' <https://ec.europa.eu/commission/presscorner/detail/en/MEMO_17_15> accessed 11 March 2021.

15 Christopher Kuner et al, 'If the legislature had been serious about data privacy...' (2019) 9 (2) International Data Privacy Law 75, 77.

I. Legislation in Turkey

9 The protection of personal data does not have a long history in Turkish law. Provisions regarding processing personal data were included into the Constitution of the Republic of Turkey as the third paragraph of Article 20 titled "privacy of private life" in 2010. Furthermore, the Turkish Penal Code No 5237, which entered into force on 1 June 2005, contains provisions regarding the protection of personal data. However, as the main law that is solely regulating personal data protection, the PDP Law entered into force upon its publication in the Official Gazette on 7 April 2016.[16]

10 Transborder transfer of personal data is primarily regulated under the PDP Law. However, there are some other laws regulating this area for specific situations.

1. Law on Personal Data Protection

11 When the PDP Law entered into force, Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Directive) was in force in the EU. At that time, the GDPR was in draft form. Nevertheless, it was published less than one month later in Official Journal of the European Union and repealed the Directive upon its entering into force in May 2018.[17] GDPR brought important innovations regarding the transfer of personal data to third countries and international organizations. Since the PDP Law[18] is mainly based on the Directive, it does not include the innovations and the detailed provisions regulated under the GDPR.

12 Nonetheless, the PDP Law is of great importance in terms of Turkish law as the first law that directly regulates personal data protection. It also introduces new institutions that play an important role in data protection in Turkey: the Personal Data Protection Authority (Authority) and the Personal Data Protection Board (Board). The Authority and its organization regulated under the sixth chapter of the PDP Law are among the regulatory and supervisory in-

16 <https://www.resmigazete.gov.tr/eskiler/2016/04/20160407.htm> accessed 7 June 2021.

17 <https://op.europa.eu/en/publication-detail/-/publication/99caafe9-11bc-11e6-ba9a-01aa75ed71a1/language-en> accessed 7 June 2021.

18 For the official English translation of the PDP Law see <https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/aea97a33-089b-4e7d-85cb-694adb57bed3.pdf> accessed 7 March 2021.

stitutions.[19] Moreover, the Authority is registered as the authority regulated under Article 13(2) of Convention 108.[20] Within the Authority, which has administrative and financial autonomy[21], there is the Board, which performs and uses its duties and authorities independently under its own liability.[22] Article 22 of the PDP Law regulates various duties and powers of the Board, such as deciding on complaints, taking temporary measures, and deciding on administrative sanctions. Decisions taken by the Board can be divided into four groups in terms of their nature: (i) decision to stop data processing and transfer, (ii) instruction decision to eliminate the violation, (iii) administrative fine decision, and (iv) principal decision.[23] A Board decision may include a provision regarding one or more of these groups for the same or different reasons, because these decisions are not alternatives to each other.[24]

13 Regarding the transborder transfer of personal data, the provisions of the PDP Law on definitions and categories of transfers of personal data, conditions of transborder transfer and serious harm on interests of Turkey and the person concerned are particularly to be taken into consideration.

a) Definitions and categories of transfers of personal data

14 The PDP Law defines personal data as "*all the information relating to an identified or identifiable natural person*"[25] and divides personal data into two categories: personal data of normal nature and personal data of special nature. The conditions of processing these two categories of personal data are regulated differently under separate articles.[26]

15 The PDP Law does not define the term personal data transfer as in the Directive and GDPR. The fact that personal data goes outside the borders of Turkey is considered sufficient for transborder transfer, and transfer to a third party is not considered as a condition[27].

16 Within the scope of the PDP Law, the transfer of personal data is divided into two categories as transfer within Turkey and transfer outside of Turkey (transfer abroad or transborder transfer). These two categories of transfers are regulated under two different articles.[28] The transborder transfer of personal data of both normal and specific natures is regulated under "Transfer of Personal Data Abroad" titled Article 9 of the PDP Law.

b) Conditions of transborder transfer of personal data

17 In the PDP Law, it is essential that personal data is not transferred abroad without the explicit consent of the data subject concerned.[29] However, the exemptions from this rule are regulated under Article 9(2) of the PDP Law. Accordingly, provided that one of the compliance conditions for processing

19 Cemal Başar, 'Türk İdare Hukuku ve Avrupa Birliği Hukuku Işığında Kişisel Verilerin Korunması (Protection of Personal Data in Turkish Administrative Law and EU Law)' (PhD Thesis, Dokuz Eylül Üniversitesi 2019) 150.

20 <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/declarations?p_auth=YP6ZdjNO&_coeconventions_WAR_coeconventionsportlet_enVigueur=false&_coeconventions_WAR_coeconventionsportlet_searchBy=state&_coeconventions_WAR_coeconventionsportlet_codePays=TUR&_coeconventions_WAR_coeconventionsportlet_codeNature=3> accessed 23 April 2021.

21 PDP Law Article 19(1).

22 PDP Law Article (1).

23 Samet Saygı, '6698 Sayılı Kanunun Sistematiğinde Yargısal Başvuru Yolları (Judicial Remedies in the Systematics of Law No. 6698)' 2020 2 (2) Kişisel Verileri Koruma Dergisi 30, 44-54.

24 Samet Saygı, '6698 Sayılı Kanunun Sistematiğinde Yargısal Başvuru Yolları (Judicial Remedies in the Systematics of Law No. 6698)' 2020 2 (2) Kişisel Verileri Koruma Dergisi 30, 49.

25 PDP Law Article 3(1)(d).

26 PDP Law Articles 5 and 6.

27 Murat Volkan Dülger, *Kişisel Verilerin Korunması Hukuku (Personal Data Protection Law)* (3. Edition, Hukuk Akademisi 2020) 437-438.

28 PDP Law Articles 8 and 9.

29 PDP Law Article 9(1).

personal data of normal[30] or special nature[31] exists, the personal data can be transferred abroad on the basis of fulfilling one of the conditions set forth under Article 9(2). These conditions are as follows:

i. Adequate level of protection is provided in the foreign country where the data is to be transferred,

ii. The controllers in Turkey and in the related foreign country undertake an adequate level of protection in writing and the Board has authorized such transfer, where adequate level of protection is not provided.

18 The PDP Law does not include specific provisions regarding the derogations and appropriate safeguards, apart from written undertakings. Additionally, explicit consent has become the most widely used transfer mechanism. In order to understand the role given to the explicit consent in Turkey and how the practice is mainly based on the explicit consent, it is first essential to understand how the other transfer mechanisms are regulated and implemented in practice in Turkey.

30 The conditions of processing personal data of normal nature without the explicit consent of the data subject concerned are regulated as follows under Article 5(2) of the PDP Law: (i) it is clearly provided for by the laws; (ii) it is mandatory for the protection of life or physical integrity of the person or of any other person who is bodily incapable of giving his consent or whose consent is not deemed legally valid; (iii) processing of personal data belonging to the parties of a contract, is necessary provided that it is directly related to the conclusion or fulfilment of that contract; (iv) it is mandatory for the controller to be able to perform his legal obligations; (v) the data concerned is made available to the public by the data subject himself; (vi) data processing is mandatory for the establishment, exercise or protection of any right; (vii) it is mandatory for the legitimate interests of the controller, provided that this processing shall not violate the fundamental rights and freedoms of the data subject.

31 The conditions of processing personal data of special nature without the explicit consent of the data subject concerned are regulated as follows under Article 6(3) of the PDP Law: Personal data, excluding those relating to health and sexual life, listed in the first paragraph may be processed without seeking explicit consent of the data subject, in the cases provided for by laws. Personal data relating to health and sexual life may only be processed, without seeking explicit consent of the data subject, by any person or authorised public institutions and organizations that have confidentiality obligation, for the purposes of protection of public health, operation of preventive medicine, medical diagnosis, treatment and nursing services, planning and management of health-care services as well as their financing.

(aa) Adequate level of protection

19 It is regulated under Article 9(3) of the PDP Law that the Board shall determine and announce the countries where adequate level of protection is provided. In this regard, the Board shall take into consideration the following factors[32]:

i. The international conventions to which Turkey is a party,

ii. The state of reciprocity concerning data transfer between the requesting country and Turkey,

iii. The nature of the data, the purpose and duration of processing regarding each concrete, individual case of data transfer,

iv. The relevant legislation and its implementation in the country to which the personal data is to be transferred,

v. The measures guaranteed by the controller in the country to which the personal data is to be transferred.

20 If needed, the Board shall decide upon receiving the opinions of related public institutions and organisations.[33]

21 Additionally, on 2 May 2019, the Board disclosed its criteria for countries with adequate levels of protection.[34] Through this decision, the Board created a detailed table regarding the criteria regulated in the PDP Law and ensured transparency on this subject. The criteria set forth by this decision are as follows[35]:

i. Reciprocity status,

ii. Legislation of the relevant country and implementation of this legislation regarding the processing of personal data,

(a) Personal data protection is a constitutional right,

32 PDP Law Article 9(4).

33 PDP Law Article 9(4).

34 02.05.2019 dated and 2019/125 numbered decision of Personal Data Protection Board <https://www.kvkk.gov.tr/Icerik/5469/-Yeterli-korumanin-bulundugu-ulkelerin-tayininde-kullanilmak-uzere-olusturulan-form-hakkindaki-02-05-2019-tarihli-ve-2019-125-sayili-Kurul-Karari> accessed 23 April 2021.

35 <https://kvkk.gov.tr/SharedFolderServer/CMSFiles/93aa4e79-816f-4383-8377-a6e9f8a7574c.pdf> accessed 7 June 2021.

(b) The existence of a basic law on the personal data protection,

(c) Effective date of the basic law,

(d) Secondary regulations and compliance of these regulations with our legislation,

(e) Basic concepts of personal data protection,

(f) General principles on the personal data protection,

(g) Compliance of the personal data processing conditions with the personal data processing conditions in the PDP Law,

(h) Existence of specific processing conditions and additional security measures for the processing of personal data of special nature,

(i) Existence of legal guarantees that personal data processing activities are carried out in accordance with the principle of transparency,

(j) Obligation to take the necessary technical and organizational measures to provide the adequate level of security in order to prevent unlawful processing and access to personal data and to ensure the protection of personal data,

(k) Implementation status of administrative and/or penal sanctions against the data breach and other mechanisms to prevent data breach,

(l) Rights of data subject,

(m) The right to request of data subjects to the controller and the right to lodge complaint with to the data protection authority,

(n) The right to compensation of data subjects whose rights on personal data have been violated according to the general provisions,

(o) Implementation guidelines/publications as reference,

(p) Exemptions to the implementation of the Law,

(q) Data transfer system,

iii. Existence of an independent data protection authority,

(a) Structure,

(b) Independence status,

(c) Duties and powers,

(d) Its authority to audit/investigate,

(e) Whether there is a remedy to appeal against its decisions,

iv. The status of being a party in the international agreeme nts on personal data protection and being a member of international organizations,

(a) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data No. 108,

(b) Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows No.181,

(c) Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (CETS 182),

(d) European Convention on Human Rights,

(e) International Conference of Data Protection and Privacy Commissioners (ICDPPC),

(f) Global Privacy Enforcement Network (GPEN),

v. Whether a member of global and regional organizations that Turkey is a member,

vi. Trade volume with relevant country,

vii. Other.

22 Among these criteria, which largely overlap with the criteria in Article 45 of the GDPR, criterion on the trade volume with the concerned country and reciprocity criterion are worrisome.[36] For instance, the reciprocity criterion raises the question: whether EU member states shall not be accepted as the countries with appropriate level of protection. Considering that GDPR is a much more detailed and advanced legislation than the PDP Law, this result would be unlikely. However, due to this reciprocity criterion, the key questions are whether Turkey shall be accepted as a country with appropriate level of protection in accordance with the GDPR; and if not, whether this reciprocity criterion shall avoid EU member states from being recognized as

36 Murat Volkan Dülger, *Kişisel Verilerin Korunması Hukuku (Personal Data Protection Law)* (3. Edition, Hukuk Akademisi 2020) 447.

the countries with appropriate level of protection in accordance with the PDP Law. At this point there is a conflict between the protection of human rights in the scope of personal data protection and commerce as well as politics. Furthermore, the criterion on the trade volume raises the same worries of seeing the commercial and political dimensions of the adequacy decision.[37]

23 These two criteria and the critics they bring along are reminiscent of the relationship between the EU and the USA. Even though, the EU and the USA tried to find a solution to their situation, which would not affect the commercial relationship between them, first through the Safe Harbour Agreement[38] and then through the Privacy Shield Agreement[39], these agreements were repealed by Schrems I[40] and then Schrems II[41] judgements of the Court of Justice of the EU. Hence, the conflict between data protection and commercial and political relationships is not an issue specific to Turkey, but a global one.

24 Besides, probably the most important issue regarding this transfer mechanism in Turkey is the fact that the Board has not announced any countries with the adequate level of protection.

25 The announcement of the Authority on 26 October 2020 is significant because it replies to critics from Turkey regarding this subject.[42] The Authority stated that as of the date of the announcement, there has been no application made to the Authority by the other countries to be appointed as the country with the adequate level of protection. Besides, the Authority stated that the negotiations with the other countries in this regard are carried out in consideration of the existing and potential commercial relationships, geographical and/or cultural ties and political/diplomatic relationships and by the collaboration of the Ministries of Justice, Foreign Affairs and Commerce. Moreover, the Authority explicitly underlined that the reciprocity criterion is obligatory within these negotiations.[43]

26 Considering this announcement, it could be estimated that in the near future there will be no announcement of the countries with the adequate level of protection. Therefore, this transfer mechanism is not applicable in Turkey.

(bb) Undertakings

27 In the PDP Law, not the term "standard contractual clauses", but the term "undertakings" is used, which is regulated under Article 9(2)(b). The Board published two different sets of the clauses to be included into the undertakings as the minimum standards within scope of transborder transfers of personal data.[44] One set is for transfers from the controller to the controller, and the other is for the transfers from the controller to the processor. These undertakings do not contain the transfers made by a processor to another processor or a controller.

28 The most significant difference of these undertakings from the standard contractual clauses regulated under GDPR is that the clauses contained by these sets are amendable examples open to negotiations. Moreover, regardless of the amendments made in the sets of undertakings, all the undertakings must be submitted to the Board for the concerned transborder transfer to be authorized by the Board.

29 On 7 May 2020, the Board published an announcement regarding the matters to be considered in the undertakings to be prepared for the transborder transfer of personal data.[45] This announcement aims to prevent common deficiencies and mistakes

37 ibid.

38 <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ%3AL%3A2000%3A215%3A0007%3A0047%3AEN%3APDF> accessed 11 April 2021.

39 <https://ec.europa.eu/info/sites/default/files/celex_32016d1250_en_txt.pdf> accessed 11 April 2021.

40 CJEU, Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015].

41 CJEU, Case C-311/18 Maximillian Schrems, Facebook Ireland Ltd v Data Protection Commissioner [2020].

42 Personal Data Protection Authority, 'Yurt Dışına Veri Aktarımı Kamuoyu Duyurusu (Public Announcement on Transborder Transfer of Data)' (2020) <https://kvkk.gov.tr/Icerik/6828/YURTDISINA-VERI-AKTARIMI-KAMUOYU-DUYURUSU> accessed 23 April 2021.

43 ibid.

44 Personal Data Protection Board, 'Taahhütnameler: Veri Sorumlusundan Veri Sorumlusuna Aktarım, Veri Sorumlusundan Veri İşleyene Aktarım (Undertakings: Transfer from Data Controller to Data Controller, Transfer from Data Controller to Data Processor)' (2020) <https://www.kvkk.gov.tr/Icerik/5255/Taahhutnameler> accessed 23 April 2021.

45 Personal Data Protection Authority, 'Yurt Dışına Kişisel Veri Aktarımında Hazırlanacak Taahhütnamelerde Dikkat Edilmesi Gereken Hususlara İlişkin Duyuru (Announcement on the Matters to be Considered in the Undertakings to be Prepared for the Transborder Transfer of Personal Data)' (2020) <https://www.kvkk.gov.tr/Icerik/6741/YURT-DISINA-KISISEL-VERI-AKTARIMINDA-HAZIRLANACAK-TAAHHUTNAMELERDE-DIKKAT-EDILMESI-GEREKEN-HUSUSLARA-ILISKIN-DUYURU> accessed 23 April 2021.

in the applications for authorization of transborder transfer of personal data through submitting an undertaking to the Board. The issues are divided into three categories: procedural ones, meritorious ones, and matters to be considered in the explanations given under the headings in the annex of the commitments.

30 As of August 2021, the Board announced its authorization of four transborder transfers upon reviewing the submitted undertakings, and the first authorization announcement was dated 9 February 2021.[46] Due to the delay in consideration process of the applications and the long interval between the first authorization date and the effective date of the PDP Law, this mechanism has not been an effective and fast-paced choice.

(cc) Binding corporate rules

31 On 10 April 2020, the Board published an announcement on binding corporate rules (BCR) and stated that BCR may be used within the principles set forth by the Board as the alternative mechanism for the transborder transfer of personal data.[47] The Board justified this due to the inadequacy of the undertakings in regard of the data transfers made between multinational groups of companies.

32 This parallels the development of the BCR in the EU where in the Directive, it was also not an explicitly regulated transfer mechanism. Article 29 Working Party determined the BCR as a transfer mechanism based on Article 26(2) of the Directive. This article regulates adequate safeguards without naming directly BCR and without limiting the mechanisms. As for the situation in Turkey, the adequate safeguard term is not used within the PDP Law. Instead, Article 9(2)(b) of the PDP Law regulates written undertakings. The Board based BCR on this article,[48] which proves that this undertaking term is to be broadly interpreted and can contain any written alternative safeguard mechanisms, such as standard contractual clauses and BCR. The Board defines BCR as follows:

> *Binding Corporate Rules are data protection policies used for the transfer of personal data for the multinational group of companies operating in countries where adequate level of protection is not provided and that enable them to commit adequate level of protection in writing.*[49]

33 In the annex of the relevant announcement, there are an auxiliary document regarding the main points to be included in BCR and an application form. The main points to be included in BCR are gathered under seven main topics: (i) binding nature, (ii) effectiveness, (iii) cooperation with the Authority, (iv) processing and transfer of personal data, (v) mechanisms for reporting and recording changes, (vi) data security, (vii) accountability and other tools.[50] This table is like a literal translation of a working document of the Article 29 Working Group,[51] with a few changes and additions. Although the Board preferred this method, it was criticized for not being original and causing other problems in practice.[52]

34 While the Board's adoption of the BCR is an important step due to its simplifying effect on the transborder transfers made among the multinational group of companies, it is criticized for not being sufficient to solve the problems in practice and to prevent illegal transfers.[53] Moreover, it is criticized for requiring a great deal of effort and time to put into practice,

46 <https://www.kvkk.gov.tr/Icerik/6867/TAAHHUTNAME-BASVURUSU-HAKKINDA-DUYURU> accessed 23 April 2021; <https://www.kvkk.gov.tr/Icerik/6898/TAAHHUTNAME-BASVURUSU-HAKKINDA-DUYURU> accessed 23 April 2021; <https://kvkk.gov.tr/Icerik/6985/TAAHHUTNAME-BASVURUSU-HAKKINDA-DUYURU> accessed 15 September 2021.

47 Personal Data Protection Authority, 'Bağlayıcı Şirket Kuralları Hakkında Duyuru (Announcement on Binding Corporate Rules)' (2020) <https://www.kvkk.gov.tr/Icerik/6728/YURT-DISINA-KISISEL-VERI-AKTARIMINDA-BAGLAYICI-SIRKET-KURALLARI-HAKKINDA-DUYURU> accessed 23 April 2021.

48 ibid.

49 ibid Application Form 2.

50 ibid main points to be included in BCR.

51 Article 29 Working Party, 'Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules' (2008) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp153_en.pdf> accessed 23 April 2021.

52 Murat Volkan Dülger/Cansu Ceren Kahraman, 'KVKK'dan Kişisel Verilerin Yurt Dışına Aktarımında Önemli Bir Adım: Bağlayıcı Şirket Kuralları (An Important Step in Transborder Transferring of Personal Data: Binding Company Rule)' (2021) 6 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3792375> accesed 23 April 2021.

53 ibid 6-7; Murat Volkan Dülger, 'Kişisel Verileri Koruma Kurulu'nun 108 Sayılı Sözleşme Hakkındaki Kararı ve Yurt Dışına Veri Aktarımı Sorunu (Decision of Personal Data Protection Board about Nr. 108 Agreement and Problem about Data Transfer to Abroad)' (2021) 5-6 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3792396> accessed 23 April 2021; Murat Volkan Dülger, *Kişisel Verilerin Korunması Hukuku (Personal Data Protection Law)* (3. Edition, Hukuk Akademisi 2020) 455.

and for being suitable for a limited number of controllers.[54]

35 As of August 2021, there has been no announcement by the Board, regarding authorization of transborder transfers of personal data upon submission of BCR.[55]

(dd) Explicit consent

36 The PDP Law defines explicit consent as freely given, specific, and informed consent.[56] Unlike GDPR, there is no specific article setting forth the conditions of consent in the PDP Law. However, the definition in the PDP Law sets forth three conditions for the explicit consent, which are discussed in the Explicit Consent titled Guideline of the Authority[57]: (i) freely given, (ii) being specific, (iii) informing the concerned data subject before taking the consent.

37 In order for a consent to be freely given, the Authority requires that the consenting data subject must be aware of this behaviour and this consent should be based on their decision. If the parties are not equal to each other, then it carries more importance to examine whether consent is freely given. Furthermore, consent cannot be a prerequisite for providing a service or goods.[58]

38 The Authority relates the condition of being specific to consent being related to and limited with a specific subject. Therefore, it should be clear which specific subject the consent is related to, and general or ambiguous statements are not consent in compliance with the PDP Law.[59]

39 The Authority emphasizes the importance of providing information to the concerned data subject in a clear and understandable manner before processing the data. Moreover, the Authority warns against the terms that may not be understood by the data subjects and unreadably small font sizes in written information forms.[60] However, unlike GDPR, it is not obligatory to inform the data subject about the possible risks of the concerned transborder transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards before taking the consent of the data subject.

40 In the EU law, explicit consent is among the derogations, which are to be strictly interpreted.[61] Moreover, the doctrine emphasizes that consent is not the silver bullet.[62] It is debatable whether consent is freely given and whether the data subject understands on which subject they consent, and it is not a reliable method as it can be withdrawn by the concerned data subject at any time.[63] Considering all

54 Murat Volkan Dülger/Cansu Ceren Kahraman, 'KVKK'dan Kişisel Verilerin Yurt Dışına Aktarımında Önemli Bir Adım: Bağlayıcı Şirket Kuralları (An Important Step in Transborder Transferring of Personal Data: Binding Company Rule)' (2021) 6-7 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3792375> accesed 23 April 2021; Murat Volkan Dülger, 'Kişisel Verileri Koruma Kurulu'nun 108 Sayılı Sözleşme Hakkındaki Kararı ve Yurt Dışına Veri Aktarımı Sorunu (Decision of Personal Data Protection Board about Nr. 108 Agreement and Problem about Data Transfer to Abroad)' (2021) 5-6 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3792396> accessed 23 April 2021; Murat Volkan Dülger, *Kişisel Verilerin Korunması Hukuku (Personal Data Protection Law)* (3. Edition, Hukuk Akademisi 2020) 455.

55 <https://kvkk.gov.tr/Search?keyword=bağlayıcı%20şirket%20kuralları&langText=tr> accessed 15 September 2021.

56 PDP Law Article 3(1)(a).

57 <https://kvkk.gov.tr/SharedFolderServer/CMSFiles/66b2e9c4-223a-4230-b745-568f096fd7de.pdf> accessed 7 March 2021.

58 Personal Data Protection Board, 'Açık Rıza (Explicit Consent)' 5-6 <https://kvkk.gov.tr/SharedFolderServer/CMSFiles/66b2e9c4-223a-4230-b745-568f096fd7de.pdf> accessed 01.04.2018.

59 ibid 4.

60 ibid 5.

61 Article 29 Working Party, 'Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995' (2005) 7 <https://www.pdpjournals.com/docs/88080.pdf> accessed 23 April 2021.

62 Kirill Albrecht/Kareen Lee Lust, 'GDPR Series: International Data Transfers - A High Level Review' (2017) Thomson Reuters UK Westlaw, <https://0-uk-westlaw-com.opac.bilgi.edu.tr/Document/I6A4FE8F0E71911E79CABC75D43EB17D0/View/FullText.html? navigationPath=Search%2Fv1%2Fresults%2Fnavigation%2Fi0ad62af00000017812d031ca9497f551%3Fppci%3D6c60aa16de1f41e79c6d042da8b3ce42%26Nav%3DRESEARCH_COMBINED_WLUK%26fragmentIdentifier%3DI6A4FE8F0E71911E79CABC75D43EB17D0%26parentRank%3D0%26startIndex%3D1%26contextData%3D%2528sc.Search%2529%26transitionType%3DSearchItem&listSource=Search&listPageSource=25e244b923ec2d22fe56b2baf08669ca&list=RESEARCH_COMBINED_WLUK&rank=3&sessionScopeId=6ad8a701e66706646be48252f2f7d6ddcaf651813e2177763894386479f5832d&ppcid=6c60aa16de1f41e79c6d042da8b3ce42&originationContext=Search%20Result &transitionType=SearchItem&contextData=%28sc.Search%29> accessed 8 March 2021.

63 Nikolaos I. Theodorakis, 'Cross Border Data Transfers Under the GDPR: The Example of Transferring Data from the EU to the US' (2018) TTLF Working Papers No. 39, 44 < https://law.stanford.edu/publications/no-39-cross-border-data-

these disadvantages, it is seen that explicit consent is not a frequently preferred method for transborder transfer of data in the EU,[64] and this contradicts with practice in Turkey.

41 In practice in Turkey, companies do not have many options as a transfer mechanism. The adequate level of protection is not an applicable transfer mechanism. Moreover, the slow authorization process of the undertakings and BCR has resulted in a long-term uncertainty of legal basis for the transborder transfers made by the applicants. As seen from the few authorization announcements regarding the undertakings and BCR,[65] these transfer mechanisms are also not widely implemented in practice. Additionally, through the Board decision on Convention 108,[66] it was also clarified that international agreements such as Convention 108 cannot be the sole legal basis for transborder transfers. Consequently, the most implemented transfer mechanism in practice has been to obtain explicit consent of the data subject, despite the fact that it is found risky both by the Board[67] and in the doctrine.[68]

42 In addition to unreliability of explicit consent as a transfer mechanism, it requires companies to adjust their infrastructures, location of databases, computer programs, and business relations in such a way that if explicit consent is not obtained or is withdrawn, the personal data of the related data subject can still be processed within the borders of Turkey without transborder transfer. However, such a change is often not practical, easy, or cheap particularly for large-scale companies. Moreover, requesting explicit consent from the customers instead of using other transfer mechanisms for the transborder transfers can cause a loss of customers and income in many cases. Consequently, company executives started to choose between the risk of losing customers and income versus the risk of administrative fines.

c) Serious harm on interests of Turkey and the person concerned

43 The PDP Law regulates that in cases where the interests of Turkey and the person concerned would be seriously harmed, personal data can be transferred abroad with the permission of the Board, only by obtaining the opinions of the relevant public institution or organization. However, in this case, the provisions of international conventions are

transfers-under-the-gdpr-the-example-of-transferring-data-from-the-eu-to-the-us/> accessed 8 March 2021; Christopher Kuner, 'Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future' (2011) 187 OECD Digital Economy Papers 1, 21-22.

64 Bilgi Information Technology Law Institute, 'Kişisel Verilerin Korunmasına İlişkin Düzenlemeler Çerçevesinde Uluslararası Veri Aktarımı, Güncel Gelişmeler ve Uygulamaya İlişkin Hukuki Değerlendirmeler (Legal Evaluations Regarding International Data Transfer, Current Developments and Practice within the Framework of the Regulations on the Protection of Personal Data)' (2020) 28 <https://itlaw.bilgi.edu.tr/media/2020/3/30/Final%20Veri_Aktarimi_Raporu_30.03.2020.pdf> accessed 8 March 2021.

65 <https://www.kvkk.gov.tr/Icerik/6867/TAAHHUTNAME-BASVURUSU-HAKKINDA-DUYURU> accessed 23 April 2021; <https://www.kvkk.gov.tr/Icerik/6898/TAAHHUTNAME-BASVURUSU-HAKKINDA-DUYURU> accessed 23 April 2021; <https://kvkk.gov.tr/Icerik/6985/TAAHHUTNAME-BASVURUSU-HAKKINDA-DUYURU> accessed 15 September 2021; <https://kvkk.gov.tr/Search?keyword=bağlayıcı%20şirket%20kuralları&langText=tr> accessed 15 September 2021.

66 For more detailed information on this decision see "Board decision on Convention 108" titled chapter C.IV.

67 Personal Data Protection Authority, 'Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular (Frequently Asked Questions About the Law on the Protection of Personal Data)' 25 <https://www.kvkk.gov.tr/Icerik/5412/Acik-Rizanin-Hizmet-Sartina-Baglanmasi> accessed 23 April 2021.

68 Nafiye Yücedağ, 'Medeni Hukuk Açısından Kişisel Verilerin Korunması Kanunu'nun Uygulama Alanı ve Genel Hukuka Uygunluk Sebepleri (General Legal Compliance Conditions and Field of Application of the Law on Protection of Personal Data in Terms of Civil Law)' (2017) 75 (2) İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, 765, 786; Nafiye Yücedağ, 'Kişisel Verilerin Korunması Kanunu Kapsamında Genel İlkeler (General Principles under the Law on the Protection of Personal Data)', (2019) 1 (1) Kişisel Verileri Koruma Dergisi 47, 50; Bilgi Information Technology Law Institute, 'Kişisel Verilerin Korunmasına İlişkin Düzenlemeler Çerçevesinde Uluslararası Veri Aktarımı, Güncel Gelişmeler ve Uygulamaya İlişkin Hukuki Değerlendirmeler (Legal Evaluations Regarding International Data Transfer, Current Developments and Practice within the Framework of the Regulations on the Protection of Personal Data)' (2020) 9 <https://itlaw.bilgi.edu.tr/media/2020/3/30/Final%20Veri_Aktarimi_Raporu_30.03.2020.pdf> accessed 8 March 2021; Elif Küzeci, *Kişisel Verilerin Korunması (Protection of Personal Data)* (4. Edition, On İki Levha Yayınları, 2020) 395.

reserved.[69] This provision is criticized for creating uncertainty, since there are no objective criteria for determining situations where the interest will be seriously harmed.[70]

2. Other laws regulating transborder transfer of personal data

44 Pursuant to Article 9(6) of the PDP Law, provisions regarding the transborder transfer of personal data from the other laws are reserved. As an example, in the recital on Article 9 of the PDP Law, it is stated that the articles of the Law No 5549 on the Prevention of Laundering of Crime Revenues, which authorizes the President of the Financial Crimes Investigation Board on international information exchange, shall be applied with priority.

45 Other fundamental laws that can be considered in this context are the Banking Law No 5411, the Notification Law No 7201, the Law No 6706 on International Judicial Cooperation in Criminal Matters, and the Turkish Civil Aviation Law No 2920[71].

46 The processes regulated under these laws are independent of the PDP Law, and data transfers within the scope of these laws are not subject to the authorization of the Board.[72]

II. Conventions and protocols of the Council of Europe

47 Turkey joined the CoE as the thirteenth member state on 13 April 1950.[73] Today, the CoE has forty-seven states as members, including all the EU member states.[74] It became an international organization exceeding the borders of the EU and is in a leading position in the field of human rights and personal data protection in the world.

48 The conventions adopted by the CoE are significant due to their binding nature for the EU member states in terms of constitutional law and effect on international law.[75]

49 In Turkey, in accordance with Article 90(5) of the Constitution, the international conventions duly put into effect have the force of law. Moreover, it is prohibited to apply to the Constitutional Court about such conventions under the allegation of unconstitutionality. In case such conventions regulate fundamental rights and freedoms, and these conventions and Turkish laws contain different provisions on the same subject, the provisions of international conventions should be taken as basis.

50 Consequently, it is important to consider the CoE conventions regarding the protection of personal data, which have the force of law in Turkey, in terms of ensuring integrity in practice and theoretical studies in Turkey.[76]

1. Convention for the Protection of Human Rights and Fundamental Freedoms

51 The Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), to which Turkey

69 PDP Law Article 9(5).

70 Elif Küzeci, *Kişisel Verilerin Korunması (Protection of Personal Data)* (4. Edition, On İki Levha Yayınları, 2020) 413; Elif Küzeci/Beri Boz, 'The new Data Protection Act in Turkey and potential implication for E-commerce' (2017) 7 (3) International Data Privacy Law 228.

71 Bilgi Information Technology Law Institute, 'Kişisel Verilerin Korunmasına İlişkin Düzenlemeler Çerçevesinde Uluslararası Veri Aktarımı, Güncel Gelişmeler ve Uygulamaya İlişkin Hukuki Değerlendirmeler (Legal Evaluations Regarding International Data Transfer, Current Developments and Practice within the Framework of the Regulations on the Protection of Personal Data)' (2020) 100-102 <https://itlaw.bilgi.edu.tr/media/2020/3/30/Final%20Veri_Aktarimi_Raporu_30.03.2020.pdf> accessed 8 March 2021.

72 ibid 100.

73 <https://www.coe.int/en/web/portal/turkey> accessed 8 March 2021.

74 <https://www.coe.int/en/web/portal/47-members-states> accessed 8 March 2021.

75 Hayrunnisa Özdemir, *Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması (Protection of Personal Data in the Field of Electronic Communications in Accordance with Private Law Provisions),* (1. Edition, Seçkin Yayınları 2009) 21.

76 Berna Akçalı Gür, 'Uluslararası Hukuk ve AB Hukuku Boyutuyla Kişisel Verilerin Yurt Dışına Aktarılması (Transborder Transfer of Personal Data with the Dimension of International Law and EU Law)' (2019) 25 (2) Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, 850, 870.

is a party, was signed in Rome on 4 November 1950.[77] The ECHR contains provisions on human rights, fundamental freedoms and the protection of private life and it regulates the European Court of Human Rights, which is the first organ in the field of protection of human rights.[78] The ECHR does not contain a provision directly regulating the protection of personal data, but the case-law developed by the European Court of Human Rights in this context is of particular importance.[79] The protection of personal data has been dealt with by the European Court of Human Rights under the respect for private and family life titled Article 8 of the ECHR.[80]

2. Convention 108 and Additional Protocol 181

52 CoE started working in the field of personal data protection in the 1970s and opened the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) for signature on 28 January 1981.[81] This convention is open for signature by non-EC member states.[82] Although Turkey is one of the first states to sign the Convention 108, it duly entered into force in Turkey on 17 March 2016.[83]

53 Convention 108 is the first and only convention with an international character that explicitly emphasizes the realization of the international standard in the field of personal data protection and the strengthening of data protection in domestic law.[84] Indeed, regulating the transfer of personal

77 Cemal Başar, 'Türk İdare Hukuku ve Avrupa Birliği Hukuku Işığında Kişisel Verilerin Korunması (Protection of Personal Data in Turkish Administrative Law and EU Law)' (PhD Thesis, Dokuz Eylül Üniversitesi 2019) 150.

78 Hayrunnisa Özdemir, *Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması (Protection of Personal Data in the Field of Electronic Communications in Accordance with Private Law Provisions),* (1. Edition, Seçkin Yayınları 2009) 24.

79 Personal Data Protection Authority, *Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi (Guideline on the Law on the Protection of Personal Data)* (2019) 18; Şehriban İpek Aşıkoğlu, 'Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri (Protection of Personal Data and Big Data in EU and Turkish Law)' (LL.M. thesis, İstanbul Üniversitesi 2018) 49; Sena Karaduman İşlek, 'Kişisel Verilerin Korunması Hakkı: Uygulamada Karşılaşılan Sorunlar ve Çözüm Önerileri (Right to Protection of Personal Data: Problems Encountered in Practice and Solution Suggestions)' (LL.M. thesis, Maltepe Üniversitesi 2020) 30-31.

80 Hayrunnisa Özdemir, *Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması (Protection of Personal Data in the Field of Electronic Communications in Accordance with Private Law Provisions),* (1. Edition, Seçkin Yayınları 2009) 24-25; Personal Data Protection Authority, *Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi (Guideline on the Law on the Protection of Personal Data)* (2019) 18; Şehriban İpek Aşıkoğlu, 'Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması ve Büyük Veri (Protection of Personal Data and Big Data in EU and Turkish Law)' (LL.M. thesis, İstanbul Üniversitesi 2018) 47; Ezgi Çabuk, 'Avrupa Birliği Düzenlemeleri Işığında Türk Hukukunda Kişisel Verilerin Korunması (Protection of Personal Data in Turkish Law in the light of EU Regulations)' (LL.M. thesis, Bahçeşehir Üniversitesi 2020) 19; Akif Sadık, 'Uluslararası Hukukta Kişisel Verilerin Korunması (Protection of Personal Data in International Law)' (LL.M. thesis, Anadolu Üniversitesi 2020) 22.

81 Hayrunnisa Özdemir, *Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması (Protection of Personal Data in the Field of Electronic Communications in Accordance with Private Law Provisions),* (1. Edition, Seçkin Yayınları 2009) 20; Personal Data Protection Authority, *Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi (Guideline on the Law on the Protection of Personal Data)* (2019) 17.

82 Elif Küzeci, 'Avrupa Konseyi'nin 108 sayılı Kişisel Verilerin Korunması Sözleşmesi Yenilendi! Sözleşme 108+, Carpenter kararı ve diğer bazı gelişmelere ilişkin bir değerlendirme (Council of Europe's Convention No. 108 Renewed! A review of Convention 108+, the Carpenter judgment and some other developments)' <https://medium.com/@elfkzc/avrupa-konseyinin-108-sayılı-kişisel-verilerin-korunması-sözleşmesi-yenilendi-bc8daad9decc> accessed 8 March 2021; <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures> accessed 8 March 2021.

83 Personal Data Protection Authority, *Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi (Guideline on the Law on the Protection of Personal Data)* (2019) 17.

84 Hayrunnisa Özdemir, *Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması (Protection of Personal Data in the Field of Electronic Communications in Accordance with Private Law Provisions),* (1. Edition, Seçkin Yayınları 2009) 21; Elif Küzeci, 'Avrupa Konseyi'nin 108 sayılı Kişisel Verilerin Korunması Sözleşmesi Yenilendi! Sözleşme 108+, Carpenter kararı ve diğer bazı gelişmelere ilişkin bir değerlendirme (Council of Europe's Convention No. 108 Renewed! A review of Convention 108+, the Carpenter judgment and some other developments)' <https://medium.com/@elfkzc/avrupa-konseyinin-108-sayılı-kişisel-verilerin-korunması-sözleşmesi-yenilendi-bc8daad9decc> accessed 8 March 2021; Berna Akçalı Gür, 'Uluslararası Hukuk ve AB Hukuku Boyutuyla Kişisel Verilerin Yurt Dışına Aktarılması (Transborder Transfer of Personal Data with the

data between the contracting states is among the objectives of the Convention 108.[85]

54 Transborder data flows are regulated under the third chapter of the Convention 108. Pursuant to Article 12(2) of the Convention 108, a contracting state shall not prohibit or subject to special authorisation transborder flows of personal data going to the territory of another Party for the sole purpose of the protection of privacy. However, there are two derogations regarding this rule:

i. Insofar as the legislation of the contracting state, from which data is to be transferred, includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other contracting state, which is to receive the data, provide an equivalent protection;

ii. When the transfer is made from the territory of the contracting state to the territory of a non-contracting state through the intermediary of the territory of another contracting state, in order to avoid such transfers resulting in circumvention of the legislation of the party referred to at the beginning of this derogation[86].

55 Issues such as developing technology, easy transborder transfer of data and transformation of data into a means of financial gain made it necessary for the CoE to adopt Additional protocol to Convention 108 regarding supervisory authorities and transborder data flows (Additional Protocol 181).[87] Additional Protocol 181 was signed by Turkey on 8 November 2001 and duly entered into force on 5 May 2016.[88] Additional Protocol 181 regulated two additional articles to the Convention 108, titled "Supervisory Authorities" and "Transborder Flows of Personal Data to a Recipient which is not Subject to the Jurisdiction of a Party to the Convention". Thus, contracting states are obliged to establish fully independent supervisory authorities that are responsible for ensuring compliance with the measures in domestic law that put the principles in Convention 108 and Additional Protocol 181 into practice.[89] The second novelty of Additional Protocol 181 is the provisions on transborder transfer of personal data to non-contracting states or organisations. Pursuant to Article 2 of Additional Protocol No 181, such transfers are to be made only if the receiving state or organisation ensures an adequate level of protection for the intended data transfer. However, there are two derogations from this rule:

i. In case that domestic law of the state, from which the data is to be transferred, provides for it because of specific interests of the data subject or legitimate prevailing interests, especially important public interests, or

ii. In case that safeguards, which can in particular result from contractual clauses, are provided by the controller responsible for the transfer and are found adequate by the competent authorities according to domestic law of state, from which the data is to be transferred.[90]

56 It is possible to state that the PDP Law is mainly compliant with the Convention 108[91] and Additional Protocol 181. However, the Board Decision on Convention 108, which is examined in the chapter C, carries significant importance in this context.

3. Modernized Convention 108+

57 It is a natural result that the Convention 108, adopted by the EC in 1981, is insufficient in the face of developing technology and the pace of the changing world. This situation caused modernization efforts. The seven-year-long modernization work was completed in 2018. Protocol amending the Convention for the protection of individuals with regard to the processing of personal data (Modernized Convention 108+) was adopted by the EC on 18 May 2018.[92]

Dimension of International Law and EU Law)' (2019) 25 (2) Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, 850, 854.

85 Berna Akçalı Gür, 'Uluslararası Hukuk ve AB Hukuku Boyutuyla Kişisel Verilerin Yurt Dışına Aktarılması (Transborder Transfer of Personal Data with the Dimension of International Law and EU Law)' (2019) 25 (2) Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, 850, 855.

86 Convention 108 Article 12(3).

87 Berna Akçalı Gür, 'Uluslararası Hukuk ve AB Hukuku Boyutuyla Kişisel Verilerin Yurt Dışına Aktarılması (Transborder Transfer of Personal Data with the Dimension of International Law and EU Law)' (2019) 25 (2) Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, 850, 855.

88 Personal Data Protection Authority, *Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi (Guideline on the Law on the Protection of Personal Data)* (2019) 18.

89 Additional Protocol 181 Article 1.

90 Additional Protocol 181 Article 2(2).

91 Elif Küzeci/Beri Boz, 'The new Data Protection Act in Turkey and potential implication for E-commerce' (2017) 7 (3) International Data Privacy Law 228.

92 Berna Akçalı Gür, 'Uluslararası Hukuk ve AB Hukuku

58 As of August 2021, thirty-nine CoE member states and four non-CoE member states have so far signed the Modernized Convention 108+.[93] Although it is expected in the doctrine that Turkey will be a party to the Modernized Convention 108+ since it meets today's requirements, Turkey has not signed this convention yet.[94] For this reason, this convention is not to be reviewed in detail within this article. However, it is necessary to state that while Modernized Convention 108+ keeps the main principles of the Convention 108, it also expands the scope of the Convention 108 and raises the standards of the Convention 108.[95] Modernized Convention 108+ carries significant importance with its potential to establish a standard for transborder transfers of personal data,[96] and it is hoped that soon this convention duly enters into force in Turkey.

C. Transborder Transfers in Turkey in the Light of Board Decisions

59 The fact that the PDP Law does not regulate the transborder transfer of personal data as detailed as the GDPR does not result in simplicity, but in ambiguity. This situation raises more questions in practice causing more work for the Authority. Additionally, Board decisions and publications have often shape the practice of transborder transfers of personal data. On the one hand, many decisions of the Board put an end to various discussions in the doctrine and in practice; while on the other hand, few decisions of the Board tend to complicate the matters in practice and result in unrealistic outcomes, such as qualifying explicit consent as the only applicable transfer mechanism.

60 Since the relevant publications of the Board have been examined under the previous chapter, in this chapter, the progress of the transborder transfer practice is examined in the light of the relevant Board decisions. The decisions below carry significant importance in the transborder transfer of personal data practice in Turkey as an addition to the decision for criteria determining whether countries have adequate levels of protection (that was reviewed under the previous chapter).

I. Board decision on the process of job application[97]

61 In business life, it is common for all the companies under a group of companies to operate using one common database. At the beginning of the legal compliance studies in Turkey, it was discussed whether such recordings would be considered as transfer of personal data in terms of the PDP Law

Boyutuyla Kişisel Verilerin Yurt Dışına Aktarılması (Transborder Transfer of Personal Data with the Dimension of International Law and EU Law)' (2019) 25 (2) Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, 850, 855.

93 <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures> accessed 8 March 2021.

94 Elif Küzeci, 'Avrupa Konseyi'nin 108 sayılı Kişisel Verilerin Korunması Sözleşmesi Yenilendi! Sözleşme 108+, Carpenter kararı ve diğer bazı gelişmelere ilişkin bir değerlendirme (Council of Europe's Convention No. 108 Renewed! A review of Convention 108+, the Carpenter judgment and some other developments)' <https://medium.com/@elfkzc/avrupa-konseyinin-108-sayılı-kişisel-verilerin-korunması-sözleşmesi-yenilendi-bc8daad9decc> accessed 8 March 2021.

95 Berna Akçalı Gür, 'Uluslararası Hukuk ve AB Hukuku Boyutuyla Kişisel Verilerin Yurt Dışına Aktarılması (Transborder Transfer of Personal Data with the Dimension of International Law and EU Law)' (2019) 25 (2) Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, 850, 855; Elif Küzeci, 'Avrupa Konseyi'nin 108 sayılı Kişisel Verilerin Korunması Sözleşmesi Yenilendi! Sözleşme 108+, Carpenter kararı ve diğer bazı gelişmelere ilişkin bir değerlendirme (Council of Europe's Convention No. 108 Renewed! A review of Convention 108+, the Carpenter judgment and some other developments)' <https://medium.com/@elfkzc/avrupa-konseyinin-108-sayılı-kişisel-verilerin-korunması-sözleşmesi-yenilendi-bc8daad9decc> accessed 8 March 2021.

96 Elif Küzeci, 'Avrupa Konseyi'nin 108 sayılı Kişisel Verilerin Korunması Sözleşmesi Yenilendi! Sözleşme 108+, Carpenter kararı ve diğer bazı gelişmelere ilişkin bir değerlendirme (Council of Europe's Convention No. 108 Renewed! A review of Convention 108+, the Carpenter judgment and some other developments)' <https://medium.com/@elfkzc/avrupa-konseyinin-108-sayılı-kişisel-verilerin-korunması-sözleşmesi-yenilendi-bc8daad9decc> accessed 8 March 2021.

97 <https://www.kvkk.gov.tr/Icerik/5410/Is-Basvurusu-Surecinde-Islenen-Kisisel-Verilerin-Hukuka-Aykiri-Sekilde-Paylasilmasi> accessed 23 April 2021.

and what would be the attitude of the Board in this regard. Through one of the first decisions published by the Board, an end to the relevant discussions was put in accordance with the PDP Law.

62 In this decision, the Board stated that each of the companies within a group of companies was a controller separately. Therefore, the personal data transfers between the companies within a group of companies were transfers of personal data within the scope of the PDP Law. For this reason, recording the personal data of the employee candidate in the database accessed by all the companies within a group of companies, without the explicit consent of the concerned employee candidate was to be interpreted as the transfer of personal data that violates the provisions of the PDP Law.

II. Board decision on Gmail[98]

63 In this decision, it was stated that the e-mails sent and received through Google's Gmail e-mail service infrastructure were kept in data centers located in various parts of the world. Therefore, if Gmail was used, there would be transborder transfer of personal data in terms of Article 9 of the PDP Law. Furthermore, in this decision, the Board emphasized that the storage services provided by controllers or processors, which had servers outside of Turkey, transferred the personal data outside of Turkey.

64 It is expected that this decision will cause serious changes in information technologies in Turkey due to the infrastructure change in the corporate operation, the emergence of additional and higher costs, the loss of efficiency during the adaptation of employees to the new system, and the need for finding domestic and national solutions in Turkey.[99]

65 In this context, 7 April 2020 dated Announcement of the Authority on Distance Education Platforms[100] is also significant. In its announcement, the Authority stated that most of the software used in the distance education process was served by cloud service providers and the data centers belonging to these softwares. If these platforms were used, due to the fact that their data centers were abroad, it would result in transborder transfer of the personal data and bring an obligation to comply with Article 9 of the PDP Law. It should be noted that EDPB also emphasized that remote access from a third country (for instance in support cases) and/or storage in a cloud located outside the European Economic Area would be considered to be a transfer.[101]

III. Board decision on Amazon Turkey[102]

66 Due to the fact that transborder transfer of data from Turkey involves many uncertainties in practice and the Board does not publish the list of countries with appropriate level of protection, it has become technically impossible to ensure compliance with the law in many cases.[103] This situation created an expectation that the Board would not decide on a violation regarding transborder transfers and would not impose administrative fines under the current conditions.[104] However, contrary to this expectation, the Board imposed a large amount of administrative fine on Amazon Turkey based on a series of violations, including the violation regarding the transborder transfer of personal data.

67 In this Board decision, it was stated that Amazon Turkey, as the controller, had submitted its under-

98 31.05.2019 dated and 2019/157 numbered decision of Personal Data Protection Board <https://www.kvkk.gov.tr/Icerik/5493/2019-157> accessed 23 April 2021.

99 Murat Volkan Dülger, 'Kişisel Verileri Koruma Kurulunun 17 Temmuz 2019 Tarihli Karar Özetlerine İlişkin Değerlendirme (Evaluation of the Personal Data Protection Board's Decision Summary dated 17 July 2019)' (2021) 2-3 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3792321> accessed 23.04.2021.

100 <https://kvkk.gov.tr/Icerik/6723/Uzaktan-Egitim-Platformlari-Hakkinda-Kamuoyu-Duyurusu> accessed 23 April 2021.

101 European Data Protection Board, 'Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data' (2020) 9 < https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/recommendations-012020-measures-supplement_en> accessed 23.04.2021.

102 27.02.2020 dated and 2020/173 numbered decision of Personal Data Protection Board <https://www.kvkk.gov.tr/Icerik/6739/2020-173> accessed 23 April 2021.

103 Murat Volkan Dülger, 'Kişisel Verileri Koruma Kurulu'nun 108 Sayılı Sözleşme Hakkındaki Kararı ve Yurt Dışına Veri Aktarımı Sorunu (Decision of Personal Data Protection Board about Nr. 108 Agreement and Problem about Data Transfer to Abroad)' (2021) 1 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3792396> accessed 23 April 2021.

104 Murat Volkan Dülger, 'Yurt Dışına Veri Aktarımında Milyonluk Ceza: Kişisel Verileri Koruma Kurulunun Amazon Kararı (Million Lira Fine About Transferring Data Abroad: Decision from Board of Personal Data Protection about Amazon)', (2021) 1 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3792388> accessed 23.04.2021.

takings to the Board for the authorization of the concerned transborder transfers of personals data, but the Board had not yet decided on this issue. Therefore, it was underlined by the Board that the sole legal option for Amazon Turkey's transborder transfers of personal data was to obtain the explicit consent of the concerned data subject. It was determined that the method followed by Amazon did not contain explicit consent and was not in compliance with the procedure set forth by the PDP Law.

68 The current legislation and this Board decision are based on Turkey's government policy on ensuring that data is hosted within the country.[105] However, this decision contains many elements that are open to criticism. Some of the criticised points can be summarized as follows:

i. The Board's narrow and literal interpretation of the PDP Law, its failure to consider the law as a whole, and its failure to account for international conventions duly enacted in accordance with Article 90 of the Constitution, particularly the Convention 108 and the Additional Protocol 181.[106]

ii. The Board's acceptance of explicit consent as the only applicable mechanism in transborder transfers of the personal data and its conflict with the Board's other decisions and guidelines of the Authority.[107]

iii. The impossibility of transborder transfers of personal data solely on the basis of the explicit consent of the concerned data subject, especially for large-scale companies or companies with many employees or connections abroad.[108]

iv. The Board's refusal to publish the list of countries with appropriate levels of protection for years, but its ability to make such decisions, when it does not fulfil its own obligation, which constitutes one of the cornerstones for legal compliance in transborder transfers.[109]

v. The fact that the Board did not authorize any transborder transfers under the submitted undertakings, including Amazon Turkey's application, on the date of the decision .[110]

69 All these justified criticisms raise the question of how fair this Board decision was.

IV. Board decision on Convention 108[111]

70 This decision is of particular importance due to the Board's interpretation of how Convention 108 and Additional Protocol 181 should be applied in domestic law.

71 Since the mechanism of obtaining the explicit consent of the data subject for transborder transfers of the personal data is difficult in practice, it was discussed whether personal data could be transferred to the contracting states based on the basic rule in Article 12(2) of the Convention 108. Since the Board had not announced the countries with appropriate levels of protection, it was argued that pursuant to the Convention 108, it was possible to consider the personal data transfers to the contracting states of the Convention 108 as lawful.[112] Moreover, the transborder transfer scheme included in the

105 Mehmet Bedii Kaya, *Kişisel Verilerin İşlenmesi ve Korunması Arasındaki Denge (Balance between Processing and Protecting Personal Data)* in Leyla Keser Berber and Ali Cem Bilgili (eds), *Güncel Gelişmeler Işığında Kişisel Verilerin Korunması Hukuku (Law on Protection of Personal Data in the Light of Current Developments)*, (On İki Levha Yayınları 2020) 33, 54.

106 ibid 55.

107 ibid 55.

108 Murat Volkan Dülger, 'Yurt Dışına Veri Aktarımında Milyonluk Ceza: Kişisel Verileri Koruma Kurulunun Amazon Kararı (Million Lira Fine About Transferring Data Abroad: Decision from Board of Personal Data Protection about Amazon)', (2021) 2 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3792388> accessed 23.04.2021.

109 ibid 1-2.

110 ibid 11.

111 22.07.2020 dated and 2020/559 numbered decision of Personal Data Protection Board <https://kvkk.gov.tr/Icerik/6790/2020-559> accessed 23 April 2021.

112 Bilgi Information Technology Law Institute, 'Kişisel Verilerin Korunmasına İlişkin Düzenlemeler Çerçevesinde Uluslararası Veri Aktarımı, Güncel Gelişmeler ve Uygulamaya İlişkin Hukuki Değerlendirmeler (Legal Evaluations Regarding International Data Transfer, Current Developments and Practice within the Framework of the Regulations on the Protection of Personal Data)' (2020) 18 <https://itlaw.bilgi.edu.tr/media/2020/3/30/Final%20Veri_Aktarimi_Raporu_30.03.2020.pdf> accessed 8 March 2021; Murat Volkan Dülger, Kişisel Verilerin Korunması Hukuku, 3. Baskı, İstanbul, 2020, 454; Murat Volkan Dülger, 'Kişisel Verileri Koruma Kurulu'nun 108 Sayılı Sözleşme Hakkındaki Kararı ve Yurt Dışına Veri Aktarımı Sorunu (Decision of Personal Data Protection Board about Nr. 108 Agreement and Problem about Data Transfer to Abroad)' (2021) 6-7 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3792396> accessed 23 April 2021.

Board's current Guideline on Transborder Transfer of Personal Data supported this interpretation.[113]

72 In this case, the relevant controller claimed that since the recipient company of the personal data was in an EU state, which was also a contracting state of Convention 108 and Additional Protocol 181, this transborder transfer of personal data is lawful pursuant to the Convention 108, Additional Protocol 181 and Article 90 of Constitution and cannot be subject to any prohibition or special authorisation.

73 In its assessment, the Board referred to the Explanatory Report to the Convention 108 and stated that the purpose of the provision of Article 12(2) of the Convention 108 was to facilitate the data flow between the parties, based on the pre-acceptance that the contracting states provided sufficient assurances in terms of the protection of personal data. The Board therefore concluded that this provision did not mean that data flows between contracting states cannot be subject to prohibition or special authorization. As an example, the Board pointed out that in the light of the GDPR, the contracting states of Convention 108 are not directly qualified as countries with adequate level of protection, and this situation is only a criterion to be considered in the adequacy assessment.

74 As explained above, in accordance with Article 90(5) of the Constitution, in case international conventions regulating fundamental rights and freedoms, that are duly put into effect in Turkey, and Turkish laws contain different provisions on the same subject, the provisions of international conventions should be taken as basis. In its interpretation of this article, the Board stated that the relevant international convention provision should be directly applicable and emphasized that this means that it is sufficiently clear, precise and unconditional and this does not require the state to take any additional measures for its implementation. The Board concluded that Convention 108 did not meet these criteria, therefore, as in the EU practice, it was not sufficient on its own in terms of determination of the country with adequate levels of protection under the PDP Law, but only had the quality of a positive element in the assessment to be made by the Board.

75 Since the Board is responsible for the implementation of the PDP Law, it was criticised that the Board evaluated when and under which conditions a provision of the Constitution would find application, that this evaluation was not based on any jurisprudence or doctrine, and that such an important interpretation was detached from the necessary justification and depth.[114]

76 Despite these criticisms, it is not possible to claim that solely the fact that the recipient is in a contracting state of Convention 108 and Additional Protocol 181 is sufficient for the lawful transborder transfer of personal data.[115]

D. Conclusion

77 Personal data protection law is a developing and rapidly changing field all over the world. Despite this change, personal data protection law has difficulty in keeping up with the requirements of today's technology and data-based economy. Considering the different dynamics of law and technology, this is not a surprising outcome. Nevertheless, this outcome means that there is more work to do for legislators, authorities and jurists in order to speed up the process of creating appropriate legal principles and rules. Only with such fast, detailed and ever-developing works, the legal systems would have the chance to establish a realistic and applicable balance between the right to protect personal data and the data-based economy in the PDP Law in the future.

78 In the past six years, Turkey took significant steps to develop personal data protection law and to enlighten people in Turkey. Examples include the PDP Law's entry into force, establishment of the Authority and the Board, ratifications of the Convention 108 and Additional Protocol 181, various decisions of the Board, court and supreme courts and proactive works of the Authority, et cetera. The Authority sought to be active in organizing and attending conferences on the personal data protection, creating various videos on data protection and rights of the data subjects, regular publishing its journal, organizing various competitions, taking decisions, and publishing announcements and guidelines. All these efforts resulted in the enlightenment of people and lawyers in Turkey in this field, which is not to be taken lightly. Nevertheless, these efforts have not been sufficient to clear the vagueness regarding transborder transfers of personal data. Thus, there is much to do, and the Authority is burdened even

113 Personal Data Protection Authority, 'Kişisel Verilerin Yurt Dışına Aktarılması (Transborder Transfer of Personal Data)' <https://kvkk.gov.tr/yayinlar/KİŞİSEL%20VERİLERİN%20YURTDIŞINA%20AKTARILMASI.pdf> accessed 8 March 2021.

114 Murat Volkan Dülger, 'Kişisel Verileri Koruma Kurulu'nun 108 Sayılı Sözleşme Hakkındaki Kararı ve Yurt Dışına Veri Aktarımı Sorunu (Decision of Personal Data Protection Board about Nr. 108 Agreement and Problem about Data Transfer to Abroad)' (2021) 12-13 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3792396> accessed 23 April 2021.

115 ibid 16.

more than usual due to the fact that this field is new in Turkey.

79 Even though, the evaluation of the law does not come to an end, there are urgent steps-to-be-taken for the personal data protection in Turkey. First, there is a need of more detailed and developed provisions on transborder transfer, which makes it necessary for Turkey to sign and ratify Modernized Convention 108+ and for the legislators to make the related amendments in the PDP Law as soon as possible. Secondly, all the transfer mechanisms are to be enabled, so that the explicit consent does not come to the fore as the first option among the other mechanisms. In this regard, adequate levels of protection are to be an effective transfer mechanism in Turkey. For this purpose, it is required that the trade volume with concerned country and reciprocity criteria with the relevant country are not considered as mandatory in the evaluation process of countries with highly developed personal data protection legislation and legal implementation. Also, the authorization process of BCR and undertakings need to be accelerated. In this context, the future announcements regarding clarification of the requirements and details of such new mechanisms need to be made by the Board at an earlier stage. Furthermore, the undertaking sets for the transfers by a processor to another processor or a controller would be useful in solving the problems experienced regarding the transborder transfer of personal data by data processors. Additionally, the creation of undertaking sets, which do not require the authorization of the Board if used without any amendments, would be a practical solution against the ineffectiveness of this mechanism in practice. Thirdly, the ambiguity of the provision on serious harm on interest of Turkey and the person concerned need to be removed in the light of the related international conventions. Finally, even if inspired by the GDPR, the critiques of the GDPR should be considered during such works, and the works of the Board need to be original instead of literal translations and to aim to bring transborder transfer of personal data to a new level. These needs are essential by today's data-based economy and the obligatory speed for creating appropriate legal principles, rules, and processes.

80 The Authority and the Board are among the key figures in this process of required change. In order to achieve these goals without delay and to accelerate the process of authorizations, more experts can be recruited by the Authority if necessary. Moreover, the list of the countries with adequate levels of protection should be announced by the Board without any further delay. Furthermore, a deadline for authorization processes of the applications regarding transfer mechanisms is necessary in order to notify the applicants about the maximum period of time required and to avoid long-term uncertainties. Additionally, narrow and literal interpretations of the PDP Law are to be avoided in the Board decisions, and explicit consent is not to be considered as the sole applicable transfer mechanism. Finally, Board decisions need to be based on more detailed justifications through Turkish and foreign doctrines, resolutions, and international conventions.

The responsibility of online intermediaries for illegal user content in the EU and in the US by Folkert Wilman

Edward Elgar:Cheltenham, 2020, ISBN 978 1 83910 482 4

by **Gerald Spindler,** Univesity of Göttingen

Book Review

Recommended citation: Gerald Spindler, Book Review: The responsibility of online intermediaries for illegal user content in the EU and in the US by Folkert Wilman, 12 (2021) JIPITEC 476 para 1

I.

1 The responsibility of Internet intermediaries has become "evergreen" in the international discussion, starting with the boom of E-Commerce and the Internet in the 90s until nowadays reaching a peak in legal reforms such as the new proposal of the EU-commission regarding a Digital Services Act and decisions of courts such as the CJEU concerning copyright infringements of platforms like YouTube. The author, Folkert Wilman, is like no other suited to treat this wide area of aspects in a comparative way by taking both the perspectives of the EU and the US into account. Wilman is a true "insider" as he is a member of the Legal Service of the EU-commission and has been involved in law-making process in the EU as well as representing the EU-commission in many cases brought to the CJEU regarding liability of internet intermediaries.

2 The book is divided into four parts, the first dealing with the *lex lata* situation in the EU, while the second looks at the legal framework in the US. The third chapter is dedicated to an in-depth analysis of interests, fundamental rights and private speech regulation and finally, the fourth looks to policy recommendations and conclusions. The book aims to assess whether the "old" balance being struck by the E-Commerce-Directive between interests of providers, users, and victims is still appropriate and fit for the situation today. Folkert Wilman restricts his analysis, however, to host providers, thus excluding similar questions for access providers as well as hybrid phenomena like search engines etc. which is justified according to the breadth of the topics which Wilman delves into.

II.

3 The first part of the book is dedicated to an in-depth analysis of Articles 14 and 15 of the E-Commerce-Directive, the famous safe harbour privileges, and the prohibition of general monitoring obligations. Wilman scrutinizes in particular the jurisdiction of the ECJ like the L'Oréal case[1] or the Google-France[2] decision concerning the distinction of "active" and "passive" host providers (2.40 – 2.57). The author

1 ECJ Case C-324/09 *L'Oréal v eBay* [2011] EU:C:2011:474.

2 ECJ Joined Cases C-236/08 to C-238/08 *Google France* [2010] EU:C:2010:159.

also deepens the interpretation of Article 14 E-Commerce-directive regarding the level of substantiation for notices in order to assume knowledge of the host provider. Unfortunately, Wilman does not take into account relevant jurisdiction on the national level, like decisions of the German Federal Court (Bundesgerichtshof) such as in Stift-Parfüm.[3] Moreover, the author deals intensively with the issues of notice-and-take-down procedures as well as duties of care, with special regard to the Communication of the EU-commission on Illegal content (COM(2018) 1177 final). However, from the perspective of member states an important point is missing in the analysis: the possibility of injunctions which open the floor for many courts to introduce duties of care concerning stay-down-obligations for future infringements. Wilman discusses these points more broadly in the following chapter dedicated to a thorough inspection of Article 15 E-Commerce-directive in relationship with recent measures and actions, such as the reform of the Audio-visual Media Directive, the new DSM-directive in copyright (here in particular Article 17 DSM-D) or anti-terrorism directive. The author lies stress on an interpretation of Article 15 E-commerce-directive based on fundamental rights such as user's rights (3.25 – 3.34). Very clearly, Wilman states rightfully that the new directives constitute a more or less inconsistent change in policies at the EU level directed "towards the establishment of an EU-level duty of care" (3.88), creating a lot of legal uncertainty, thus also affecting fundamental rights of involved parties (3.86).

4 The second part turns to the legal framework of liability of internet intermediaries in the US, starting with Section 230 of the Communications Decency Act and the provisions on liability privileges for providers (which cannot be qualified as publishers) and in particular the "Good Samaritan" safe harbour for providers. Wilman impressively describes the broad interpretation of Section 230 of the CDA by US courts by shielding providers from liability even if victims have notified providers about illegal activities and even if providers obviously have taken an active role in disseminating and promoting illegal content. The next subchapter takes up the discussions on one of the most famous safe harbour privileges, Section 512 of the Digital Millennium Copyright Act which relies mainly—unlike the CDA—on notice-and-take down procedures. Even though these provisions have been analyzed to a large extent by previous authors, Wilman succeeds in giving a precise, yet concise overview of the actual legal conditions under which a provider can plead for liability exemptions by elaborating and using a wide range of US court decisions. From an European perspective (in particular with a view on Article 17 DSM-D) the critical assessment of Section 512 DMCA is of outmost interest and is reminiscent of the same discussion in Europe, such as the rightholders' perspective. Namely, the view that the notice-and-take down procedures are too burdensome for the enforcement of the copyrights and that a notice-and-stay down obligation is missing (5.51 – 5.52) or on the other hand of the user`s perspective that there is an outright abuse of takedown notices (5.56). Moreover, the fact that "DMCA plus" agreements between intermediaries and rightholders in order to foster automated filtering mechanisms can be observed (however, also affecting user`s rights) (5.59 – 5.65) could be a blueprint for the "high industry standards" required under Article 17 (4) b) DSM-D concerning automated filtering mechanisms.

5 The third part sheds light on the different involved interests, fundamental rights and private speech regulation. Within this framework Wilman also stresses the fact that often direct infringers can be identified and thus, introducing intermediary liability gives a strong incentive for victims to concentrate on intermediaries rather than on the direct infringers (6.25 – 6.26). The author carves out that a compromise has to be found between the extreme positions (strict liability of providers versus total exemption of liability of providers); however, Wilman stops at this point by stating that the compromise should be a matter of policy decision and legal context (6.49 – 6.55). The next subchapter is dedicated to the related fundamental rights, starting with the freedom of expression, particularly the chilling effects of liability provisions (7.10 – 7.24). Wilman of course takes other fundamental rights such as the freedom to conduct business, intellectual property rights, and data protection into account. In sum, the author stresses the different impact of freedom of expression in the US and the EU, as courts in the EU are striking a balance between freedom of expression and other fundamental rights which contrasts the US where freedom of expression has an overriding importance (7.68 – 7.81). Wilman also delves into a deeper analysis of the decisions of the European Court of Human Rights in the cases Delfi v. Estonia (64569/09) and MTE v. Hungary (22947/13). He concludes rightfully that extreme solutions, be it favouring too one-sidedly freedom of expression or be it intellectual property rights are not tenable under EU law. The final subchapter of this part turns to different phenomena of private speech regulation such as the "privatization" of enforcement by placing intermediaries in the role of a judge, content moderation, and knowledge and control. Wilman discusses here at length the use of automated means (filtering technology) and its limits (8.40 – 8.50) by pointing out that context dependence of content restricts the use of such automated means; meanwhile, the author concludes that despite these limits the growing capacities of enterprises to monitor user-generated content also leads to a need for filtering technology,

3 BGH MMR 2012, 178.

or in other terms, leads to a potential knowledge of providers of user-generated content (8.50). Wilman also mentions the chilling effects to newcomers on the market generated by obligations to use automated means (8.59). The conclusion that the author draws from these developments is not an abolishment of the safe harbour privileges rather than a careful evolution.

6 Regarding this evolution of liability privileges Wilman turns in his last part to the assessment of arguments, recommendations and conclusions. The author formulates five requirements, starting with the need for a balanced approach between different interests, then the effectiveness in tackling with illegal content, the need for a clear regime, for safeguards and transparency, and finally a proportionate and workable system. Whereas Wilman deems the EU liability system based on knowledge to be balanced and effective, he also stresses injunctions (9.18 – 9.19); as mentioned already, Wilman unfortunately does not go beyond pointing out that injunctions are left to member states. As the German example proves, injunctions are widely used and impose obligations to providers to monitor illegal activities in the future (as part of notice-and-stay-down procedures). With good reasons Wilman criticizes Article 14 E-Commerce-directive as lacking safeguards and transparency (9.29) with regard, in particular, to missing notice-and-counter-notice procedures. He, however, argues strongly for retaining the knowledge-based liability scheme for providers (9.34 – 9.42) as well as the prohibition of general monitoring obligations (9.43 – 9.53). However, Wilman also identifies two shortcomings: first, the system`s effectiveness in tackling content which can entangle serious public harm and second (as already mentioned), the lack of binding rules on notices and takedown procedures including counter-notice procedures.

7 Taking up these challenges in the following chapter, Wilman elaborates certain recommendations for more precise notices and the requirements of substantiation (10.14 – 10.15), including the concept of trusted flaggers (10.16 – 10.25). Much of what the author describes reminds the reviewer of what is now enshrined in the proposal of the Digital Services Act of the EU commission, in particular the role of trusted flaggers and safeguards against misuse of notices. Wilman then discusses possible measures regarding injunctions, such as a "right to reply" (10.44); however, as already mentioned, Wilman unfortunately restricts his analysis to a purely EU level, not taking into consideration developments in the member states which provide many cases regarding specific measures and counter-notice procedures (just as recently stated by the German Federal Court concerning an injunction against Facebook, judgement of 29.07.2021 -III ZR 192/20). Wilman also strengthens the importance of public oversight empowering public authorities to issue injunctions against providers, in order to overcome gaps in enforcement. Moreover, he stresses a necessary modification regarding the introduction of a good-Samaritan principle and eliminating disincentives for providers to voluntarily tackling illegal content.

8 Finally, Wilman concludes that a "double-sided duty of care" is required (Chapter 11) to complement the knowledge-based liability system in the EU. The author, however, restricts these duties of care to very serious and manifestly illegal online content, such as child sexual abuse material, racist and xenophobic speech, and terrorist content. Once again, this chapter reflects the approach taken by the EU-commission in its proposal of a Digital Services Act, by only imposing certain obligations on very large online platforms which disseminate content (and not only store it). These obligations should, according to Wilman, consist in using a combination of automated means and human oversight as well as the prohibition of illegal content in the terms and conditions, and finally in cooperating with authorities through reporting schemes and retaining and disclosing relevant information. Also, the "other" side of duties of care can be found in the Digital Service Act, as Wilman proposes safeguards for user interests ensuring that providers do not block content automatically and that users have access to quick, effective and impartial means of redress. However, Wilman does not deal with Article 17 DSM-D and the balancing of automated filtering technology which quite certainly deviates—as the author stated himself—from the knowledge-based liability scheme. Moreover, whereas the notion of "manifestly illegal content" can be applauded it remains to be seen how criteria can be established in order to specify what is "manifestly illegal".

9 Wilman summarizes in the last chapter his findings by pleading for complementary measures to be added to the E-Commerce-directive, as already mentioned.

III.

10 Wilman has written a great and overwhelming book that can without doubt be qualified as a landmark in the discussion of liability of providers. The book contains a thoughtful analysis which is clearly structured and brings many debates to a precise point. Where one wants to criticize the analysis, there are only some minor points which do not alter the overall impression of an analysis that should be read by everyone who is doing research in this area. These criticisms refer mainly to the concentration on the EU-Level and the jurisdiction of the CJEU and the European Court of Human Rights; Wilman here, unfortunately, does not take into account the numerous cases at the member state level, in particular regard-

ing injunctions and safeguards. Moreover, his analysis is mainly restricted to host providers; however, as we can observe in practice, access providers are being attacked on grounds of injunction, such as in the famous UPC Telekabel-case of the CJEU (which is of course mentioned by Wilman). Finally, regarding the main conclusions and recommendations of Wilman, it is arguable what the view of Wilman would be finally with regard to Article 17 DSM-D, which deviates from the knowledge-based liability by introducing duties of care. As copyright infringements cannot be qualified as causing public harm such as child sexual abuse or terrorist content Article 17 DSM-D does not fit into the scheme developed by Wilman.

11 In sum, Wilman has written a great book which should be used widely, and obviously reflects many views shared by the EU commission, enshrined in the proposal of the Digital Services Act.

Competition and Regulation in the Data Economy: Does Artificial Intelligence Demand a New Balance? by Gintarė Surblytė-Namavičienė

Edward Elgar, Cheltenham (U.K.) and Northampton (USA), 2020. ISBN: 978-1-78811-664-0

by **Heiko Richter,** MPI München

Book Review

Recommended citation: Heiko Richter, Book Review: TCompetition and Regulation in the Data Economy: Does Artificial Intelligence Demand a New Balance? by Gintarė Surblytė-Namavičienė, 12 (2021) JIPITEC 480 para 1

1 **Gintarė Surblytė-Namavičienė**, Lecturer in the Faculty of Law at Vilnius University, asks in her comprehensive book on competition and regulation in the data economy, whether artificial intelligence needs a new balance. The cardinal question is whether AI has in fact changed fundamental economic parameters which would demand drastic legal changes. And in the end, she pleads for a fine-tuning of the legal framework, rather than for radical legal changes. How Surblytė-Namavičienė arrives at her conclusion with regard to several different, but yet linked, aspects of regulation (i.e. trade secret law, data protection, competition law, and consumer protection), becomes clear when delving into her intelligible and thought-provoking analysis. The result is a book that is much worth reading.

2 **Chapter 2** lays the foundation by introducing the functional characteristics and essence of the digital economy. Surblytė-Namavičienė clarifies upfront what is meant by artificial intelligence and highlights the decisive distinctions between "general" and "narrow" AI and between "strong" and "weak" AI. While general AI still appears as a utopia, she highlights the learning mechanism as distinctive feature of AI. From a standpoint of Luhmann's systems theory, AI cannot be considered as an 'autopoietic system', but at least the increasing use of AI may disrupt the interaction between individuals and therefore the basis of existing systems.[1] For this reason, AI can have a significant social impact. Yet from the perspective of economic theory, Surblytė-Namavičienė regards the data economy not as a "revolution", but rather as a development which follows classic economic principles. Based on the work of Adam Smith, she highlights the significance of self-interest for the functioning of the data- and algorithm-driven economy, which can also explain the 'privacy paradox' in her view. Yet, what has indeed changed is the general importance of the economic role of data, which has dramatically

1 See for a more differentiated and critical discussion on systems theory and machine learning Nassehi, Theorie der digitalen Gesellschaft, C.H.Beck, München, 2019, pp. 228 et seq.

increased over the last years. While Surblytė-Namavičienė regards the regulatory debate on data access and ownership as essential, she criticizes the focus on non-personal data as being too narrow. For this reason, she then goes into more detail about the difference between personal and non-personal data, which forms the basis for the following chapters, in which she addresses the interface between data protection and the other relevant areas of law on several occasions. She concludes by raising the seminal question of how to strike a balance between economic incentives of the undertakings when implementing AI on the one hand and the protection of consumers (also data subjects) on the other hand.

3 **Chapter 3** focuses on trade secret protection. The justification for attaching the pole position to this often-overlooked regulatory regime lies in its significance for the data economy: trade secret protection does not depend on intellectual efforts, it may protect datasets as well as algorithms, and it may be extensively applied in practice. Therefore, trade secret protection reaches far beyond IoT-settings, which initially triggered the discussion on the significance of trade secret protection in the digital economy. However, the exact scope and application of rules under Directive (EU) 2016/943 on the Protection of Trade Secrets to the data economy are far from clear. For this reason, Surblytė-Namavičienė performs a comprehensive analysis of the requirements for and legal consequences of trade secret protection, for which she also takes an informative side glance at the protection mechanism in the US. Surblytė-Namavičienė regards data as generally eligible for trade secret protection. She then focuses on personal data as a particular subject matter of trade secret protection. As a consequence, natural tensions occur between the undertaking's interest to protect such data as a secret on the one hand and data subjects' rights under the GDPR on the other hand, because claiming such rights under the GDPR may require the undertaking to share the data with the data subject or third parties. This is especially true for the right of access under Article 15 GDPR and the right to data portability under Article 20 GDPR, which Surblytė-Namavičienė takes a meticulous look at. In addition, the right to not be subject of automated decision-making, including profiling (Article 22 GDPR), adds to the tension between data protection and trade secrets, because algorithms that serve automated decision-making may indeed be subject of trade secret protection. Surblytė-Namavičienė then points to the fundamental right to conduct business, which may cover trade secrets, but she concludes that the EU Trade Secret Directive itself does not explain how fundamental rights are to be balanced. This leads to significant uncertainty for the legal application in scenarios where secrecy protection collides with data protection. In future, much remains to be clarified on a case-by-case basis by the courts. Another important aspect is reverse engineering, which is allowed for information protected under the trade secrecy rules. Surblytė-Namavičienė argues that for effectively enabling reverse engineering, it is necessary to refuse trademark protection for functional signs, while contractual restrictions may nevertheless prevent reverse engineering. Although trade secrets undoubtedly play an important role for the data economy, regulating algorithms reaches beyond trade secret law, especially with regard to competition.

4 **Chapter 4** therefore deals with competition, the key question being how much 'rethinking' of competition law is needed in light of the technical developments of recent years. In particular, Surblytė-Namavičienė puts three issues under the microscope. First, she examines algorithmic price adjustments, which the competition law community started to discuss comparatively early. Regardless of this phenomenon's actual practical significance, which Surblytė-Namavičienė puts into question, she extensively analyzes the standard on price-fixing and concerted practices under Article 101 TFEU. She illustrates how the CJEU's E-Turas decision[2] has considerably broadened the scope. This decision leaves us with significant uncertainty and further blurs the line between concerted practices and mere parallel behavior. Surblytė-Namavičienė considers the legal implications of the E-Turas decision as highly relevant for the algorithm-driven economy and warns against overenforcement of EU competition law in this domain. The second issue relates to competition *for* data traffic. This concerns selective distribution as well as rights relating to datasets. Regarding the latter, Surblytė-Namavičienė reflects on the crucial *sui generis* right for databases under Directive 96/9/EC, which illustrates the significance of exclusive rights protection from a competition point of view. She accurately highlights the importance of the CJEU's Ryanair decision[3] for the data economy, according to which merely contractual restrictions to data scraping are valid if the database is not protected under the *sui generis* right. According to Surblytė-Namavičienė, such contractual restrictions can generate anticompetitive effects and may negatively affect consumers by preventing them from choice. The third issue concerns data access under Article 102 TFEU.[4] Surblytė-Namavičienė

2 *"Eturas" UAB and Others v Lietuvos Respublikos konkurencijos taryba* (C-74/14) EU:C:2016:42 [2016].

3 *Ryanair Ltd v PR Aviation BV* (C-30/14) EU:C:2015:10 [2015].

4 For a recent comprehensive account on this topic Schmidt, Zugang zu Daten nach europäischem Kartellrecht, Mohr Siebeck, Tübingen, 2020.

argues that for such access claims, the "exceptional circumstances test"[5] from the *IMS Health* case should not be overestimated, because this case depended on specific facts and appears rather informative regarding its implications for unfair competition. Instead, the CJEU's *Bronner* decision,[6] which sets out a "pure" indispensability requirement, would provide the relevant legal standard for claiming access to data on the basis of Article 102 TFEU.

5 **Chapter 5** then broadens the view beyond competition law and asks which other regulatory regimes become relevant for the data economy. Here, Surblytė-Namavičienė focuses on the threat of algorithmic manipulation, especially in the fields of personalized services and personalized pricing in the business-to-consumer relationships and with regard to rankings by online platforms. After elaborating on these issues, she identifies a regulatory gap with respect to the protection of consumers and calls for regulation which should ensure transparency and prohibit certain behavior for undertakings. In this regard, she considers the already existing regulation of algorithmic trading of financial instruments as informative. A further aspect for regulation is consumer contract protection, in relation to which Surblytė-Namavičienė pleads for "more robust state control of terms and conditions". In particular, she highlights the significance and complexity of consent regarding the use of personal data as well as the role of competition law by discussing the infamous Facebook decision of the Bundeskartellamt.[7] Finally, she remains critical with regard to approaches of self-regulation, especially when fundamental rights and privacy are involved, as is often the case with AI-driven markets.

6 These chapters reveal how Surblytė-Namavičienė elaborates on a wide range of topics, which are undoubtedly all highly relevant for the functioning and development of the data and algorithm-driven economy. Of course, they cannot be held as exhaustive, and rather than a holistic picture, the analytical depth and focus on selected issues and the well-considered hinting to important links between regulatory regimes is a particular strength of the book. This work is especially informative for researchers who deal with trade secrets, algorithmic collusion, access to data under competition law, and the competition/data protection interface. Surblytė-Namavičienė refers to classical thinkers (such as Smith, Turing, Arrow, Coase, and Schumpeter), and she explicitly justifies her focuses before spotting respective legal uncertainties, which indeed need more clarification. In substance, one could argue that classic economic theory has been contested on grounds of behavioral economics. In fact, Surblytė-Namavičienė acknowledges the role that psychological effects play in competition, while leaving it to the reader to think about what impact they might have on the found solutions. Overall, AI technology has not changed the underlying economic principles based on which the data economy functions *as such* (e.g. the economic ingredients of the platform economy were all already known). However, the effects of different forces working together have led to unprecedented situations, which indeed challenge the law. Therefore, one can ask what circumstances would lead to a drastic change and which parameters and contexts are relevant to understand when a change of paradigm is needed for approaches to regulate the data economy.

7 Some significant developments haven taken place *after* the publication of the book, and they could therefore not be considered. This is true for the German Facebook decisions of the OLG Düsseldorf and the Federal Court of Justice[8] and the recent reform of the *German Act Against Restraints of Competition*.[9] Also, the book could not take the Commission's proposals for a *Digital Market Act*[10] and a *Digital Services Act* into account,[11] which in fact address some of the issues Surblytė-Namavičienė elaborates on. Furthermore, the upcoming *Data Act*, (the Commission's proposal is expected to be published in Spring 2022), aims to address the intersection between trade secrets and

5 *IMS Health GmbH & Co. OHG v NDC Health GmbH & Co. KG* (C-418/01) EU:C:2004:257 [2004].

6 *Oscar Bronner GmbH & Co. KG* (C-7/97) EU:C:1998:569 [1998].

7 Case B6-22/16, Bundeskartellamt, *Facebook*, 6 February 2019, available at: www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=5 (accessed 21 January 2021).

8 Case VI-Kart 1/19 (V), *Facebook*, 26 August 2019, ECLI:DE:OLGD:2019:0826.VIKART1.19V.00; Case KVR 69/19, *Facebook*, 23 June 2020, ECLI:DE:BGH:2020:230620BKVR69.19.0, available at: http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&client=12&pos=0&anz=1&Blank=1.pdf&nr=109506 (accessed 21 January 2021). For an English translation see 51 IIC (2020), 1137-1165.

9 BGBl. I 2021, S. 2.

10 European Commission, "Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)" COM (2020) 842 final.

11 European Commission, "Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC" COM (2020) 825 final.

data economy[12]. In this regard, it would be wise for the EU legislator to consult Surblytė-Namavičienė's book.

8 In times when academic writing on digital regulation tends to compete for the most visionary and most revolutionary approach, the route taken by Surblytė-Namavičienė is remarkably critical, prudent, and cautious. This contributes to the attractiveness of the work, as she clearly delineates the potential and limitations of competition law and critically highlights the crucial interfaces between the regulatory regimes. Surblytė-Namavičienė disregards many common assumptions as "speculative", "overestimated", "exaggerated", and "hypothetical". Rather than claiming that things *are*, she prefers to say that they *might* or *could*. This absence from overhasty generalizations appears like an honest approach that puts, however, the question for empirical evidence and its significance for evidence-based policy making on the table. Here, the book asks the right questions, but answering them in a definite way would require an extensive evaluation of empirical research results, which would surely go beyond the book's scope. As a consequence, Surblytė-Namavičienė does neither provide speculative answers, nor do her suggestions on how to adjust the legal framework become overly concrete. Rather, the reader gains inspiration and is indeed left with the sensible claim that it is all about the fine-tuning of the legal framework. Surblytė-Namavičienė rightly points to the neuralgic spots and, even more so, urges for timely reforms in this regard. Considering the recently initiated but by far not yet completed legislative actions on the EU level, it appears too early to tell though whether this remains wishful thinking in light of political realities.

12 European Commission, Communication "A European strategy for data" COM (2020) 66 final, p. 13.

JIPITEC

Journal of
Intellectual Property,
Information Technology,
and Electronic Commerce
Law

www.jipitec.eu