jipitec

3| 2024

Volume 15(2024)
Issue 3 ISSN 2190-3387

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

www.jipitec.eu

2024

jipitec

Journal of Intellectual Property, Information Technology and Electronic Commerce Law

Volume 15 Issue 3 December 2024
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

Editorial

by **Lucie Guibault and Orla Lynskey**

Recommended citation: Lucie Guibault and Orla Lynskey, Editorial, 15 (2024) JIPITEC 210 para 1

1 With this issue of JIPITEC, we are delighted to announce the arrival of Orla Lynskey, Chair of Law and Technology at University College London, as a member of the editorial board. Her expertise in the law and regulation of the digital society, with a particular focus on data laws, enriches the common knowledge of the members of the board and has already proved extremely valuable in the preparation of this issue. Orla and I are proud to present you with this issue which assembles seven captivating articles on a variety of topics involving distinct technological and/or legislative developments. The papers in this issue are a true reflection of the diversity of legal issues which fall under the auspices of JIPITEC and of the dynamic legal and technical context in which the journal sits.

2 This issue of JIPITEC opens with a contribution from Donatella Casaburo in which the author investigates the phenomenon of real-time bidding for the placement of digital advertisements in publishers' inventories, following a competitive bidding process. As real-time bidding for advertisements has been described as the "biggest data breach ever recorded", the article investigates its GDPR compliance with a particular focus on the role and responsibilities of data controllers 'behind the scenes'.

3 Next, Lorena Arismendy Mengual's article focuses on user liability for wrongful behavior in the Metaverse. More particularly, she delves into the legal issues arising from avatar misconduct in online virtual worlds. She describes how harm suffered by a person may be caused by or through an avatar, but observes that compensation for such harm hinges on whether avatars are recognised as legal persons and she documents the lack of said recognition. Would granting avatars legal personhood provide a path toward redress? Could the institution of civil liability and compensation offer useful reparation in circumstances of misconduct?

4 The following article tackles the challenges associated with the co-regulatory arrangement of Articles 34 and 35 of the Digital Services Act (DSA) for the mitigation of the risks posed by harmful but legal content. Andrea Palumbo notes that the DSA moved from a model of *ex post* intermediary liability into the realm of both *ex ante* and *ex post* regulation through the introduction of new due diligence obligations for the providers of these services. His article focuses, in particular, on the due diligence obligations imposed on the providers of very large online platforms (''VLOPs'') and of very large online search engines (''VLOSEs'').

5 In their article entitled 'Towards an optimal regulatory strategy for data protection: insights from law and economics', Donatas Murauskas and Raminta Matulytė use Shavell's law and economics model to compare the *ex ante* regulatory approach to data protection in the EU with the *ex post*

liability approach of the US. While the two cross-Atlantic approaches to data protection are difficult to compare under a law and economics lens, the research provides insight into how efficiency driven considerations may better support and justify more fragmented legislation such as in the US.

6 This focus on law and economics creates a natural bridge with the subsequent article on competition law. Maryam Pourrahim investigates who, between the various levels of suppliers or end-product manufacturers of Internet of Things (IoT) or connected cars, should be responsible for obtaining licenses for Standard Essential Patents (SEPs). She first describes the value chain involved in the production of IoT and connected cars, before analyzing the potential of patent law, FRAND commitments, and competition law to force SEP holders to license suppliers in alignment with recent case law.

7 The final two articles turn to copyright law related issues. Kacper Szkalej & Martin Senftleben study how the application of share-alike obligations under a Creative Commons License impact Generative AI, ranging from trained models, to curated datasets and AI output. The authors question whether the obligation to license under similar conditions inhibits the use of CC-licensed materials through the various steps of the AI generative process. Last, but certainly not least, Martin Stierle turns his attention to the question of whether Luxembourg should implement a regime of fair compensation for private copying and if so, under what conditions. Luxembourg is one of only three EU Member States to not have complied with the requirements of Directive 2001/29 on Copyright in the Information Society. Should this change?

8 All in all, this is a fascinating issue and we wish you a lot of reading enjoyment!

Lucie Guibault — Halifax

Orla Lynskey — London

Digital Advertising and the GDPR Identifying the (Joint) Controllers in the Real-Time Bidding Ecosystem

by **Donatella Casaburo** *

Abstract: In digital advertising, real-time bidding allows advertisers to place their advertisements in publishers' inventories in real time, after having participated in an auction with competing bidders. In Europe alone, personal data on users' online behaviour is collected and shared 197 billion times per day by more than 1000 firms' part of the real-time bidding ecosystem. This gives real-time bidding the title of the "biggest data breach ever recorded". Having a clear understanding of the roles and responsibilities of the entities involved in real-time bidding becomes of paramount importance to enhance compliance with the data protection legislation and adequately safeguard data subjects' rights. This paper aims to identify the (joint) controllers for the personal data processing operations performed during a real-time bidding auction.

Keywords: Real-time Bidding, Digital Advertising, Controller, Data Protection, GDPR

Recommended citation: Donatella Casaburo, Digital Advertising and the GDPR- Identifying the (Joint) Controllers in the Real-Time Bidding Ecosystem, 15 (2024) JIPITEC 212 para 1

A. Introduction

1 In 2023, the spending for digital advertising in Europe reached a total of €96.9 billion, registering a €69 billion increase compared to 2013.[1] While the marketing and advertising industry has always relied on data, the rise and convergence of machine learning and big data contributed to increase the effectiveness of data-driven advertising of more than 500%.[2] As a result, 90% of digital advertising now involves the processing of behavioural data of online users.[3]

* Donatella Casaburo is a Doctoral Researcher at the Faculty of Law, Economics and Finance of the University of Luxembourg and at the KU Leuven Centre for IT & IP Law (CiTiP). The author would like to thank Pierre Dewitte for the idea and the valuable comments. This research has received funding from the Cybersecurity Research Program Flanders 2024.

1 Interactive Advertising Bureau Europe, 'AdEx Benchmark 2023 Study' (*IAB Europe*, May 2024) <https://iabeurope.eu/wp-content/uploads/IAB-Europe_AdEx-Benchmark-2023-Report.pdf> accessed 12 August 2024.

2 Interactive Advertising Bureau Europe, 'IAB Europe Press Release: The dire unintended consequences of restricting data-driven ads' (*IAB Europe*, 7 September 2017) <https://iabeurope.eu/the-dire-unintended-consequences-of-restricting-data-driven-ads/> accessed 29 January 2024.

3 IHS Markit, 'The Economic Value of Behavioural Targeting in Digital Advertising' (*IAB Europe*, 2017) <https://iabeurope.eu/wp-content/uploads/2019/08/BehaviouralTargeting_FINAL.pdf> accessed 29 January 2024.

2 Digital advertising mainly relies on the real-time bidding technology (RTB),[4] which allows advertisers to place their ads in publishers' spaces in real time, after having participated in an auction with competing bidders. To function, RTB heavily relies on the collection and further use of online users' personal data, to an extent it has been defined as the "biggest data breach ever recorded": in Europe alone, data on users' online behaviour is collected and shared 197 billion times per day and by more than 1058 firms.[5] Having a clear understanding of the roles and responsibilities of the entities involved in RTB becomes of paramount importance to enhance compliance with the data protection legislation and adequately safeguard data subjects' rights.

3 This paper aims to identify the (joint) controllers for the personal data processing operations performed during a RTB auction. To this aim, we first introduce the notion of (joint) controller, on which we build a '(joint) controllership test' [Section B.]. Then, we apply the test to the personal data processing operations of a RTB auction [Section C.]. To conclude, we present some final considerations deriving from the problematic allocation of responsibilities among the joint controllers [section D.].

B. The Notion of (Joint) Controller and the (Joint) Controllership Test

4 Article 4(7) of the General Data Protection Regulation (GDPR) provides that the controller is "the natural or legal person [...] which, alone or jointly with others, determines the purposes and means of the processing of personal data".[6] To ensure effective and complete protection of data subjects,[7] the concept of 'controller' is an autonomous one, to be broadly interpreted according to the GDPR, as clarified by the Court of Justice (CJEU).[8] The principles established by the CJEU are further complemented by the guidelines issued by the European Data Protection Board (EDPB).[9]

5 According to the EDPB, the essential characteristic of the controller is its capacity to exercise decision-making powers over the processing of personal data, thus influencing its key elements: to be qualified as controller, an entity needs to determine both that the processing needs take place and why it takes place.[10] The controller decides on the purposes and means of the processing, namely on the 'why' and 'how' of the processing activities. As clarified by the CJEU in its *Wirtschaftsakademie* judgement, while the controller needs to decide on both purposes and means, the level of influence may vary and it might be sufficient to contribute to impact on the whether or not, or on the manner in which, personal data are processed.[11] In particular, controllers can leave some manoeuvrability in deciding the means of the entities processing personal data on their behalf, i.e., the processors. It is, then, possible to distinguish between essential and non-essential means of the processing.[12] The essential means are closely linked to the purposes pursued (e.g., type of data processed, categories of data subjects involved, disclosure of personal data and categories of recipi-

4 Michael Veale and Frederik Zuiderveen Borgesius, 'Adtech and Real-Time Bidding under European Data Protection Law'(2022) 23 Ger. Law J. 226, 226.

5 Irish Council for Civil Liberties, 'The Biggest Data Breach – ICCL report on scale of Real-Time Bidding data broadcasts in the U.S. and Europe' (*Irish Council for Civil Liberties*, May 2022) <https://www.iccl.ie/wp-content/uploads/2022/05/Mass-data-breach-of-Europe-and-US-data-1.pdf> accessed 29 January 2024.

6 Regulation (EU) 2016/679 of the European Parliament and of the Council 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.

7 Case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] ECLI:EU:C:2014:317, para 34.

8 European Data Protection Board, 'Guidelines 07/2020 on the concepts of controller and processor in the GDPR' (*EDPB*, 7 July 2021) <https://edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf> accessed 10 October 2024.

9 *Ibid.*

10 *Ibid.* 11.

11 Case C210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* [2018] ECLI:EU:C:2018:388, para 35.

12 EDPB (n 8) 14-15.

ents[13]) and their determination is of exclusive competence of the controller. On the contrary, the non-essential means are related to technical aspects of the processing (e.g., choice of the infrastructure or detailed security measures) and can be determined by the processor.

6 Article 26 of the GDPR provides that there is joint controllership when "two or more controllers jointly determine the purposes and means of processing". This definition reflects that of 'controller', by restating its essential elements.[14] Therefore, joint controllers are controllers jointly determining purposes and means of the processing. As noted by the EDPB, a joint controllership can take the form of either common or converging decisions on the purposes and essential means of the processing activities.[15] While common decisions imply common intentions of the controllers, converging decisions are closely linked and complement each other, thus being necessary for the processing to happen in that specific form.[16] As clarified by the CJEU in its *Fashion ID* judgement, the joint controllership among two or more controllers is, however, limited to those operations in the chain of processing for which the entities jointly determine both the purposes and means of the processing.[17]

7 To jointly determine the purposes of the processing, controllers do not necessarily need to share the same or common purposes: the purposes pursued may be different, as long as they are closely linked or complementary.[18] For instance, in the *Fashion ID* judgement, the CJEU held that the existence of a mutual (economic) benefit of the parties may be one of the possible factors leading to joint controllership.[19] However, an entity that merely receives a payment for a service offered, and does not pursue an own purpose through the processing, cannot be qualified as a joint controller.[20]

8 To jointly determine the means of the processing, as clarified by the CJEU in the *Fashion ID* and *Wirtschaftsakademie* judgements, it is sufficient that a controller decides to make use of the infrastructure allowing the personal data processing (e.g., a platform or a standardized tool) provided by another controller,[21] especially if the former can set up some of the parameters of the processing activities.[22] Again, an entity that merely relies on an infrastructure provided by a controller cannot be qualified as joint controller unless, by using such infrastructure, it exercises a true influence on the collection and processing of personal data, for instance by making the same processing possible,[23] while also being able to decide when it terminates.[24]

9 Whenever multiple controllers are involved in the processing, but they do not jointly determine its purposes and means, they are separate controllers, independent from each other.

I. The (Joint) Controllership Test

10 The criteria to identify controllers and to qualify the joint participation of more than one entity to the processing provided by the CJEU and the EDPB can be summarised, and systematised in a '(joint) controllership test'.

11 In line with what is suggested by the EDPB,[25] the (joint) controllership test consists of two phases. In the first phase, we conduct a 'micro-level' analysis

13 CJEU (n 7) para 36.

14 EDPB (n 8) 18-19.

15 *Ibid.* 19-20.

16 *Ibid.*

17 Case C-40/17 *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV* [2019] ECLI:EU:C:2019:629, para 74.

18 EDPB (n 8) 20.

19 CJEU (n 17) para 80.

20 EDPB (n 8) 21.

21 CJEU (n 17) para 78; CJEU (n 11) para 35.

22 CJEU (n 11) paras 36-37.

23 CJEU (n 17) para 75.

24 Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* [2017] ECLI:EU:C:2017:796, Opinion of AG Bot, para 56.

25 EDPB (n 8) 17.

of each processing operation.[26] To do so, first, we decompose the chain of processing into smaller processing operations. Then, we identify the entities involved in each of them. Finally, we qualify each entity as either (joint) controller or processor vis-á-vis each of the processing operations. During this last step, we can rely on the two template tables below.

12 The first template table summarises the controllership test. The table is filled in relation to each entity involved in the processing and with regard to each processing operation in which it is involved. To facilitate the analysis, the table already lists the criteria laid down by the CJEU and the EDPB to qualify an entity as controller, which pertain to the existence of a decisive influence on purposes and essential means of the processing.[27]

[Entity involved]	
[Processing operation(s)]	
Purpose	**Essential means**
[Yes, .../No]	[Determining personal data processed and/or categories of data subjects concerned]
	[Determining disclosure of personal data and (categories of) recipients]
	[Providing infrastructure for the processing]
	[Using infrastructure provided by other entity for its own purpose, but makes the processing possible, and/or sets parameters, and/or chooses when ending the processing]
	[No decisive influence]
Controllership: [Yes/No/Only if ...]	

Table 1: Template table for controllership test

13 The second template table summarises the joint controllership test. When multiple controllers are involved in the same processing operation, the second table is filled. To facilitate the analysis, the table already lists the criteria laid down by the CJEU and the EDPB to qualify multiple entities as joint controllers, pertaining to the joint determination of purposes and means of the processing.[28]

[Entities involved]	
[Processing operation(s)]	
Joint determination of purpose	**Joint determination of means**
[The entities pursue purposes which are identical/common, or closely linked/complementary] [The entities pursue their own separate purposes]	[The entities determine together the essential means] [The entities rely on the same infrastructure, provided by one of them, while the other makes the processing possible, and/or sets the parameters, and/or chooses when ending the processing]
Joint controllership: [Yes/No/Only if ...]	

Table 2: Template table for joint controllership test

14 In the second phase of the (joint) controllership test, starting from the results of the micro-level analysis, we conduct a 'macro-level' analysis of the processing, to double check whether we identify further joint controllerships.[29] To do so, we verify if the processing operations can be grouped into one or more unified set of operations pursuing a joint purpose using jointly defined means. This finalises the results of the analysis, by extending the responsibilities of joint controllers to those stages of the processing for which they exercise decision-making powers.[30]

26 *Ibid.*

27 EDPB (n 8) 15; CJEU (n 17) paras 75, 78; CJEU (n 11) paras 35-37; CJEU (n 7) para 36; Opinion of AG Bot (n 24), para 56.

28 EDPB (n 8) 19-22; CJEU (n 17) paras 75, 78; CJEU (n 11) paras 35-37; CJEU (n 7) para 36; Opinion of AG Bot (n 24), para 56.

29 EDPB (n 8) 17.

30 CJEU (n 17) para 70.

C. Assessment of (Joint) Controllership in a RTB Auction

15 The RTB ecosystem consists of two sides and involves three main entities, as illustrated in Figure 1.[31]

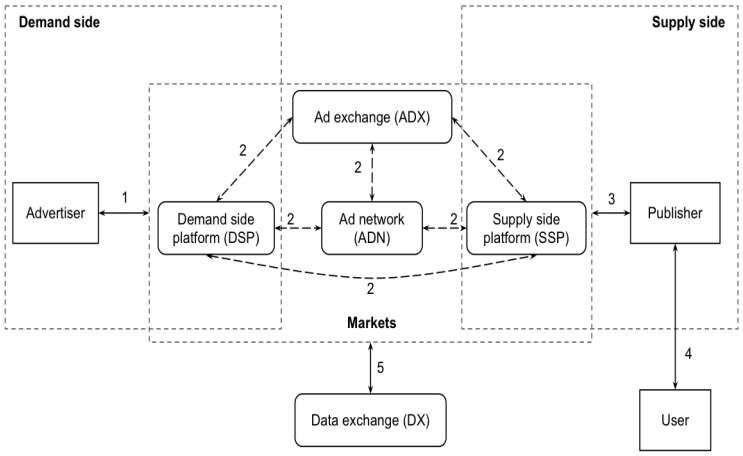


Figure 1: The RTB ecosystem. Source: Jun Wang, Weinan Zhang and Shuai Yuan (n 31).

16 On the one hand, in the 'demand side', Demand-Side Platforms (DSPs) are responsible for organizing the targeted advertising campaigns on behalf of advertisers or advertising agencies.[32] But on the other hand, in the 'supply side', Supply-Side Platforms (SSPs) are responsible for registering the publishers' advertising inventories and selling the spaces.[33] DSPs and SSPs are connected and interact via an Ad Exchange (AdX), responsible for conducting the auction processes.[34]

17 In addition to these three main entities, the RTB ecosystem generally includes also Ad Networks (AdNs) and Data Exchanges (DXs). AdNs increase RTB's efficiency, by aggregating and balancing the advertisement demand and supply.[35] DXs collect and analyse users' information from different sources, enabling DSPs to perform better targeted advertising campaigns.[36]

18 The RTB auction initiates when a user visits a publisher's website[37] which incorporates a space to be filled with an advertisement. With a certain degree of simplification, the next steps are the following:[38]

1. While the website page loads, the SSP sends an advertisement request on behalf of the publisher to the AdX;
2. For the incoming ad request, the AdX creates a bid request incorporating the users' information collected through cookies and forwards it to DSPs;
3. DSPs can ask the DX for user's data retrieved from third parties;
4. If DSPs decide to bid based on the instructions received by advertisers, they send the bid responses with the bid price to the AdX;
5. The AdX selects the winner and sends the winning notice to the selected DSP; and
6. The winner's advertisement is displayed on the website page for the specific user.

19 To facilitate the implementation of RTB, the Interactive Advertising Bureau Tech Lab has standardised the technology in a common protocol, OpenRTB.[39]

31 Jun Wang, Weinan Zhang and Shuai Yuan, 'Display Advertising with Real-Time Bidding (RTB) and Behavioural Targeting' (*arXiv*, 2017) <https://arxiv.org/abs/1610.03013> accessed 29 January 2024.

32 Tobias Urban and others, 'A Study on Subject Data Access in Online Advertising After the GDPR' in Cristina Pérez-Solà et al. (eds), *Data Privacy Management, Cryptocurrencies and Blockchain Technology, ESORICS 2019 International Workshops, DPM 2019 and CBT 2019, Luxembourg, September 26–27, 2019, Proceedings* (Springer 2019) 63, 64.

33 Jun Wang, Weinan Zhang and Shuai Yuan (n 31).

34 Lukasz Olejnik, Tran Minh-Dung and Claude Castelluccia, 'Selling Off Privacy at Auction' (*HAL-Inria*, 2013) <https://hal.inria.fr/hal-00915249/PDF/SellingOffPrivacyAtAuction.pdf> accessed 29 January 2024.

35 Jun Wang, Weinan Zhang and Shuai Yuan (n 31).

36 Tobias Urban and others (n 32) 64.

37 While mobile applications can also support RTB, we will only refer to websites to avoid unnecessary complications in the text.

38 Jun Wang, Weinan Zhang and Shuai Yuan (n 31).

39 Interactive Advertising Bureau Tech Lab, 'OpenRTB' (*IAB Tech Lab*, January 2024) <https://iabtechlab.com/standards/openrtb/> accessed 12 August 2024. The protocol previously provided by Google Developers, 'Authorized Buyers Real-time Bidding Proto' (*Google Developers*, August 2024) <https://developers.google.com/authorized-buyers/

The types personal data collected through cookies and further processed during the RTB auction depend on the content of the bid request which, according to the latest OpenRTB protocol, may include: the user's unique identifier, details and location of the user's device, the browser used, additional known information about the user, such as their year of birth, gender, interests and relevant keywords about them.[40]

20 While RTB can properly function with the limited number of entities and through the six steps explained above, the scenario in practice is normally far more complicated. To maximize their effectiveness and profits, both publishers and advertisers can rely on more Supply-Side and Demand-Side Platforms, which in turn rely on more AdXs and AdNs. Therefore, the process for adjudicating a single advertisement space can involve numerous entities and/or auctions, finally competing amongst themselves.[41] Considering the inherent complexities of the RTB ecosystem, we focus on the simplified scenario described above. In other words, we analyse the (joint) controllership in a RTB auction involving the least possible number of entities: a publisher, a SSP, an AdX, more than one DSP and more than one advertiser.

I. Micro-Level

21 In the first step of the micro-level analysis of the RTB auction process, we identify the personal data processing operations. These are:

(i) The retrieval of cookies stored in the web browser;
(ii) The creation of a bid request;
(iii) The transfer of the bid request to DSPs;
(iv) The retrieval of the bid request;
(v) Potentially, the sale of additional personal data collected by the DX;
(vi) Potentially, the retrieval of additional personal data collected by the DX;
(vii) The use of the personal data.

22 In the second step of the micro-level analysis, we identify the different entities involved in each of the processing activities. To simplify the task, we divide the RTB auction process in two phases. During the first phase, the AdX is the entity that, on behalf of the publisher as represented by the SSP, (i) processes the personal data contained in the cookies, (ii) so to create a bid request (iii) and to transfer it to several DSPs. In the second phase, DSPs are the entities that (iv) receive the personal data contained in the bid request and, (v) after the potential sale of additional personal data by the DX and (vi) their retrieval, (vii) use them to decide on whether placing a bid on behalf of advertisers.

23 In sum, three entities process personal data during a RTB auction: the AdX, DSPs and the DX. However, the following entities are also part of the picture:

1. the publisher, mandating the AdX to carry out the RTB auction;
2. the SSP, acting as intermediary between the publisher and the AdX; and
3. advertisers, mandating DSPs to bid on their behalf.

24 In the third step of the micro-level analysis, we conduct the (joint) controllership test for the first [Section 1.] and second [Section 2.] phases of the RTB auction, to qualify the involved entities.

1. First Phase: Publisher, AdX and SSP

25 The first phase of the RTB auction sees the involvement of the publisher [Section (a)], of the AdX [Section (b)] and of the SSP [Section (c)].

a.) Publisher

26 The publisher does not engage directly in any processing activity, which are delegated to the AdX. As clarified in the CJEU in the Jehovah's Witnesses

rtb/realtime-bidding-guide> accessed 12 August 2024, has recently been deprecated to fully migrate to OpenRTB.

40 Interactive Advertising Bureau Tech Lab (n 39).

41 See Lukasz Olejnik, and Claude Castelluccia, 'To bid or not to bid? Measuring the value of privacy in RTB' (*Lukasz Olejnik*, 2014) <https://lukaszolejnik.com/rtb2.pdf> accessed 29 January 2024; Damien Geradin and Dimitrios Katsifis, '"Trust me, I'm fair": analysing Google's latest practices in ad tech from the perspective of EU competition law'(2020) 16 Eur. Competition J. 11, 18-19.

judgement, this is not an obstacle *per se* to the qualification as controller, as long as the publisher is able to determine purposes and means of the processing.[42]

27 As for the determination of purposes, the publisher has an own primary economic interest in all the processing operations performed by the AdX, as they create profit through the sale of the impression. As for the determination of the (essential) means of the processing, we need to distinguish between the different processing operations performed by the AdX. On the one hand, the publisher exercises a decisive influence on the way personal data is processed during the retrieval of cookies and the creation of the bid request. By embedding RTB in its webpage, the publisher enables the AdX to process personal data, thus triggering the start of a processing which would not be possible otherwise.[43] Moreover, the publisher can terminate the processing, by simply removing RTB from its webpage.[44] On the other hand, we can theorise two different cases for the transfer of the bid requests to DSPs. If the publisher cannot set any parameters on the personal data included in the bid request and on recipient DSPs, the transfer is out of the publisher's sphere of influence. Otherwise, the publisher exercises a decisive influence on the essential means of the processing.[45]

28 Therefore, the publisher is a controller for (at least part of) the processing of personal data performed by the AdX,[46] as summarized in Tables 3 and 4 below.

Publisher	
(i) Retrieval of cookies stored in the web browser and (ii) creation of a bid request	
Purpose	**Essential means**
Yes, increasing profits from the sale of the impression through a RTB auction	Using infrastructure provided by AdX for its own purpose, but makes the processing possible and chooses when ending the processing
Controllership: Yes	

Table 3: Controllership test for publisher for the retrieval of cookies and the creation of a bid request

Publisher	
(iii) Transfer of the bid request to DSPs	
Purpose	**Essential means**
Yes, increasing profits from the sale of the impression through a RTB auction	Determining personal data collected
	Determining disclosure of personal data and recipients
Controllership: Only if setting parameters on essential means	

Table 4: Controllership test for publisher for the transfer of the bid request to DSPs

b.) AdX

29 The AdX is the entity processing personal data during the first phase of the RTB auction.

30 As for the retrieval of cookies, a preliminary observation is needed: normally, due to the domain specificity of cookies, the AdX does not only retrieve the cookies stored in the web browser, but it acts as a tracker entity itself.[47] In principle, tracker entities can be either controllers or processors, depending on whether they determine their own purposes and means.[48] The AdX benefits from the processing, enhancing the quality of its services by building users' profiles or providing statistics. The AdX also develops the software code that enables the processing, thus determining *de facto* some of its essential means,

42 Case C-25/17 *Tietosuojavaltuutettu v Jehovan todistajat — uskonnollinen yhdyskunta* [2018] ECLI:EU:C:2018:551, para 69.

43 CJEU (n 17) para 75.

44 Opinion of AG Bot (n 24), para 56.

45 CJEU (n 11) paras 36-37; CJEU (n 7) para 36; EDPB (n 8) 15.

46 This conclusion is supported by the Article 29 Data Protection Working Party, 'Opinion 2/2010 on online behavioural advertising' WP171 11-12.

47 Article 29 Data Protection Working Party (n 46) 10-11; Brendan Van Alsenoy, *Data Protection Law in the EU: Roles, Responsibilities and Liability* (Intersentia Ltd, 2019) 404.

48 Brendan Van Alsenoy (n 47) 438.

including the type of data processed and the categories of data subjects involved. As principal designer of the data processing,[49] the AdX is a controller in its own right for the retrieval of cookies,[50] as summarised in Table 5 below.

AdX	
(i) Retrieval of cookies stored in the web browser	
Purpose	**Essential means**
Yes, enhancing the quality of its services and providing statistics	Determining personal data processed and categories of data subjects concerned
	Providing infrastructure for the processing
Controllership: Yes	

Table 5: Controllership test for AdX for the retrieval of cookies

31 As for the creation and further transfer of the bid request to DSPs, the responsibility of the AdX is even greater. The AdX pursues its own purpose, as it gains from the processing a benefit other than the mere payment for the services offered.[51] Moreover, the AdX exercises a decisive influence on the means of the processing, by creating the infrastructure connecting the publisher and advertisers. Thus, the AdX organizes, coordinates and encourages both its and other actors' processing activities.[52] This influence is stronger whenever the publisher does not set parameters on the bid request, so that the AdX determines the categories of data subjects involved and the type of personal data that will be shared during the whole RTB auction process, as well as the DSPs recipient of the bid request.[53] Therefore, the AdX is a controller in its own right for the creation of the bid request and its transfer to DSPs, as summarized in Table 6 below.

AdX	
(ii) Creation of a bid request and (iii) transfer of the bid request to the DSPs	
Purpose	**Essential means**
Yes, enhancing the quality of its services and providing statistics	Determining personal data processed and categories of data subjects concerned
	Determining disclosure of personal data and recipients
	Providing infrastructure for the processing
Controllership: Yes	

Table 6: Controllership test for AdX for the creation of a bid request and its transfer to the DSPs

c.) SSP

32 The SSP is not processing personal data and acts as an intermediary between the publisher and the AdX.

33 The SSP exercises some influence on the means of the processing performed by the AdX, as it creates the infrastructure connecting it with the publisher. However, the SSP does not pursue its own purposes in the processing: normally, the services offered by SSPs consist in aggregating publishers' advertising inventories and organising advertising campaigns.[54] Both services are neither linked to the processing or performed to the only interest of publishers, as the mere fact of receiving remuneration is not *per se* sufficient to identify a SSP's purpose in the processing.[55] Therefore, since its activity is limited to that of an

49 Opinion of AG Bot (n 24) para 47.

50 This conclusion is supported by: European Data Protection Board, 'Guidelines 8/2020 on the targeting of social media users', (*EDPB*, 13 April 2021) <https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf> accessed 30 January 2024; Article 29 Data Protection Working Party (n 46); CJEU (n 17); CJEU (n 11).

51 EDPB (n 8) 50.

52 CJEU (n 42) para 73.

53 CJEU (n 7) para 36.

54 Jun Wang, Weinan Zhang and Shuai Yuan (n 31).

55 EDPB (n 8) 50.

intermediary service, the SSP is GDPR-irrelevant, as shown in Table 7 below.

SSP	
(i) Retrieval of cookies stored in the web browser, (ii) creation of a bid request and (iii) transfer of the bid request to DSPs	
Purpose	**Essential means**
No	Providing infrastructure for the processing
Controllership: No	

Table 7: Controllership test for SSP for the retrieval of cookies, creation of a bid request and its transfer to DSPs

d.) Joint Controllership

34 Since both the publisher and the AdX are controllers for the processing operations performed during the first phase of the RTB auction, we now assess whether they are joint controllers.

35 The processing operations would not occur without the decisions taken by both the publisher and the AdX. Even though the purposes pursued by the two entities differ, both entities are benefitting from the same processing, so that their own commercial purposes are mutually complementary.[56] Moreover, both entities participate in determining the means of the processing: while the AdX provides the infrastructure for the processing, the publisher actively decides to make use of it, thus enabling the processing.[57] The processing cannot be considered separable, as it could not be performed by one party without the intervention of the other:[58] Therefore, the publisher and the AdX are joint controllers for (at least part of) the processing.

36 The extent of the joint control depends on the publisher's contribution to the determination of the essential characteristics of the processing. By enabling the AdX to process the data, the publisher exercises a decisive influence on the retrieval of cookies and creation of the bid request. However, the joint controllership for the transfer of the bid request to DSPs depends on whether the publisher can set parameters on the data to be shared and their recipients. If that is not the case, the last processing operation is out of the publisher's sphere of influence and under the sole control of the AdX. Tables 8 and 9 below summarise the assessment of the joint controllership between the publisher and the AdX.

Publisher and AdX	
(i) Retrieval of cookies stored in the web browser and (ii) creation of a bid request	
Joint determination of purpose	**Joint determination of means**
The entities pursue purposes which are complementary	The entities rely on the same infrastructure, provided by the AdX, while the publisher makes the processing possible, sets the parameters and chooses when ending the processing
Joint controllership: Yes	

Table 8: Joint controllership test for publisher and AdX for the retrieval of cookies and creation of a bid request

Publisher and AdX	
(iii) Transfer of the bid request to DSPs	
Joint determination of purpose	**Joint determination of means**
The entities pursue purposes which are complementary	The entities rely on the same infrastructure, provided by the AdX, while the publisher sets the parameters
Joint controllership: Only if publisher is setting parameters on essential means	

Table 9: Joint controllership test for publisher and AdX for the transfer of the bid request to the DSPs

56 Case C-40/17 *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV* [2018] ECLI:EU:C:2018:1039, Opinion of AG Bobek, para 105.

57 CJEU (n 17) para 75.

58 EDBP (n 8) 19-20.

2. Second Phase: Advertisers, DSPs and DX

37 The second phase of the RTB auction sees the involvement of advertisers [Section (a)], DSPs [Section (b)] and of the DX [Section (c)].

a.) Advertisers

38 Advertisers do not engage directly in any processing activity, which are delegated to DSPs. Again, this is not an obstacle *per se* to the qualification as controller, as long as advertisers are able to determine purposes and means of the processing.[59]

39 As for the determination of purposes, advertisers have their own primary economic interest in the processing operations performed by the DSPs and DX, as they increase the advertisers' chances to deliver their ads to a specific targeted audience and, ultimately, enhance their overall profit. As for the determination of the (essential) means of the processing, we need to distinguish between the different processing operations performed by DSPs. On the one hand, advertisers exercise a decisive influence on the way personal data is processed during the retrieval of the bid request and the use of the data therein contained. By deciding to initiate a RTB advertising campaign and accordingly accepting the terms and conditions, the advertisers enable DSPs to process personal data, thus triggering the start of a processing which would not be possible otherwise.[60] Moreover, advertisers can stop the processing, by simply terminating the contract with DSPs.[61] On the other hand, we can theorise two different cases for the potential sale and retrieval of additional personal data from the DX. If advertisers cannot decide on whether requesting this additional data transfer or on selecting the DX, the retrieval of additional data is out of the advertisers' sphere of influence. Otherwise, advertisers exercise a decisive influence on the means of the processing.[62]

40 Therefore, advertisers are controllers in their own right for (at least part of) the processing of personal data performed by DSPs. The controllership test is summarized in Tables 10 and 11 below.

Advertisers	
(iv) Retrieval of the bid request and (vii) use of personal data	
Purpose	**Essential means**
Yes, increasing profits from the delivery the of ad to a targeted audience through a RTB auction	Using infrastructure provided by DSPs for their own purpose, but make the processing possible and choose when ending the processing
Controllership: Yes	

Table 10: Controllership test for advertisers for the retrieval of the bid request and use of personal data

Advertisers	
(v) Sale and (vi) retrieval of additional personal data	
Purpose	**Essential means**
Yes, increasing profits from the delivery the of ad to a targeted audience through a RTB auction	Determining personal data processed and categories of data subjects concerned
Controllership: Only if setting parameters on essential means	

Table 11: Controllership test for advertisers for the retrieval of additional personal data

41 DSPs are the entities performing three of the four processing operations during the second phase of the RTB auction.

59 CJEU (n 42) para 69.

60 CJEU (n 17) para 75.

61 Opinion of AG Bot (n 24) para 56.

62 CJEU (n 11) paras 36-37; EDPB (n 8) 15.

b.) DSPs

42 In principle, DSPs can be either controllers or processors, depending on whether they determine their own purposes and means. DSPs benefit from both the processing they perform on behalf of advertisers' and that potentially performed by the DX, by using the data acquired to gain an advantage over other competitor DSPs and by enriching the users' profile to better target them, thus enhancing the quality of the services they offer.[63] This holds, *a fortiori*, whenever DSPs collect additional data from the DX. DSPs also develop the infrastructure that enables the processing, thus determining *de facto* some of its essential means. The influence on the processing is even greater whenever advertisers do not set any parameters on the sale and retrieval of additional data from the DX: in this case, DSPs are also determining the essential characteristics of the transfer of the additional data. As principle designers of the data processing,[64] DSPs are controllers in their own right for the data processing operations performed by them and by the DX,[65] as summarised in Table 12 below.

DSPs	
(iv) Retrieval of the bid request, (v) sale and (vi) retrieval of additional personal data and (vii) use of personal data	
Purpose	**Essential means**
Yes, enhancing the quality of the services to win as many auctions as possible	Determining personal data processed and categories of data subjects concerned
	Providing infrastructure for the processing
Controllership: Yes	

Table 12: Controllership test for DSPs for the retrieval of the bid request, the retrieval of additional personal data and their use

c.) DX

43 The DX is another tracker entity, which collects, aggregates and analyses personal data from various sources and for its own purposes,[66] thus qualifying as sole controller for the processing operations performed outside of the RTB ecosystem.[67] If solicited by advertisers or DSPs, the DX may intervene in the RTB auction process to sell the personal data to better target users.

44 As for the retrieval of the bid request and the use of personal data, the DX does not exercise any influence on the processing: the DX neither pursues a purpose of its own or decides on the means, nor does it perform the operations. Therefore, the DX is GDPR irrelevant, as shown in Table 13 below.

63 Michael Veale and Frederik Zuiderveen Borgesius (n 4) 232.

64 Opinion of AG Bot (n 24) para 47.

65 This conclusion is supported by MED 2018-042 *Décision n° MED 2018-042 du 30 octobre 2018 mettant en demeure la société X* [CNIL, 2018].

66 EDPB (n 50) 10-11.

67 Brendan Van Alsenoy (n 47) 439.

DX	
(iv) Retrieval of the bid request and (vii) use of personal data	
Purpose	**Essential means**
No	No decisive influence
Controllership: No	

Table 13: Controllership test for DX for the retrieval of the bid request and the use of personal data

45 As for the sale and retrieval of the additional personal data, the legal qualification of the DX is context-dependent. In principle, the sale of personal data as a 'product'[68] can be qualified as a processing operation performed by either a controller or a processor, depending on whether the seller determines its own purposes and means.[69] The decisive factor is whether the service provided is specifically targeted at processing personal data. If so, likely, the service provider cannot determine the purpose of the processing activities.[70] In the RTB auction, the DX offers the sale of data as a product, as a specific service and against remuneration, which is *per se* not sufficient to identify an own purpose in the processing.[71] Not gaining any additional benefits from the sale of data to DSPs, the DX is a processor for the sale and the retrieval of additional personal data,[72] as summarised in Table 14 below. However, the result of this assessment would be different, for instance, in all those cases in which the transfer of personal data is bidirectional (i.e., both from the DX to DSPs and from DSPs to the DX). If so, it is reasonable to argue for the existence of an own purpose in the processing for the DX as, through the processing operations performed, it can enrich the amount of personal data collected and enhance the quality of the services offered.

DX	
(v) Sale and (vi) retrieval of additional personal data	
Purpose	**Essential means**
No	Using infrastructure provided by DSPs, but makes the processing possible and choose when ending the processing
Controllership: No	

Table 14: Controllership test for DX for the sale and retrieval of additional personal data

d.) Joint Controllership

46 Since both advertisers and DSPs are controllers in their own right for the processing operations performed during the second phase of the RTB auction, we now ascertain whether they are joint controllers.

47 The processing operations would not occur without the decisions taken by both advertisers and DSPs. Even though the purposes pursued by the two types of entities differ, both are benefitting from the same processing operations, so that their commercial purposes are mutually complementary.[73] Moreover, both types of entities participate in determining the means of the processing: while DSPs provide the infrastructures for the processing, advertisers actively decide to make use of them, thus enabling the processing.[74] The processing cannot be considered separable, as it could not be performed by one party without the intervention of the other:[75] therefore, advertisers and DSPs are joint controllers for (at least part of) the processing.

48 The extent of the joint control depends on the advertisers' contribution to the determination of the essential characteristics of the processing. By decid-

68 Namely, personal data already collected, aggregated and analysed.

69 For two different qualifications, see EDPB (n 8) 17-18 and Brendan Van Alsenoy (n 47) 405.

70 EDPB (n 8) 27.

71 *Ibid.* 50.

72 This conclusion is supported by: Jaap Wieringa and others 'Data analytics in a privacy-concerned world'(2021) 122 J. Bus. Res 915, 917, 923; Brittany Martin 'The Unregulated Underground Market for Your Data: Providing Adequate Protections for Consumer Privacy in the Modern Era' (2020) 105 Iowa Law Rev. 865, 885.

73 Opinion of AG Bobek (n 56) para 105.

74 CJEU (n 17) para 75.

75 EDBP (n 8) 19-20.

ing to start a RTB advertising campaign and signing a contract with DSPs, advertisers exercise a decisive influence on the retrieval of the bid request and further use of personal data. However, the joint controllership for the sale and subsequent retrieval of additional personal data depends on if advertisers can decide on whether whether to buy the data and from which DX. If that is not the case, these two processing operations are out of the advertisers' sphere of influence and under the sole control of DSPs.

Tables 15 and 16 below summarise the assessment of oint controllership between advertisers and DSPs.

Advertisers and DSPs	
(iv) Retrieval of the bid request and (vii) use of personal data	
Joint determination of purpose	**Joint determination of means**
The entities pursue purposes which are complementary	The entities rely on the same infrastructure, provided by DSPs, while advertisers make the processing possible and choose when ending the processing
Joint controllership: Yes	

Table 15: Joint controllership test for advertisers and DSPs for the retrieval of the bid request and the use of personal data

Advertisers and DSPs	
(v) Sale and (vi) retrieval of additional personal data	
Joint determination of purpose	**Joint determination of means**
The entities pursue purposes which are complementary	The entities rely on the same infrastructure, provided by the DSPs, while advertisers set the parameters
Joint controllership: Only if advertisers are setting parameters on essential means	

Table 16: Joint controllership test for advertisers and DSPs for the sale and retrieval of additional personal data

II. Macro Level

49 In the micro-level analysis [Section I.], we qualified the entities of the RTB ecosystem vis-á-vis the processing operations in which they are involved. The results of the analysis are summarised in Table 17 below

Processing operation	**Actor(s) involved**	**Legal qualification(s)**	**Joint controllership**
(i) Retrieval of cookies	Publisher	Controller	Yes
	AdX	Controller	
	SSP	n/a	n/a
(ii) Creation of bid request	Publisher	Controller	Yes
	AdX	Controller	
	SSP	n/a	n/a
(iii) Transfer of bid request	Publisher	Controller, if setting parameters on means	Only if publisher sets parameters on means
	AdX	Controller	
	SSP	n/a	n/a
(iv) Retrieval of bid request	DSPs	Controllers	Yes
	Advertisers	Controllers	
	DX	n/a	n/a
(v) Sale of additional personal data	DSPs	Controllers	Only if advertisers set parameters on means
	Advertisers	Controllers, if setting parameters on means	
	DX	Processor	n/a
(vi) Retrieval of additional personal data	DSPs	Controllers	Only if advertisers set parameters on means
	Advertisers	Controllers, if setting parameters on means	
	DX	Processor	n/a
(viii) Use of personal data	DSPs	Controllers	Yes
	Advertisers	Controllers	
	DX	n/a	n/a

Table 17: Results of the micro-level analysis

50 Starting from these results, we conduct the macro-level analysis of the RTB auction process, to identify further joint controllerships.

51 On the one hand, we can imagine the seven processing activities as a unified set of operations pursuing a unified and jointly determined purpose, that of performing a RTB auction, to the economic benefit of all the four entities involved. Even though the publisher, the AdX, DSPs and advertisers pursue their own diverse purposes, all of them can be considered as closely linked and mutually complementary, as they all contribute to substantiate the RTB auction process, which would be impossible without the participation of all these entities.[76]

52 On the other hand, the argument does not hold for the means of the processing. For instance, while the publisher is exercising a decisive influence on the processing means used by the AdX, an equally decisive influence is not exercised on the means of DSPs. Similarly, while advertisers are influencing the processing of DSPs, they are not equally influencing the processing of the AdX. Therefore, the publisher, the AdX, DSPs and advertisers are joint controllers only vis-á-vis those processing operations of the processing chain for which they exercise a decisive influence on the means of processing.[77]

53 As for the retrieval of cookies and the creation of a bid request, the micro-level analysis still stands: since the processing is not separable and could not be performed by only one party, the publisher and the AdX are joint controllers.

54 As for the transfer of the bid request to DSPs, the assessment is more context-dependent. The publisher and the AdX are joint controllers whenever the first can set any of the parameters on the transfer of personal data. Otherwise, the processing is out of the publisher's sphere of influence. Additionally, we can theorise a further joint controllership between (the publisher,) the AdX and DSPs, whenever DSPs rely on the AdX's infrastructure to transfer the bid request, and especially if they set parameters on the types of requests they process. Otherwise, the transfer of personal data involves sole controllers.

55 As for the retrieval of the bid request, the micro-level analysis still stands: DSPs and the advertisers are joint controllers, as the processing is, again, not separable. Additionally, we can theorise a further joint controllership between DSPs, advertisers and the AdX, whenever the AdX provides the infrastructure enabling the transfer and retrieval of the bid request by DSPs.

56 As for the sale and retrieval of additional personal data and their further use, the micro-level analysis still stands: advertisers and DSPs are joint controllers for the sale and retrieval of additional personal data whenever they set parameters on the processing, while they are always joint controllers for the use of the personal data.

57 The final results of the (joint) controllership assessment are summarised in Table 18 below.

76 CJEU (n 17); CJEU (n 11).

77 CJEU (n 17) para 70.

Processing operation	Actor(s) involved	Legal qualification(s)	Joint controllership
(i) Retrieval of cookies	Publisher	Controller	Yes
	AdX	Controller	
(ii) Creation of bid request	Publisher	Controller	Yes
	AdX	Controller	
(iii) Transfer of bid request	Publisher	Controller, if setting parameters on means	Only if publisher sets parameters on means or if DSPs use infrastructure and set parameters on means
	AdX	Controller	
	DSPs	Controller, if using infrastructure and setting parameters on means	
(iv) Retrieval of bid request	DSPs	Controllers	Yes
	Advertisers	Controllers	
	AdX	Controller, if providing infrastructure	Only if AdX provides infrastructure
(v) Sale of additional personal data	DSPs	Controllers	Only if advertisers set parameters on means
	Advertisers	Controllers, if setting parameters on means	
	DX	Processor	n/a
(vi) Retrieval of additional personal data	DSPs	Controllers	Only if advertisers set parameters on means
	Advertisers	Controllers, if setting parameters on means	
	DX	Processor	n/a
(viii) Use of personal data	DSPs	Controllers	Yes
	Advertisers	Controllers	

Table 18: Final results of the controllership assessment

D. The Problematic Consequences of Joint Controllership in RTB

58 Pursuant to Article 26 of the GDPR, when two or more controllers are joint controllers, they must determine their respective responsibilities to ensure compliance with the data protection obligations in a transparent manner, particularly regarding the data subjects' rights and the duty to provide information. In other words, joint controllers have the flexibility to decide among themselves who will comply with what obligations established by the GDPR, as long as full compliance is ensured.[78] However, reaching an effective allocation responsibilities in the context of RTB is particularly difficult.

59 First, due to the high number of entities participating to a single RTB auction, the implementation of Article 26 of the GDPR is complex. While contractually assigning responsibilities among the publisher and the AdX can be feasible, this becomes ex-

78 EDPB (n 8) 43.

tremely more complicated, for instance, whenever DSPs are joint controllers: this scenario requires as many joint controllership agreements as many as there are DSPs participating in the auction. This complexity is exacxerbated when the group of joint controllers extends to advertisers, since the number of joint controllership agreements needed increases exponentially.

60 Second, the high number of joint controllers in a single RTB auction inevitably leads to a lack of clarity and transparency.[79] In the words of the CJEU's Advocate General Bobek, "[...] effective protection of something tends to dramatically decrease if everyone is made responsible for it. Making everyone responsible means that no-one will in fact be responsible. Or rather, the one party that should have been held responsible for a certain course of action, the one actually exercising control, is likely to hide behind all those others nominally 'co-responsible', with effective protection likely to be significantly diluted."[80] Paradoxically, this lack of transparency particularly impacts the two controllers' obligations expressly mentioned by Article 26 of the GDPR: the duty to ensure data subjects' rights and the related duty to provide information.

61 This diluted distribution of control leads to a problematic unpredictability.[81] As concluded above [Section C.II.], the entities involved in the RTB auction are joint controllers only for some of the processing operations in the chain, with the extent of the joint controllership highly depending on the parties' practical implementation of the RTB protocol. As a result, it is extremely difficult to predict which entity is a joint controller for each processing operation.[82] This unpredictability primarily affects data subjects, who should always be aware of the identity of the responsible controller so to effectively exercise their rights. However, it also negatively impacts joint controllers. For instance,[83] controllers will particularly struggle to respect their duty to inform data subjects about the processing performed.[84] The controller contractually assigned by the joint controllers to ensure compliance with Article 13 of the GDPR is obliged to provide data subjects with the identities and contact details of all the controllers, the purposes of the processing, and the specific[85] recipients of the personal data.[86] Since controllers have the duty to provide meaningful information on the most important consequences of the processing,[87] the assigned controller cannot only provide information restricted to those processing operations in the chain it controls without violating the principle of transparency.[88] However, the assigned controller can provide meaningful information only if it can rely on the cooperation of all the controllers involved in the processing operations in the chain, including those outside of the assigned controller's sphere of influence. Since there is no central entity with a complete overview of who is involved in the auction, the assigned controller will face great difficulties in obtaining the information required by Article 13 of the GDPR. The assigned controller will face even more troublesome difficulties while trying to comply with data subjects' right to access a faithful reproduction of all their personal data processed, including any further data that may be generated during the processing[89] (e.g., users' profiles generated through aggregated data). Still, this compliance burden is unreasonably shifted towards a (joint) control-

79 Article 29 Data Protection Working Party 'Opinion 1/2010 on the concepts of "controller" and "processor"' WP169, 24.

80 Opinion of AG Bobek (n 56) para 92.

81 Benjamin Wong 'Problems with controller-based responsibility in EU data protection law' (2021) 11 Int. Data Priv. Law 375, 379.

82 *Ibid.*

83 See René Mahieu and Joris van Hoboke 'Fashion-ID: Introducing a phase-oriented approach to data protection?' (*European Law Blog,* 30 September 2019) <https://europeanlawblog.eu/2019/09/30/fashion-id-introducing-a-phase-oriented-approach-to-data-protection/> accessed 31 January 2024.

84 GDPR (n 6) Article 13.

85 Case C-154/21 *RW v Österreichische Post AG* [2023] ECLI:EU:C:2023:3, para 46.

86 GDPR (n 6) Article 13(1)(a), (b), (e).

87 Article 29 Data Protection Working Party 'Guidelines on transparency under Regulation 2016/679' WP260 rev.01, 7.

88 René Mahieu and Joris van Hoboke (n 84).

89 Case C-487/21 *FF. v Österreichische Datenschutzbehörde* [2023] ECLI:EU:C:2023:369, para 70.

ler that does not have real control on some stages of the processing.[90]

62 The problematic allocation of responsibilities among the high number of joint controllers in a RTB auction has serious consequences for the possibility to ensure effective and complete protection of data subjects' rights.[91] Over the last years, national data protection authorities have investigated the RTB ecosystem's (often poor) compliance with the GDPR.[92] Recently, the issue escalated to the CJEU, which analysed the personal data processing in the Transparency & Consent Framework, a standardised tool provided by the European branch of the Interactive Advertising Bureau (IAB) to facilitate compliance with the GDPR.[93] While the CJEU applied its established doctrine [Section B.I.] to shed light on the personal data controllership within the Transparency & Consent Framework,[94] the narrow focus of the proceeding did not allow the Court to delve into the broader topic of the (joint) controllership within RTB in general. This occasion will probably be seized soon by Hamburg's data protection authority, which is currently investigating the GDPR-compliance of the data sharing operations within the broader RTB ecosystem.[95] Meanwhile, the (joint) controllership test performed in Section C. of this paper sheds some light on the roles and, therefore, responsibilities of the entities involved in a RTB auction to the benefit of both data subjects and joint controllers. While the controllership assessment, as summarised in Table 18 above, cannot *per se* resolve all the challenges created by RTB, it can lessen its lack of transparency and unpredictability, thus facilitating the exercise of data subjects' rights and a clearer allocation of responsibilities among the joint controllers.

90 Benjamin Wong (n 82) 379.

91 CJEU (n 7) para 34.

92 DOS-219-01377 *Decision on the merits 21/2022 of 2 February 2022* [Gegevensbeschermingsautoriteit, 2022]; MED 2018-042 (n 65); MED 2018-043 *Décision n° MED 2018-043 du 8 octobre 2018 mettant en demeure la société x* [CNIL, 2018]; MED-2018-023 *MED-2018-023 du 25 juin 2018 mettant en demeure la société X* [CNIL, 2018].

93 Interactive Advertising Bureau Europe, 'Transparency & Consent Framework' (*IAB Europe*, May 2023) <https://iabeurope.eu/transparency-consent-framework/> accessed 12 August 2024.

94 Case C604/22 *IAB Europe v Gegevensbeschermingsautoriteit* [2024] ECLI:EU:C:2024:214, paras 52-77.

95 Mattia Fosci, 'The Death and Rebirth of the Real-Time Bidding' (*Anonymised*, 6 March 2023) <https://www.anonymised.io/blog-posts/the-death-and-rebirth-of-real-time-bidding> accessed 12 August 2024.

Liability for Wrongful Behaviour in the Metaverse

by **Lorena Arismendy Mengual ***

Abstract: Although the Metaverse presents various potential legal issues including cybersecurity problems, jurisdictional conundrums, an obscure characterization of digital property, and personal data protection just to name a few. This paper specifically focuses on those issues arising from avatar misconduct in online virtual worlds. It is argued that harm suffered by a person may be caused by or through an avatar and that this argument hinges on whether avatars are recognised as legal persons and the lack of said recognition. Currently, avatars do not have legal personhood, making it an essential task to identify a liable party, prove harm and causation, and establish a basis for imputation to successfully bring a claim for compensation before national courts of Law. These issues must be addressed under existing regulations, highlighting the need for new approaches to handle these situations effectively when adequate. Civil liability for tortious conduct is examined under civil law systems to shed some light on whether actions by or through avatars in online virtual environments can be translated into this framework, leading to the enforceable legal consequence that is compensation for harm suffered.

Keywords: Metaverse, Online Platforms, Avatars, Civil Liability, Fault, Damage

Recommended citation: Lorena Arismendy Mengual, Liability for Wrongful Behaviour in the Metaverse, 15 (2024) JIPITEC 229 para 1

A. Introduction

1 In the dynamic landscape of the Metaverse, avatars are the digital embodiment of users, facilitating interactions and representing their virtual identity. As technology continues to evolve, the regulatory framework and the legal implications of interactions through avatars remain a subject of interest and debate. Therefore, this research paper explores the framework of non-contractual civil law claims for damage caused through an avatar in virtual worlds, where such claims are brought under a fault-based liability regime.

2 Although the Metaverse presents various potential legal issues, including cybersecurity problems, jurisdictional challenges, an obscure characterization of digital property, and personal data protection, this paper focuses on those issues arising from avatar misconduct in virtual worlds, considering that the Metaverse is currently dominated by so-called "walled gardens."

3 With virtual interactions becoming more prevalent and present in our daily lives, and with the advent of web4.0, the infringement of rights and other legally protected interests multiplies exponentially. Consider, for instance, real cases of alleged virtual

* Dr. Lorena Arismendy Mengual is a Private Law Professor at CUNEF University; ORCID: https://orcid.org/0000-0002-9969-9186; The author expresses gratitude to the Institute of European and Comparative Law (IECL) at Oxford University for their insights during the IECL Seminar Series in Trinity term 2024. Acknowledgment is also given to Keble College for its funding and support during the completion of this research.

sexual violence or assault already taking place.[1] Although criminal offences are outside the scope of this paper, these reports are a reminder that misconduct in digital environments, especially when immersive, should be taken seriously to better understand the path towards adequate relief for any compensable harm caused in a digital reality. It is argued in this study that despite their digital nature, avatars can be the source of real-world harm and thus are subject to real-world legal principles. By exploring cases where harm inflicted through avatars must meet with established legal regimes, insights are provided into the institution of civil liability and compensation.

4 This paper used a normative juridical method to approach these issues, incorporating statute, case, analytical, and comparative approaches. The study relied on secondary data gathered through literature reviews. Primary and secondary legal materials were used, and information was analysed using mostly a descriptive-qualitative method. After considering a deemed necessary differentiation between the concept of the Metaverse with that of online virtual worlds, an in-depth exploration of avatars in the Metaverse and online virtual worlds is addressed, particularly focusing on the impact of wrongful behavior performed by users when it is harmful. The question of AI-equipped avatars and prohibited AI practices is also addressed. The discussion then raises questions about legal personhood and the appropriate remedial responses to address the harm caused via avatars as well as key issues in fault-based liability regimes, including fault, causation, and compensation.

B. Preliminary Remarks

5 As an opening remark, it is stressed that it is necessary to distinguish between the Metaverse and metaverses because legal issues arising from these two concepts can differ significantly.

6 The Metaverse (singular and with a capital "M") refers to a unique, interconnected technological landscape which is envisioned as a seamless, persistent online realm where users can interact with digital elements as well as with other users in real-time, which has been described as living in a *digital reality*.[2] Although there is no consensus on a definitive definition of the Metaverse, it has been argued that the Metaverse is not simply a place or a destination accessible through a virtual reality device. Instead, it represents a complex technological environment that ultimately transforms habits, daily activities, acts and/or legal transactions as they occur in the real world, with equivalent ones in a digital world. Bearing this in mind, the Metaverse can be defined as a unique digital ecosystem which, through the use of different technologies, allows the physical and digital aspects of people's lives to converge in the same immersive experience in such a way that users perceive a persistent, synchronous, and interoperable environment where they can seamlessly transition between different digital spaces, engaging in social, economic, commercial, labour, cultural, industrial, legal, political, and other activities within a digital reality.[3] According to the leading technology scholarly opinion, the Metaverse is currently experiencing a development stage. However, experts anticipate that this evolution could occur relatively swiftly.[4]

1 The feelings of disorientation and confusion experienced by a SumOfUs researcher –only two hours into navigating in Meta Horizon Worlds in 2022–, are as real as the result of other types of socially acceptable scarring experiences. In this case, while using a female-looking, the researcher's avatar was lured into a private room during a virtual party, where another user allegedly, non-consensually approached her in such a way that she described as *rape*. The case exemplifies that the digital reality perceived in online virtual worlds by real-world users can trigger legally relevant responses to harmful conduct when performed by digital means of an avatar. The full report can be consulted here: <https://www.eko.org/images/Metaverse_report_May_2022.pdfhttps://www.eko.org/images/Metaverse_report_May_2022.pdf> Accessed: 26 Sept. 2024.

2 T R Gadekallu, *et al.* 'Blockchain for the Metaverse: A Review' (2022) arXiv preprint arXiv:2203.09738, 7.

3 L M Arismendy Mengual 'Legal Challenges of the Metaverse: Data Protection, Intellectual Property and Civil Liability' (2023) 80 Cuadernos de Derecho y Comercio 74.

4 J Dionisio, et al; '3D virtual worlds and the metaverse: Current status and future possibilities' (2013) 45(3) ACM Computing Surveys (CSUR) 2-3; D Wang, X Yan and Y Zhou 'Research on Metaverse: Concept, development and standard system' (2021) 2nd International Conference on Electronics, Communications and Information Technology (CECIT). IEEE, 983-991; C Hackl et al *Navigating the Metaverse* (John Wiley & Sons Newark 2022) 46.

7 On the other hand, metaverses (in lowercase and possibly in a plural form) refer to multiple, distinct online platforms showcasing digital worlds. These have been the focus of most scholarly attention over the past few decades, often leading to confusion between this concept and the singular, wider idea of the Metaverse. Online virtual worlds are mainly digital standalone platforms offering an immersive digital world experience where users can interact, create content, and participate in activities. Still, these do not necessarily connect or integrate. Such digital worlds include individual gaming environments, virtual social spaces, or enterprise-focused virtual meeting platforms like Second Life,[5] Roblox,[6] Fortnite,[7] Minecraft[8] or Meta Horizon Worlds.[9] As Lastiri emphasizes, the idea of virtual worlds is not new among us. However, they are rapidly gaining more scholarly attention mainly due to the application and impact of blockchain technology in these scenarios.[10]

8 The legal issues arising from these two concepts are often not the same, as seen throughout this study. For these reasons, the scope of this paper will only address problems arising from avatar interactions in online virtual worlds that nonetheless take place in the Metaverse, notwithstanding some necessary reference to the Metaverse –as a whole– whenever it is adequate.

C. Avatars in the Metaverse and Online Virtual Worlds

9 Avatars, as manifestations of digital data, serve as central components of virtual interaction. Designed for immersive experiences, they represent users (whether human or otherwise) rather than static elements within digital landscapes. In online virtual worlds, the user is their avatar; which acts as a conduit for user behavior. Avatars, lack inherent autonomy –unless powered by AI technologies. Moreover, unlike AI agents, they lack opacity or a "black box" effect.[11] This section addresses several relevant aspects of avatars to determine and assess civil liability for wrongful behavior in online virtual worlds; digital identity, some inquiries into a possible legal status, and the overall involvement of online platforms are considered.

I. Digital Identity in the Web3.0 and the Web4.0.

10 This section addresses the relevance of the connexion between avatars and their controllers through the notion of identity. It is herein considered that the question of the legal consequences of using avatars also falls within a broader digital identity framework. It is also argued that the human user's perception of the avatar constitutes a fundamental element in establishing the legal relevance of using avatars. Understanding this perception is crucial for framing the legal discourse on avatars, as it underpins some implications of digital representation and the extent to which virtual actions may translate into legal consequences in real-world contexts.

11 Besides being considered a key factor to protect individuals and their digital interactions online –as set forth by the European Parliament and the Council and the Commission joint Declaration on Digital Rights and Principles for the Digital Decade,[12] the

5 <https://secondlife.com/> Accessed: 26 Sept. 2024. A good example of this is presented by early Metaverse researchers such as J Kemp and D Livingstone 'Putting a Second Life "metaverse" skin on learning management systems' (2006) Proceedings of the Second Life education workshop at the Second Life community convention, 12; A Kaplan and M Haenlein 'The fairyland of Second Life: Virtual social worlds and how to use them', (2009) 52 6 Business horizons 563-572; A Davis et al. 'Avatars, people, and virtual worlds: Foundations for research in metaverses' (2009) 10(2) Journal of the Association for Information Systems, 1; as well as more current works, cf. I Filipova 'Creating the metaverse: consequences for economy, Society, and Law' (2023) 1(1) Journal of Digital Technologies and Law 7–32.

6 <https://www.roblox.com/> Accessed: 26 Sept. 2024.

7 <https://www.fortnite.com/> Accessed: 26 Sept. 2024.

8 <https://www.minecraft.net/> Accessed: 26 Sept. 2024.

9 <https://horizon.meta.com/> Accessed: 26 Sept. 2024.

10 M Lastiri Santiago 'Metaverse in the world of trademark law' (2024) Uniform Law Review, 2.

11 Infra. Section C.IV. (AI-equipped avatars' wrongful behavior).

12 For the purposes of this paper, identity is also approached

idea of identity relates to the sense of self, and engagement, for this work, within digital platforms. In this sense, a person will use an avatar to identify him or herself in a given digital world.[13] This raises a concern for the extension and the applicability of this concept from physical to digital domains.

12 The immersive experience provided by online virtual worlds in the Metaverse is partly facilitated by the perception of a Metaverse digital reality through the avatar. The graphical representation of an avatar can range from realistic human likenesses to fantastical creatures, abstract shapes, or even inanimate objects. The level of detail can vary considerably depending on the platform where it is created, from highly detailed, lifelike models to simplistic, cartoonish designs. This study argues that this variety raises essential legal questions about the extent to which avatars are treated under existing law.

13 Customisation possibilities, although seemingly trivial and unimportant, are not without potential legal consequences, the extent of which remains to be determined. Some examples can be emphasised:

1. The visible appearance of the avatar may qualify as a protected work under European intellectual property protection rules to which the user may be entitled if it meets the necessary originality criteria, provided the platform in question has not reserved such rights under their Terms of Service.[14]

2. Changes made by platforms to avatars' appearance can directly impact users' rights to the digital goods they have acquired to customize them, which could constitute grounds for a contractual liability claim. In this sense, and regardless of the motivation, users might invest in their avatars, e.g., by purchasing digital clothing items or accessories with their real money. This makes it questionable for online platforms to unilaterally alter the overall look of avatars, as recently exemplified by Niantic's decision to update and alter avatar appearances in Pokémon Go, which has sparked controversy among users.[15]

3. The likeness of avatars may be subject to unauthorised use by another; as Lake argues, users could be recognised in their online communities based on the appearance and popularity of their avatars; which often results in other users being increasingly tempted to exploit the popularity of another's avatar and deceive or mislead others for personal gain.[16] The use of avatars can therefore make an impact on real-world reputation and rights.

4. According to some studies, it is possible for users to develop deep psychological attachments to their digital twins. In this regard, digital identity in online virtual worlds certainly involves the concept of self-presence, which closely relates to the subjective feeling of existing within the digital sphere. While identifying themselves with their avatars, participants of a virtual world can experience what happens to the avatars in the virtual world as happening to themselves.[17] Self-presence is a psychological condition wherein individuals perceive their virtual identity (avatars) as synonymous with their real-world persona.[18]

as a key factor to protect individuals and their digital interactions online, as set forth by the European Parliament and the Council and the Commission joint Declaration on Digital Rights and Principles for the Digital Decade, Brussels, 26 January 2022, COM(2022)28 final. Chapter II: Solidarity and inclusion, and Chapter V: Safety, security and empowerment.

13 A comprehensive definition and notion of identity can be found in D Parfit 'Personal Identity' (1971) 80(1) The Philosophical Review, 3-27.

14 For instance, Second Life allows users to retain intellectual property rights in their digital creations, including avatar characters and other types of digital objects, cf. <https://lindenlab.com/legal/second-life-terms-and-conditions> Accessed: 26 Sept. 2024; Also: infra. Section D. (Harm caused via avatars).

15 The press release of the event: <https://pokemongolive.com/rediscovergo> Accessed: 26 Sept. 2024.

16 J Lake 'Hey, You Stole My Avatar!: Virtual Reality and Its Risks to Identity Protection' (2020) 69 Emory L. J. 836.

17 J M Balkin 'Virtual Liberty: Freedom to Design and Freedom to Play in Virtual Worlds' (2004) 90(8) Virginia Law Review, 2048.

18 J-A Lee, L Yang and P Hui 'Legal implications of self-presence in the metaverse' (2023) 25(4) Media & Arts Law Review, 268. The authors follow Belk's 'extended self' theory and argue that there is a digital equivalence concerning the connection between users and their digital identities. R W

This argument has been supported by several legal, psychological, and sociological studies, which also provide a basis for potential claims for moral damages.[19]

14 While acknowledging the ongoing nature of these discussions, the above underscores the possibility of compensable harm being caused to human users, and that it may ground a claim for damages where legal interests can be infringed.

15 It is also argued here that one must consider that avatars might not be a reliable source for identifying individuals in online virtual worlds. The nature of interactions in virtual worlds complicates identifying individuals responsible for harmful conduct, potentially impeding the pursuit of compensation for damages. This is founded on two main reasons: (i) the Metaverse is currently composed of "walled gardens", meaning each virtual world operates independently with its own set of rules, systems, and user data. This fragmentation prevents a unified method of identification across different platforms; (ii) a user may create and operate in an online virtual world with multiple avatars rather than a singular one, making it difficult to associate a specific avatar with a particular individual consistently.[20]

16 Otherwise, as far as technology goes and similarly argued by some scholars, other technologies do a better job for accurately and legally identifying users in online virtual worlds.[21] For example, blockchain-based ID protocols have emerged as a considerable solution. These protocols could make use of the public, transparent and decentralised nature of blockchain technology to establish secure and immutable digital identities, offering interesting authentication and verification mechanisms within virtual environments.[22]

17 Additionally, digital avatars will likely play a significant role in the so-called Web 4.0 (an autonomous, interconnected, interoperable, immersive network), according to the recent new EU strategy on Web 4.0 and Virtual Worlds.[23] Digital avatars are, in fact, a central part of virtual worlds and the Metaverse envisioned in Web 4.0. The EU strategy, therefore, aims for virtual worlds reflecting EU values and principles, where people's rights fully apply.[24]

18 The EU's commitment to ensuring that virtual worlds reflect values and rights indicates a growing acknowledgment of avatars' legal implications, reinforcing the need to address these issues as technology and virtual worlds continue to evolve. This should necessarily consider the legal implications of avatar conduct in the Metaverse, which will be addressed in the following section.

Belk, 'Possessions and the Extended Self' (1988) 15(2) Journal of Consumer Research, 139–168; R W Belk, 'Extended Self in a Digital World' (2013) 40(3) Journal of Consumer Research, 478; Although current, this notion es not new, *vid.* J W Penney, 'Privacy and the New Virtualism' (2008) 10 Yale J.L. & Tech. 221.

19 Infra. Section D. (Harm caused via avatars) of this study; F G Lastowka and D Hunter, 'The Laws of the Virtual Worlds', (2004) 92 Cal. L. Rev. 1, 73; Balkin (n17) 2043; S Triberti et al 'Changing Avatars, Changing Selves? The Influence of Social and Contextual Expectations on Digital Rendition of Identity' (2017) 20(8) Cyberpsychology, Behavior and Social Networking 501–507.

20 These ideas are emphasised in L M Arismendy Mengual 'A legal status for Avatars in the Metaverse from a Private Law perspective' (2024) 2 InDret 109. A clear explanation on online virtual worlds governance from a technological perspective can be found in T R Gadekallu (n2) at 2, 8, 10, 13-14.

21 See for instance the proposal for a registration system for online personas. J Bryson et al. 'Of, for, and by the people: the legal lacuna of synthetic persons' (2017) 25 Artificial Intelligence and Law 273–291.

22 See for instance N Schreier R Renwick and T Ehrke-Rabel (2021). 'The Digital Avatar on a Blockchain: E-Identity, Anonymity and Human Dignity' 2(3) Austrian Law Journal 202–218.

23 More information on this initiative is available here: <https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3718> Accessed: 26 Sept. 2024.

24 According to the recent *Trend Report of Virtual Worlds (Metaverse)* published on 24 May 2024 by the Directorate-General for Communications Networks, Content and Technology, see: <https://blockchain-observatory.ec.europa.eu/publications/trend-report-virtual-worlds-metaverse_en?prefLang=et> Accessed 28. May 2024.

II. Wrongful Behavior in Online Virtual Worlds. A Brief Assessment of the Impact of the Terms of Services

19 For this study, wrongful behavior—regardless of the perpetrator—is outlined narrowly. Hence, this paper focuses on addressing harmful misconduct, and finds an obligation to compensate, also disregarding criminal offences.[25]

20 Wrongful conduct in virtual platforms often involves actions that, if committed in the physical world, would fall under established civil liability fundamentals such as damage —mainly[26]— fault or negligence as well as causation. As virtual worlds become more immersive and realistic, the lines between virtual and physical worlds blur. As stressed above, actions taken in online virtual worlds can have real-world consequences, both psychological and patrimonial. Therefore, it is critical to identify a clear legal framework to address wrongful conduct in these spaces, as the impact can be just as severe as in the physical world, as is argued herein.

21 In online virtual worlds, covenants set out in End User License Agreements (EULA) or in the Terms of Service (ToS) are not a mere formality for access to metaverses. Indeed, these agreements are legally binding for the parties involved and cover a range of matters, including detailed regulations of behavior, rights, and obligations of users. They fundamentally establish the limits of what is allowed in each virtual world while also granting the platforms extensive moderation powers over user conduct.[27]

22 This provides a context for online interactions among users within an online virtual world but does not set out rules for harm that may be caused, e.g., to a third party. Moreover, as will be explored in this study, even if users agree to the ToS, this does not exempt anyone who causes compensable damage to another person from tort liability. Even with these agreements, online virtual world platform owners still face significant difficulties in ensuring user safety within virtual worlds. The sheer volume of user interactions makes it difficult for platform owners to oversee and manage every occurrence of misconduct, which they are also not obliged to do.[28] Another section of this work considers the scope of their obligation in light of the recent EU Digital Services Act (DSA).[29]

III. Misconduct by or Through an Avatar; Queries on Legal Personhood and Remedial Responses. A Matter of Control

23 This section addresses the question of whether avatars themselves can bear liability for harmful interactions in online virtual worlds, considering it a prerequisite to the attribution of liability in any legal system worldwide.

24 Legal personhood is typically ascribed to natural persons and legal entities in most legal systems. Avatars, as digital proxies for users, do not possess independent legal personhood today.

25 This clarification is deemed necessary, as for scholars from common law systems, "wrong" typically refers to torts, breaches of contract, and breaches of confidence or confidentiality (whether contractual or not). More broadly, according to the English legal perspective, a "wrong" involves a breach of duty. This broader definition arises from the fundamental effort not to limit the concept of wrongs exclusively to torts or fault. P Birks. *Introduction to the Law of Restitution* (Clarendon Press, Oxford, 1985) 313; A Burrows *English Private Law* (3rd edn Oxford University Press Oxford 2013).

26 Notwithstanding that, in civil law, there are several possibly applicable liability regimes. See infra. Section E. (Main issues in fault-based liability regimes. Considerations on fault, causation, fault, and compensation).

27 J Langenderfer 'End-User License Agreements: A New Era of Intellectual Property Control' (2009) 28(2) Journal of Public Policy & Marketing, 202-211; J M Balkin 'Law and Liberty in Virtual Worlds' In *The State of Play* (2nd edn. New York University Press New York 2020) 86–118.

28 This has expressly been stated by the Court of Justice of the European Union. See for instance: Case 70/10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL* (SABAM), ECLI:EU:C:2011:771. Recital 30 of the Regulation (EU) 2022/2065 (Digital Services Act) –Further addressed in Section C.V. (Other liable agents? Views on secondary or vicarious liability)– confirms the same stance.

29 Infra Section C.V. (Other liable agents? Views on secondary or vicarious liability).

25 The need for proper regulation of avatars has been explored for over a decade,[30] coinciding with the launch and popularisation of virtual reality platforms. Scholars advocating for legal personhood of avatars mainly argue over a *de lege ferenda* viability of a recognition analogous to that already granted to juristic persons.[31] A similar argument has been made regarding AI agents, suggesting they should be given legal personhood due to their autonomous agency and complex capabilities. However, it should be useful to remark that this argument has not changed their legal status; AI systems have not been recognised with any form of independent or intermediary legal personhood despite their increasing autonomy from programmers or designers. Moreover, following the implementation of the Regulation (EU) 2024/1689 (AI Act),[32] there has been no such recognition. This can be considered a clear indication of how the European Union intends to approach the issue. Other minoritarian approaches consider, e.g., a *tertium genus* affairs parallel to the e-personality posed by the Committee on Legal Affairs of the European Parliament for AI agents.[33]

26 Minding this situation, a further case for avatar legal personality has risen under the premise that avatars may be endowed with self-learning capabilities or may be able to make autonomous decisions (which may be wrongful) and should be treated separately from their controller, at least for all civil liability purposes. This is the case of the so-called increasingly smart avatars.[34]

27 To be sure, it was argued that avatars can identify a user, the avatar being a direct representation of the user in the online virtual worlds, also possibly allowing a person to create a psychological bond with this digital immersive element. While this is herein deemed accurate, for the purposes of online virtual worlds interaction dynamics and civil liability law, avatars must be considered tools and mere conduits for another's actions, whether legal or not. It should also be considered that said control upon avatars can be asserted by an AI agent. Therefore, the avatar entails a virtual or digital character that is completely controlled by another, making control a key aspect to further analyse the legal consequences of using them.

28 By following this reasoning, responsibility for wrongful behavior using avatars should primarily fall on the controlling entity (human or otherwise); hence, as it stands, harmful behavior in online virtual worlds can only be committed *through* an avatar, rather than *by* the avatar itself.[35]

29 Moreover, an avatar in an online virtual world more closely resembles a digital good or service rather than a person. To determine its nature in this regard, it is helpful to consider whether the avatar remains within the online virtual world's cloud and can only be accessed while logging in and utilizing the online platform. In such cases, avatars are more akin to digital services than digital goods.[36] In this sense, and

30 A M Franks 'Unwilling avatars: Idealism and discrimination in cyberspace' (2011) 20 Colum. J. Gender & L. 224.

31 T Day, 'Avatar Rights in a Constitutionless World', (2009) 32 Hastings Comm. & Ent. L.J., 151; B C Cheong 'Avatars in the metaverse: potential legal issues and remedies', (2022) International Cybersecurity Law Review, 5; It has been argued that avatars bear a closer resemblance to companies than AI agents do. See for instance L M Arismendy Mengual (n20) 112-117'.

32 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828. Accessed: 23 Sept. 2024.

33 Said notion of e-personality was intended for overly sophisticated and autonomous AI agents. European Parliament (EP) 'Motion for a European Parliament Resolution' CLA 2015/2103(INL), 27 January 2017 <https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_EN.html> Accessed: 26 Sept. 2024; This proposal was clearly not accepted by renowned scholars and experts, as argued in the Open Letter to The European Commission Artificial Intelligence and Robotics, Available in: <http://www.robotics-openletter.eu> Accessed: 26 Sept. 2024.

34 W Barfield and A Williams 'Chapter 1: The law of virtual reality and increasingly smart virtual avatars', in *Research Handbook on the Law of Virtual and Augmented Reality* (Edward Elgar, Cheltenham 2018), 2-43.

35 This statement will hold true as long as no legal personhood is endowed to avatars or to AI-agents.

36 M P García Rubio 'Non Conformity of Goods and Digital Content and its Remedies' in *European Perspectives on the*

according to article 2.2. of Directive (EU) 2019/770,[37] digital service means a service that allows the consumer to create, process, store or access data in digital form; or a service that allows the sharing of or any other interaction with data in digital form uploaded or created by the consumer or other users of that service means data which are produced and supplied in digital form. From this broad and ambiguous definition, the avatar can accurately be perceived as a digital service that can be supplied by a digital service provider (labelled trader under this Directive), which in today's Metaverse would be the centralised digital world or the platform on which it is created. The Directive above does not provide many useful elements for this discussion, as it excludes many activities that already occur or are planned to be undertaken in online virtual worlds, such as gambling, health, and financial services (as specified in Article 3.5 of the Digital Content Directive). Additionally, the Directive is designed solely to regulate B2C (business-to-consumer) relationships, focusing on interactions between the trader and consumers.[38]

IV. AI-Equipped Avatars' Wrongful Behavior

30 This section addresses the essential question of scenarios where AI-powered avatars might influence or exploit users with the objective to or the effect of materially distorting human behavior, leading to real-world harm. The issue is approached particularly in light of Article 5(1)(a) and (b) of the AI Act.

31 It is herein maintained that if avatars are powered by AI systems—whether fully or partially—they should not be legally distinguishable from other AI agents. As a result, all regulatory frameworks applicable to AI agents would also apply to avatars in online virtual worlds and the Metaverse. Bearing this in mind, the rapid evolution of AI technology raises important questions about the potential for avatars to engage in increasingly autonomous wrongful actions. This development calls for a closer examination of its legal implications, including liability issues and potential remedies.

32 Although the AI Act does not resolve the issue of civil liability, it establishes important fundamental lines, such as the concept of artificial intelligence systems –as per article 3(1) of the AI Act[39] that will be ultimately applicable to AI powered avatars. This is also the case of the risk-based classification of AI systems that structures the regulation. It means that the deployment of an AI-powered avatar may entail different levels or risks; namely, unacceptable, high-risk, limited-risk, minimal-risk or no risk whatsoever.[40] This approach becomes particularly relevant when determining whether certain AI practices involving avatars fall under prohibited activities.

33 At the core of determining if an AI system practice that has been used or deployed in the market is prohibited, a joint assessment of provisions 5(1)(a) and (b) of the AI Act reveals three key aspects:

- The objective or the effect of the AI agent's deployment is to materially distort the behavior of a person or group of persons. Consequently, the provider or the deployer's intention –or lack thereof– to cause harm is ultimately irrelevant.
- The AI system causes individuals to take decisions they would not have otherwise taken.
- The AI system's intervention causes or it is reasonably likely to cause significant harm to a person, or a group of persons.

34 From this point on, the regulation differs depending on whether it addresses manipulative or exploitative practices that cause harm. Article 5(1)(a) specifically requires (i) that the AI system deploys subliminal

Common European Sales Law Studies in European Economic Law and Regulation (Springer New York 2015).

37 Directive of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services regulates contracts for the supply of digital content and services.

38 Further explanation on this topic is presented by J M Carvalho 'Sale of Goods and Supply of Digital Content and Digital Services – Overview of Directives 2019/770 and 2019/771' (2019) 8(5) Journal of European Consumer and Market Law, 194–201.

39 Cf. Recital 12 of the AI Act.

40 Critical considerations on the lack of a clear methodology for risk assessment under the AI Act are presented by C Novelli et al 'AI Risk Assessment: A Scenario-Based, Proportional Methodology for the AI Act' (2024) 3(1) Digital Society 13-26.

techniques beyond a person's consciousness (e.g. imperceptible audio, image, video stimuli),[41] or that it purposefully uses manipulative or deceptive techniques; (ii) the person's ability to make an informed decision must be appreciably impaired. On the other hand, Article 5(1)(b) addresses the exploitation of vulnerabilities –due to age, disability, a specific economic or social situation (e.g., extreme poverty, ethnic or religious minorities[42])– of a specific group of persons.

35 Many of the concepts introduced by the regulation as it stands foster greater uncertainty rather than providing much-needed clarity. For instance, it is difficult to identify a specific AI-powered avatar that employs subliminal techniques[43] and that is able to imperceptibly manipulate another user to effectively change their behavior 'beyond a person's consciousness' under Article 5(1)(a) –also, what does the latter term mean, and how can it be proven by the victim.[44] It should also be noted that the final text of these provisions suggests that manipulative or exploitive practices without harm are nonetheless acceptable.

36 Avatar-related misconduct, particularly when involving AI-driven behaviors –even if not fully autonomous legal entities– can cause real-world harm and should be subject to the same regulatory scrutiny as other AI systems. This raises a question in scenarios where the avatar is partially user-controlled yet also possesses AI autonomous capabilities.[45] Some noteworthy criteria have been raised in this regard and are also echoed here: The identification of a liable agent –who primarily operates the technology– may heavily depend on whether the service provider (ensuring the necessary technical framework for its operation) has a higher degree of control than the owner or user of an AI-equipped product or service, v.gr., the avatar. Also, the view that a person using an avatar with a certain degree of autonomy should not be held less accountable for any resulting harm than if that harm had been caused by a human auxiliary can also be herein supported.[46]

V. Other Accountable Agents? Views on Secondary or Vicarious Liability

37 Before further examining the legal configuration of a claim for damages arising from misconduct in online virtual worlds, it is important to consider the overall involvement of these worlds, which may lead to liability risks due to their platform operations.

41 Recital 29 of the AI Act.

42 Recital 29 of the AI Act, cf. Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services.

43 Although prohibitions against subliminal techniques date from more than five years, cfr. Article 9(1)(b) of the Audiovisual Media Services Directive –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 in view of changing market realities. A discussion on this topic can be found in M Franklin, et al. 'Missing Mechanisms of Manipulation in the EU AI Act' (2022) The International FLAIRS Conference Proceedings 2022.

44 The issue closely relates to the so-called dark patterns introduced in Recital 67 of the DSA regarding 'practices that materially distort or impair, either on purpose or in effect, the ability of recipients of the service to make autonomous and informed choices or decisions'; An in-depth assessment of the lack of clarity posed by Articles 5.1.a and 5.1.b of the AI Act can be found in M Leiser 'Psychological Patterns and Article 5 of the AI Act: AI-Powered Deceptive Design in the System Architecture and the User Interface' (2024) 1(1) Journal of AI law and Regulation, 6-14; Also: H Zhong et al. 'Regulating AI: Applying Insights from Behavioural Economics and Psychology to the Application of Article 5 of the EU AI Act'. (2024) 38 Proceedings of the AAAI Conference on Artificial Intelligence, 20001-20009.

45 While users can generate scripts or pre-defined tasks for their avatars when offline, no evidence of user's avatars AI-driven operation was found in this research. However, technological advancements suggest this could happen in the future. For example, Somnium Space (a virtual world platform < https://somniumspace.com/> Accessed: 26 Sept. 2024) is working on integrating AI into its avatars through a feature called the "Live Forever" mode. It is intended to allow users to have their movements, conversations, and behaviors recorded as data, which would then be used to create an AI-driven avatar that continues to exist and interact even when the original user is offline or deceased. < https://somniumtimes.com/2024/04/04/live-forever-in-somnium-space-again/>Accessed: 26 Sept. 2024.

46 These aspects reflect the opinion of the Expert Group on Liability and New Technologies New Technologies Formation Liability for artificial intelligence and other emerging digital technologies (Publications Office, 2019) 23.

38 It can be argued that platforms should bear part of the costs associated with addressing illegal content or interactions online, as they are the primary beneficiaries of the increased internet traffic generated by such content. However, solutions to this issue are not straightforward; regulatory obligations in this area may threaten users' freedom of expression and access to information online. Additionally, they may reinforce market asymmetries by favoring larger, well-resourced players over smaller competitors, potentially causing more harm than good.[47]

39 As it has been until now, the opportunities to benefit from conditional exemptions and immunity that effectively mitigate online platforms' exposure are in place under the Directive 2000/31/EC (E-commerce Directive).[48] Therefore, online platforms mostly enjoy a so-called "safe harbor" provision for claims other than intellectual property rights infringements.[49] Essentially, this provision shields online platforms from legal liability regarding user-transmitted content as long as they remove illegal content promptly upon notification. This safeguard extends to various online services like social media platforms, search engines, e-commerce sites, and hosting providers.[50] However, as a matter of definition, it is problematic to consider that online virtual worlds match such characterization as per recitals 17 and 18 of the E-commerce Directive.[51] This makes said guideline ultimately disconnected from the discussion.[52]

40 In this regard, the DSA mostly maintains the conditional liability exemptions for online intermediaries from the e-Commerce Directive. Still, it provides more detailed rules on notice-and-action mechanisms for illegal content. However, the DSA does not directly establish a new framework for civil liability related to online platforms and services. Indeed, it does not harmonize or create new rules across the EU for platforms' civil liability. Rather, it leaves this aspect largely to existing national laws, simply updating the liability exemption conditions that platforms must merely meet.[53]

41 Even if it applied to the subject matter, the underlying rules about acceptable content or behavior

47 M Mariniello 'Online Content and Platform Liability' in *Digital Economic Policy: The Economics of Digital Markets from a European Union Perspective* (Oxford University Press, Oxford 2022) 217. The author builds the argument upon Sartor's analysis and classification of online platforms and their liability risks. Cf. G Sartor *Providers liability: from the eCommerce Directive to the future: in-depth analysis* (European Parliament Brussels 2017).

48 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. I C Ballon 'Chapter 49. The Liability of Platforms (including Website Owners, App Providers, eCommerce Vendors, Cloud Storage and Other Internet and Mobile Service Providers) for User Generated Content and Misconduct' *E-Commerce and Internet Law* (2d edn Thomson Reuters West 2019).

49 Provided in Articles 12-15, but also outlined in recital 42-46 and 52 of the E-commerce Directive, Cf. Copyright Directive (Directive (EU) 2019/790), Article 17 on the use of protected content by online content-sharing service providers, under which IP right holders have the option to seek an injunction against intermediaries whose services are being used by a third party to infringe copyright.

50 G Sartor (n 47). As for the types of online platforms addressed above, a wide range of economic activities which take place on-line, including the selling of goods online on e-commerce platforms (e.g., Alibaba or Amazon) the provision offering on-line information or commercial communications (e.g. advertisement funded by sponsorship revenue), the offering of online search engine tools (e.g., Google or Bing), the transmission of information or the hosting of information through internet intermediaries, etc. G Pearce and N Platten 'Promoting the Information Society: The EU Directive on Electronic Commerce' (2002) 6(4) European Law Journal 363.

51 Á Carrasco Perera and C Álvarez López 'Operadores y responsabilidad civil en el metaverso' (2022) Publicaciones GA_P 6. Nonetheless, the authors considered that the E-commerce Directive's abstract rules of imputation could be usefully transferred in part to the metaverses model. Therefore, platforms that serve as "mere conduits" or provide hosting services, without intervening in content, are generally not held liable for third-party content they do not editorially control. These platforms are not initially obligated to filter content, except in instances of intellectual property infringements. See note 41.

52 Although certain activities within online virtual platforms could fall under digital services regulation, they do not neatly align with the current definitions of online platforms under European law.

53 M Husovec 'Rising Above Liability: The Digital Services Act as a Blueprint for the Second Generation Of Global Internet Rules' (2023) 38(3) Berkeley Technology Law Journal 118.

remain to be set by the parties. Private individual remedies like claims for damages or injunctive relief against platforms do not directly arise from the obligations set out in the DSA; therefore, injured parties will still need to rely on national tort law and liability provisions when seeking compensation for harm, which, as argued here, primarily rests upon the user.[54] Furthermore, if platforms were to be made vicariously liable for user content or interactions, the model would need to be constructed in accordance with national regulations.[55]

42 These further stress that the subject matter must be examined under national rules. While it is clear that the avatar controller might be liable, a secondary liability regime for virtual worlds requires further exploration. However, this aspect will not be addressed in this discussion due to its broad scope.[56]

D. Harm Caused Via Avatars

43 This section addresses the idea that harm in virtual platforms can manifest in various forms, such as reputational damage, psychological distress, or economic loss, considering that avatar usage does not inherently contest the existing range of compensable harm. Nonetheless, while some wrongdoings depend on tangible or physical harm in the real world—such as killing or causing physical injuries—other types of wrongful actions or omissions can transcend physical boundaries. The central question is whether these actions, when carried out through avatars, can be translated into the framework of civil liability law and result in an enforceable duty to compensate the injured party. For example, an avatar might be used to post defamatory content, leading to reputational harm, or engage in virtual harassment, resulting in psychological trauma.[57] Patrimonial losses may occur through fraudulent schemes, e.g., involving virtual currencies or digital goods, or as a consequence of using avatars to make false statements to induce others to act to their detriment.

44 A nuanced approach is necessary when harm has been caused due to an AI-powered avatar's intervention. Under the AI Act, manipulative or exploitative practices discussed above will only be prohibited when they are harmful. However, the Act sets a special severity standard for harm that is not generally required. It does so by reference to an undefined notion of "significant harm". Despite the examples provided in Recital 29 of the AI Act (v.gr., important adverse impacts on physical, psychological health or patrimonial interests), the term remains ambiguous. Even though it should not be excessively controversial to identify and measure important physical injuries or financial losses,[58] further difficulties arise when trying to determine the extent of significant psychological distress. As rightly argued by Zhong, the challenge lies in the fact that the AI Act does not clearly define what level of psychological distress counts as "significant harm." Additionally, proving that a specific AI practice caused someone's psychological harm is difficult, given that many factors can affect a person's mental state. Effectively addressing this issue may require detailed, case-by-case discussion.[59]

45 Harm is undoubtedly a fundamental element of civil liability,[60] compelling plaintiffs to prove they suffered actual damage due to the wrongful behavior exerted upon them, in this case, using an avatar. Additionally, civil liability for damages in the Metaverse, as well as in virtual worlds according to current law will only arise if a natural or legal person experiences harm in the physical world.[61]

54 M Husovec (n 45) 114-116.

55 Ibid. 118.

56 An in-depth assessment on this topic can be consulted in M Husovec *Injunctions against intermediaries in the European Union: accountable but not liable?* (Cambridge University Press Cambridge 2017).

57 Criminal liability, however, is ultimately out of the scope of this work.

58 Which is not to say that it is without controversy.

59 H Zhong 'Implementation of the EU AI act calls for interdisciplinary governance' (2024) AI Magazine, 2.

60 Cf. Article VI-2:101 Draft Common Frame of Reference (DCFR).

61 Á Carrasco Perera and C Álvarez López (n 51) 4. However, this raises practical issues, particularly when users exploit anonymity or pseudonymity to evade accountability. Courts must then determine how to trace and identify the individuals behind such avatars to attribute liability suitably. See also infra. Section D (Harm caused via avatars).

46 Some authors have considered that actions of any kind, if committed with the consent of other players or allowed by the rules of a virtual world, do not result in real-world liability, even if they cause personal or economic harm. This is allegedly because by agreeing to the end-user agreement of the virtual world, users consent to abide by that world's specific rules and laws.[62] This statement requires some considerable nuance.[63] It highlights the idea that legal scholarship has been concerned with this issue for a long time, suggesting that avatar misconduct is not an overly novel concern.

47 What sets online virtual worlds apart from traditional social networks' user interaction experience, in terms of Web 2.0 practice,[64] is the immersive nature they offer with increasingly sophisticated technology deployed. This immersion leads to various interactions being experienced more vividly and intensely as they occur from a first-person perspective. Consequently, any misconduct directed at an avatar becomes drastically relevant, as it may target the user directly. For example, unprecedented counts of sexual assault and rape in online virtual worlds have been brought up, especially since early 2000 with the launch of Second Life (a paradigmatic example of an online virtual world).[65] Although this article does not focus on the criminal nature of such conduct,[66] it does argue that damage (e.g., mental distress) can indeed result from these types of interactions which we have referred to as wrongful behavior. Furthermore, the damage –whether moral or patrimonial– should be compensated for not being a reasonable consequence of agreeing to their Terms of Service, nor should it always be considered a risk assumed by the victim when participating in an online virtual world.[67] Additionally, if the rule of law allows for a legal right to be asserted upon avatars, treating them as the object matter of a service contract, then a user could potentially suffer patrimonial losses due to the unauthorised interference by another party with one's avatar.[68]

62 F. E. Marx 'Iniuria in cyberspace' (2010) 31(1) Obiter, 150.

63 In accordance with most legal systems, when executing a contract, parties may owe duties not only to each other but also to third parties. If the actions of a contracting party harm a third party, the injured third party might have grounds for a civil liability claim. This is particularly true if the harm resulted from negligence or other fault in the performance of the contract, although contracts often include terms that allocate risks between the parties, which means that each participant might assume certain risks explicitly stated in the contract. For example, indemnity clauses, limitation of liability clauses, and waivers can all influence the extent of liability.

64 (n 4) 48; M V Rijmenam, *Step into the Metaverse: How the Immersive Internet Will Unlock a Trillion-Dollar Social Economy* (John Wiley & Sons Inc Hoboken 2022).

65 Second Life was launched in 2003, and although the most well-known instance of this type of allegation involves a SumOfUs researcher in 2022 mentioned above (note 1), it was certainly not the first. For example, in 2007, it was reported that the Brussels public prosecutor had directed patrol detectives from the Federal Computer Crime Unit to enter Second Life to investigate a "virtual rape" incident involving a Belgian user. The original press report: <https://www.demorgen.be/nieuws/hoe-second-life~ba9ce069/> Accessed 26 Sept. 2024; O Bellini 'Virtual Justice: Criminalizing Avatar Sexual Assault in Metaverse Spaces' (2024) 50(1) Mitchell Hamline Law Review 3.

66 To add some insights into this topic, it has been argued that even though rape (namely, a physical act) is not possible in an online virtual world. "Virtual rape" might constitute another type of criminal offence. For instance, Marx argued that under South African Law it could be covered in terms of section 86 of the Electronic Communications and Transactions Act 25 of 2002. The provision, basically prohibits unauthorised access and interference with data, reads as follows: "86(1) (...), a person who intentionally accesses or intercepts any data without authority or permission to do so, is guilty of an offence. 86(2) A person who intentionally and without authority to do so, interferes with data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective, is guilty of an offence. 86(3) A person who unlawfully produces for use ... a device ... which is designed primarily to overcome security measures for the protection of data ... or performs any of those acts with regard to a password, access code or other similar kind of data with the intent to unlawfully utilise such item to contravene this section, is guilty of an offence. 86(4) A person who utilises any device or computer program mentioned in subsection (3) in order to unlawfully overcome security measures designed to protect such data or access thereto, is guilty of an offence"; Other authors propose metaverse sexual assault to be regulated a crime as a matter of statue. F. Marx (n 62) 150-151. See also: Bellini (n 65) 99-107.

67 That is, unless the specific nature and purpose of the online virtual world is to allow users to perform these types of sexually explicit acts to one another in the digital environment. However, consent would undoubtedly persist as a standard for said interactions.

68 Currently, there is a significant gap in the legal

48 Rather than devising a catalogue, we will address some relevant examples of potential tort law claims arising from alleged avatar misconduct in metaverses that leads to real-world harm.

1. Right of publicity v. IPR infringement: If a real-world person's likeness is used to create a digital avatar for commercial purposes, no doubt said person would be entitled to compensation due to the avatar exploiting these traits for commercial purposes.[69] However, there is significant room for exploring the issue of commercially exploiting the likeness of a user's digital avatar for personal gain.[70] It could be argued that the right of publicity for an avatar cannot be infringed, as an avatar is not a legal person. However, it would be incorrect to assume that an avatar's possible uniqueness or distinctiveness is not currently protected under the law. This protection, under IP rights rules, likely depends on the technical capabilities of the online virtual world to create unique avatars that meet the criteria of originality and distinctiveness required for intellectual property rights protection. Furthermore, it is essential to consider whether the platform reserves economic rights over the avatar's appearance, potentially making it its own asset, as highlighted in the recent Ada case ongoing in China.[71] Those mentioned above could unfold much-needed discussions about the extent of user ownership in relation to intellectual property rights in virtual environments. However, it should be remarked that there is enough evidence today that the unauthorised use or reproduction of copyrighted or trademarked materials in the Metaverse could lead to infringement claims and compensation.[72]

2. Other personality rights infringements: These types of issues allow us to consider that users employing avatars to make false statements that harm the reputation of a real-world person, or disclosing private information could face a lawsuit for compensation if harm is caused to a user.[73] However, it appears unlikely that a defamation claim could be brought if an avatar is the target of malicious or false comments affecting the avatar's reputation, or if an avatar's private affairs are publicly disclosed without their consent.[74] Such cases would more likely fall under the right to freedom of speech of the individual making the statements, whatever their nature. However, alleging that no protection can be granted in the latter scenarios would be inaccurate. One may consider, for example, that an unfair competition practice took place, or that the controller committed passing off, ultimately damaging the goodwill of a company.[75]

conceptualization of damage inflicted upon digital property. This loop presents an interesting ground for further scholarly inquiry and analysis. While the digital realm has witnessed an exponential expansion, accompanied by a surge in the creation and ownership of virtual assets, the legal impact of harm to such assets remains mostly unexplored and largely unaddressed in case law. Cf. *Bragg v. Linden Research*, Inc. 487F.Supp.2d593 (E.D. Penn.2007) where the very interesting issue of digital property confiscation was not judged due to the parties reaching a private settlement.

69 For instance, in *Hart v. Electronic Arts, Inc.*, No. 11-3750 (3d Cir. 2013), a case involving a football player's likeness used in a video game, in which the plaintiff sued for the violation of his right of publicity. Initially dismissed by the district court, the Third Circuit Court of Appeals overturned the decision, asserting that the games didn't sufficiently alter Hart's identity, thus upholding his rights.

70 J Lake (n16) 835-878.

71 This case marked the first time a court of law has addressed whether digital avatars are entitled to copyright protection on their own. The court concluded that Ada, being controlled by humans and supported by various aiding technologies, cannot be considered the author. Rather her developer was recognised as the intellectual property rights holder of the videos featuring the avatar's image online. Hangzhou Internet Court (2022) Zhejiang 0192 Minchu No. 9983, Civil Judgement.

72 See for instance: *Hermès International, et al. v. Mason Rothschild* (2023), 1:22-cv-00384 (SDNY), also known as the *Metabirkin* case.

73 Cheong (n31); Lee (n18); Also: B M Chin, 'Regulating Your Second Life: Defamation in Virtual World' (2007) 72(4) Brooklyn Law Review 1303, 1333.

74 It is remarked that to withhold such rights, an individual must be considered a legal person.

75 Should all criteria be met in a case for these alleged causes of action, there is no fundamental or substantive reason to deny injunctive relief or compensation to the victim.

E. Main Issues in Fault-Based Liability Regimes. Considerations on Fault, Causation, and Compensation

49 Unsurprisingly, modern regulation has not specifically covered the responsibility of individuals for damage caused through avatars, nor can it evolve as fast as technology does. Even though creating a special ad hoc liability regime is always an option for legislators, the potential application of existing civil liability regimes should be assessed to avoid unnecessary efforts, especially if current frameworks can be effective. These existing regimes include the possessor's liability for damage caused by objects, often found in civil codes, product liability regimes, and liability arising from fault or negligence as a general rule by *default*.

50 Legal systems typically have strict rules regarding liability for objects or vicarious liability.[76] This first approach should result in the liability of the real-world controller of the avatar.[77] However, the rules provided in most Civil Codes do not seem to directly apply to damage caused by the emerging technology covered in this study. This is mainly because the damage an avatar can cause is akin to that caused by a person, such as infringing a person's trademark by selling goods that use another's trademark without the legitimate IP right holder's authorization–rather than that caused by an inanimate object, e.g., falling on top of someone's head.[78]

51 These parameters appear unsuitable, primarily because they are tailored to ownership or possession of tangible property, whereas avatars possess an intangible, digital nature. For instance, considering the avatar as an animal or a building under Article 1905 or 1907 of the Spanish Civil Code (CC) is likely unrealistic.[79] Similarly, Article 1908 CC outlines owner liability in specific scenarios—such as machine explosions, excessive smoke, falling trees, and sewage emissions—that are framed to address real-world physical harm and do not readily apply to avatar-related issues. Furthermore, Article 1910 CC holds the head of the household liable for damage caused by objects falling from a house or part of a house. This provision diverges from issues likely to arise in the Metaverse and in online virtual worlds, as examined above.

52 Another possibility would be the integration of avatars within the harmonised legal framework of defective product liability.[80] However, as argued by legal scholarship, the current definition of a product predominantly encompasses tangible goods, making it a major inconvenience –and overall, not feasible– to categorize avatars as such due to their inherently digital nature. While the European Commission recognizes the inclusion of certain intangible assets as products, the applicability of this classification to avatars remains ambiguous. Furthermore, it does not seem legally suitable. This ambiguity exposes a

76 Spanish Civil Code is considered as the main reference for the purposes of this work. However, other Civil Codes or legal systems are certainly noteworthy. In general, these regimes, often approach the issue by imposing strict liability for harm or damage caused by things, (e.g., dangerous objects, defective products, or sources of special danger under one's custody or control) which will rest upon the person have factual control over the object: For instance, the French Civil Code article 1243 al. 4 (covers strict liability for harm caused by corporeal things within one's keeping) and article 1266 (which allows courts to prescribe measures to prevent harm or stop unlawful nuisances caused by things); the German Civil Code Section 833 (covers strict liability for damage caused by dangerous things or activities); the Italian Civil Code article 2051 (covers strict liability for damage caused by dangerous things in one's custody, unless the custodian proves unavoidable circumstances); the Dutch Civil Code article 6:173 (covers strict liability for damage caused by dangerous substances or objects) and article 6:174 (on liability for damage caused by defective products); the Swiss Code of Obligations article 58 (on liability for damage caused by things under one's custody, unless it is proven that all due care was taken), among others.

77 Notwithstanding the problems posed by the pseudo-anonymity of avatars in the Metaverse.

78 Should such an analogy be possible, it has been argued that "if someone can be held liable for the wrongdoing of some human helper, why should the beneficiary of such support not be equally liable if they outsource their duties to a non-human helper instead, considering that they equally benefit from such delegation?". Expert Group on Liability and New Technologies New Technologies (2019) (n46) 25.

79 Liability for animals being more similar to avatar issues for that matter.

80 Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products.

disparity between conceptual ideals and practical implementation.[81] In this regard, the recently approved Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC (PLD), aims to encompass digital content or services appears to offer a more promising approach, which warrants further attention and observation.[82]

53 In general, when no specific rule exists, liability for damage caused (perhaps by using an avatar) usually depends on the defendant's fault, whether it be intentional or negligent conduct.[83] It should also be considered that users may have varying levels of control over their avatars' actions, ranging from direct manipulation to mere indirect influence; the avatar may in fact be partially AI-powered.

54 As argued by the Expert Group on Liability and New Technologies of the European Commission, whether a legal system differentiates between objective or subjective wrongdoing, or even if it separates the basis of liability for misconduct into wrongfulness and fault, identifying the duties of care the perpetrator should have fulfilled and proving that the perpetrator's conduct failed to meet these duties are both crucial.[84] Courts may need to establish a clear duty of care guidelines and reasonable standards of behavior expected from avatar controllers (users or AI deployers) based on their capabilities. However, it remains true that the plaintiff must prove fault.[85]

55 Bearing this in mind, it should be noted that running an avatar by a human controller involves that the duty of care can be measured according to duties of care intended for human conduct.[86] For example, where users deliberately direct their avatars to engage in harmful behavior, said users should be held liable at fault.

56 Should an avatar be AI-equipped, the deployer's lack of compliance with their duties of care can be assessed by specific requirements set by the AI Act.[87] The opaque nature of AI—v.gr., the difficulty in understanding and explaining how decisions are made, due to the technology's inherent complexity—makes it particularly difficult for the claimant to establish not only fault but also causation. Furthermore, the amount of agency users possess over their avatars can vary depending on the platform or virtual environment due to technical limitations or the design of online virtual worlds' dynamics.[88] As supported here, traditional compensation for damage may not always be considered a reasonable outcome if no physical or economic injury was inflicted on another. While measures undertaken by online virtual worlds, such as confiscating virtual assets or banning avatars, could serve as deterrents, they may prove insufficient in some cases. Remedial responses for

81 Especially considering that the EU aims to approach emerging technologies from this perspective. Expert Group on Liability and New Technologies New Technologies (2019) (n46) 6, 27.

82 In light of the new legal framework: "Products in the digital age can be tangible or intangible. Software, such as operating systems, firmware, computer programs, applications or AI systems, is increasingly common on the market and plays an increasingly important role for product safety". Recital 13; "Product' includes electricity, digital manufacturing files and software." Article 4.1 PLD.

83 C V Dam 'Liability for Movable Objects' *European Tort Law*, (2nd edn Oxford University Press Oxford 2013) 402-403; Under Spanish law, the general rule is that set forth in article 1902 CC.

84 Expert Group on Liability and New Technologies New Technologies (2019) (n46) 23.

85 This would involve identifying the duties of care that the perpetrator should have fulfilled and proving that their conduct failed to meet said duties. Moreover, these duties are determined e.g., by statute, or they must be assessed by the Court afterwards, based on the individual's conviction about a reasonable course of action in specific the circumstances. Ibid.

86 However, if avatars were to gain legal personhood, they could potentially be held directly at fault, raising questions about what negligence would entail in the context of avatar behavior.

87 For instance, if the deployer or the user runs a high-risk AI-driven avatar, non-compliance with requirements outlined in Chapters 2 and 3 of the AI Act can adequately be set as the standard for fault. Cfr. Recital 26 of the Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence, COM/2022/496 final.

88 Barfield and Williams (n34) 2-43.

victims of harmful behavior committed through avatars may include several well-known forms of relief. Monetary compensation is the most common remedy aimed at covering the actual damages suffered by the plaintiff. Injunctive relief, such as court orders to remove defamatory content, may be sought to prevent ongoing or future harm.

57 If an innovative way of thinking about these issues can be noted here, minimum capitalization requirements for avatars to ensure they can pay for damages, along with the potential need for platforms to have liability insurance or victim compensation funds for major incidents, are also to be considered.

58 Provided that the avatar controller (the user or the AI-equipped avatar deployer) could be held liable for their online misconduct, the plaintiff must prove a factual and legal causal link between an avatar's actions and the harm suffered. Several aspects on a technological and juridical level should be considered for this purpose. The development of the Metaverse ought to be directed towards a reasonable balance between the anonymity rights of users. This clashes with the need to identify wrongdoers to attribute fault by tracing them to their real-world operators, thereby obscuring the causal chain.[89] However, this is not a new problem arising from using avatars but rather from using Metaverse technologies.

59 Taking all of the above into account, and although it is not a perfect analogy, the discussion on proving causation may benefit from the action taken by the EU, especially in their recent Proposal for an AI Liability Directive. It is intended to apply to non-contractual civil law claims for damages caused by an AI system (possibly an AI-equipped avatar), where such claims are brought under fault-based liability regimes.[90] The proposal above is funded by a common problem with avatars in the Metaverse (as well as in some online virtual worlds, whether AI equipped or user driven); namely, that current national liability rules, particularly when based on fault, are deemed inadequate for addressing liability claims for damage caused by digital AI. The inadequacy allegedly arises from the fact that (i) victims must demonstrate a wrongful action or omission by the individual responsible for the damage, and (ii) due to the complex structure of AI, it may be excessively difficult or costly for victims to identify the responsible party and satisfy the prerequisites for a successful liability claim. As contemplated in the proposal, victims could face substantial expenses and significantly prolonged legal proceedings when seeking compensation, potentially dissuading them from pursuing it as a legitimate remedy.[91] It was pointed out that avatars do not share the same complex architecture of AI systems (opacity or the so-called "black box effect", for that matter) per se. Nonetheless, in a scenario where an avatar is operated by a human user, it's important to note that Metaverse technologies –including AI– render it excessively expensive and complicated for victims to pursue such claims. Thus, even though addressing the use of an avatar does not substantively equate to addressing that of a high-risk AI agent (as per Article 6 of the AI Act), the Proposal for an AI Liability Directive suggests adopting a presumption of causal link in instances of fault that is herein deemed also a suitable answer. The reason to apply this specific measure is that it might be analogously excessively costly for a person to prove it—not due to the use of an avatar, but rather because of the Metaverse technologies deployed that may obscure the causal chain, making that same consideration useful for the subject matter.

60 However, as a bottom line, existing laws should apply to avatar misconduct without great need for further adaptation. Current regulations are, therefore, sufficient and should be enforced in cases of wrongful behavior conducted via avatars.

89 As emphasised by technology scholars. Cf. L-H Lee et al 'All One Needs to Know about Metaverse: A Complete Survey on Technological Singularity, Virtual Ecosystem, and Research Agenda' (2021) arxiv.2110.05352 1-47.

90 COM/2022/496 final (n87).

91 Explanatory Memorandum. Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence, COM/2022/496 final.

F. Conclusion

61 In virtual worlds, a person's online identity is represented and made visible to others through their avatar. An avatar –when used by a natural or legal person– serves as a means of interaction among users, acting as their virtual representation and identity within an online virtual world. Avatars may also be the conduit for AI systems to be deployed, which is a foreseeable outcome of the advancement of technology. Despite the importance of avatars, rightly so, the idea of regulating them as legal entities has not gained significant traction. Instead, as the technology stands today, avatars can be better considered as digital data, assets or as the subject matter of a contract concluded by a real person (natural or legal), or by an AI agent within a virtual platform. This type of arrangement allows the user to assume a digital form, navigate and undertake several actions, all of which are carried out through the essentially controllable vessel, the avatar.

62 This paper argues that damage caused by using an avatar is a real-world problem and is subject to real-world law. Furthermore, as a prerequisite, any harm considered must be experienced in the real world to successfully ground a claim for compensation, which will be assessed by national rules governing this issue.

63 In respect to compensable harm, and as explained herein, while it is true that the prejudice suffered by a person constitutes an actionable claim, alleged damage asserted upon one's avatar may also ground a compensation claim wherein an actual tort can be committed. For example, as argued above, even if an avatar's right to publicity cannot be protected, the intellectual property rights of that avatar's controller can certainly be.

64 This is grounded in the principle that the user will be liable provided the usual requisites are met. It also suggests that only some minimal nuances are necessary to conduct an analysis of non-contractual civil law claims for damages caused through an avatar, where such claims are brought under a fault-based liability regime. This is also true for instances when an avatar is run by an AI-system that can be manipulative or exploitative of others, leading to significant harm; arguably some nuances are necessary to address the issue under Union or national rules.

65 For instance, wrongdoing that causes harm is deemed relevant only if the harm extends beyond physicality in a digital environment. In these cases, fault-based civil liability remains adequate for addressing avatar misconduct. The standard of the duty of care closely resembling that of a real-world individual's behaviour when an avatar is controlled by a user, but can be assessed otherwise if the avatar is controlled by an AI-agent. Additionally, difficulties that arise, e.g., in proving the causation link, do not inherently result from avatar misconduct, but from the wider context of Metaverse technologies, which also entail the use of AI technology. As such, existing legal frameworks can address these challenges without requiring entirely new principles.

66 Without prejudice to the above, and bearing in mind the inevitable advance of technology, we may soon need to consider appropriate legal consequences for harmful occurrences that take place entirely in the interoperable, persistent digital realm and are not covered by current legislation. This could comprise the infringement of the right to an avatar's own image caused by another avatar or the protection of a trademark created by an avatar in the Metaverse without a physical world counterpart –should we reach a point in which this is possible, and they are granted legal personhood. More advanced avatars acting independently may be held directly at fault themselves, whereas less autonomous avatars merely mirroring user inputs may shift more fault to the human operator. Nevertheless, it is necessary to ground these highly hypothetical remarks in our current reality, where one can assert that such considerations only prompt a speculative exercise.

A Medley of Public and Private Power in DSA Content Moderation for Harmful but Legal Content: An Account of Transparency, Accountability and Redress Challenges

by **Andrea Palumbo** *

Abstract: This paper analyses the challenges associated with the co-regulatory arrangement of Articles 34 and 35 of the Digital Services Act (DSA) for the mitigation of the risks posed by harmful but legal content. Filling a gap in the existing literature, this paper focuses on the implications of the public-private cogeneration of content moderation policies for harmful but legal content resulting from the implementation of the DSA. This paper highlights three challenges deriving from the "hybrid" public-private governance of harmful speech in the context of the DSA. First, the potential lack of transparency on public influence over private content moderation policies. Second, the risks of unaccountability of public bodies who are able to steer private content moderation policies to pursue public policy objectives. Third, the lack of effective redress available to users against interferences with their legal speech. Building on these considerations, this paper puts forward two main arguments. First, the governance model for online speech of the DSA poses challenges that are not addressed by the current legislative framework. Second, the public-private dichotomy of EU fundamental rights law is not fit for purpose in the face of hybrid regulatory models. Based on the identified challenges, the paper discusses the main shortcomings of the legislative framework, with the aim to define a path for future research.

Keywords: Digital Services Act, Content Moderation, Systemic Risks, Harmful Content, Freedom of Expression

Recommended citation: Andrea Palumbo, A Medley of Public and Private Power in DSA Content Moderation for Harmful but Legal Content: An Account of Transparency, Accountability and Redress Challenges, 15 (2024) JIPITEC 246 para 1

A. INTRODUCTION

1 The Digital Services Act ("DSA")[1] started to apply in its entirety on 17 February 2024. The DSA is widely regarded as a paradigm shift for the governance of online content, whose consequences for the dissemination of online content are yet to be fully understood. As the E-Commerce Directive, the DSA lays down rules for providers of mere conduit, caching and hosting services, which are grouped under the umbrella category of "intermediary services".

2 By introducing new due diligence obligations for the providers of these services, the DSA moves from the model of *ex post* intermediary liability into the realm of both *ex ante* and *ex post* regulation.[2] Especially for providers of online platforms,[3] this paradigm

* Andrea Palumbo is Research Associate, Centre for IT & IP Law (CiTiP), KU Leuven.

1 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L277/1.

2 Miriam C. Buiten, 'The Digital Services Act: From Intermediary Liability to Platform Regulation' (2021) JIPITEC 361.

3 According to Article 3(i) of the DSA, an online platform is a "*hosting service that, at the request of a recipient of the service, stores and disseminates information to the public, unless that activity is a minor and purely ancillary feature of another service*

shift sees providers of intermediary services as more active, accountable and responsible actors in supervising the operation of their services and mitigating the risks they pose to fundamental rights, consumer protection and other societal and public interests.

3 In addition to entrusting new responsibilities to online intermediaries, the DSA imposes procedural obligations.[4]

4 The role given to procedural safeguards and fundamental rights in the DSA can be seen as a response that incorporates the dictates of digital constitutionalism.[5] Digital constitutionalism scholars have discussed the need to have in place solutions based on the rule of law to the challenges posed by the private ordering of online intermediaries,[6] and of online platforms.

5 The shift to platform regulation introduced by the DSA is clearest in relation to two categories of providers that, due to the heightened societal risks that may be caused by their services, are also subject to the highest standards of due diligence obligations. These are the providers of very large online platforms (''VLOPs'') and of very large online search engines (''VLOSEs'').

6 The due diligence obligations that Articles 34 and 35 of the DSA impose on VLOPs and VLOSEs are at the core of this paper. These Articles introduce risk assessment and mitigation obligations as well as a new mechanism of supervised regulation of online content. This new mechanism presents new questions and challenges that are investigated in the remainder of this paper.

7 Articles 34 and 35 DSA set up a new systemic risk mitigation system, in some respects translating a regulatory setting already tested in the field of the prudential supervision of financial institutions. While risk-based approaches are not new to EU digital regulation, systemic risk assessment and mitigation applied in relation to societal risks caused by technological design was an absolute novelty in EU legislation at the time of adoption of the DSA.

8 The focus of the analysis put forward in this article is on the content moderation policies enacted, under the supervision of the European Commission, by VLOPs and VLOSEs to mitigate the risks posed by legal content. By looking at the structure of the regulatory set-up in Articles 34 and 35 DSA, this paper argues that there is a phenomenon of cogeneration of content moderation policies resulting from the interaction between public and private actors, mainly because of the regulatory dialogue between the European Commission, on the one hand, and VLOPs and VLOSEs, on the other hand.

9 Based on this observation, this article describes the challenges that the public-private hybrid nature of decision-making processes for the moderation of legal content poses for transparency, accountability and effective redress for users whose freedom of expression may be limited. For the purposes of this article, the relevant legal framework against which these challenges are evaluated is EU law, with reference where appropriate to the European Convention on Human Rights (hereinafter, the ''ECHR'').

10 Existing literature has discussed the issues that arise in relation to public-private hybrid governance models for online content moderation. Most of the existing

or a minor functionality of the principal service and, for objective and technical reasons, cannot be used without that other service, and the integration of the feature or functionality into the other service is not a means to circumvent the applicability of this Regulation".

4 These relate to content moderation decisions, and explicitly require providers to have regard for the fundamental rights of the recipients of their intermediary services. See Articles 17, 20 and 21 of the DSA.

5 See, among others: Nicolas Suzor, 'Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms' (2018) Social Media and Society 1; Edoardo Celeste, 'Digital Constitutionalism: A New Systematic Theorisation' (2019) International Review of Law, Computers & Technology 76; Giovanni de Gregorio, *Digital Constitutionalism in Europe: reframing rights & powers in the algorithmic society* (Cambridge University Press 2022); Oreste Pollicino, 'The quadrangular shape of the geometry of digital power(s) and the move towards a procedural digital constitutionalism' (2023) European Law Journal.

6 Joao Pedro Quintais, Naomi Appelman, Ronan Fahy, 'Using Terms and Conditions to apply Fundamental Rights to Content Moderation' (2023) German Law Journal 881, p. 907.

relevant literature precedes the DSA legislative proposal,[7] and discusses the issue in relation to the EU or national legal frameworks applicable, and the informal practices taking place, at the time. One contribution discusses the entanglements between public and private censorship across different legal frameworks, including the DSA.[8] These contributions generally discuss the phenomenon of public-private online content moderation. However, they do not address in detail how this phenomenon has been 'institutionalised' in the Digital Services Act, and which are the repercussions for the protection of users' freedom of expression when harmful but legal content is moderated under Articles 34 and 35 of the DSA. Therefore, this article intends to build on existing literature and further develop it by providing two novel contributions: i) an analysis of the public-private cogeneration of content moderation policies for harmful but legal content under the systemic risk assessment and mitigation regime of the DSA, and ii) an assessment of whether this regime poses risks for the effective protection of users' freedom of expression. The assessment in ii) is based on the evaluative criteria of transparency and accountability, defined in light of the legality principle of the Charter[9] for fundamental rights' limitations, and effective redress.

7 Michael D. Birnhack, Niva Elkin-Koren, 'The Invisible Handshake: The Reemergence of the State in the Digital Environment' (2003) Virginia Journal of Law and Technology 8(6); Derek E. Bambauer, 'Against Jawboning' (2015) Minnesota Law Review 182; Christopher T. Marsden, *Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace* (Cambridge University Press, 2011); Chris Marsden, Trisha Meyer, Ian Brown, 'Platform values and democratic elections: How can the law regulate digital disinformation?' (2020) Computer Law & Security Review 36 105373; Daphne Keller, 'Who Do You Sue? State and Platform Hybrid Power Over Online Speech' (2019) Hoover Institution, Aegis Series Paper No. 1902; Paddy Leerssen 'Cut Out By The Middle Man: The Free Speech Implications Of Social Network Blocking and Banning In The EU' (2015) JIPITEC 6(2) 99.

8 Rachel Griffin, 'The Politics of Algorithmic Censorship: Automated Moderation and its Regulation', in James Garratt, Music and the Politics of Censorship: From the Fascist Era to the Digital Age, Brepols.

9 Article 52 Charter of Fundamental Rights of the European Union [2012] OJ C 364/01.

11 The novelty of this article lies both in the specific focus on the DSA and in the evaluative framework adopted. It aims to answer the following research question: does the systemic risk assessment and mitigation regime of the DSA pose risks to the effective protection of users' freedom of expression about their harmful but legal content, in light of the evaluative criteria of transparency, accountability and availability of redress channels? The analysis is developed in different stages. Section 2 outlines the main features of the regime for systemic risk assessment and mitigation laid down in the DSA. This constitutes the starting point of the discussion, which is developed with a description in Section 3 of the regulatory dialogue and interaction between the Commission and supervised intermediaries that this regime entails. Section 4 discusses whether this dialogue would include some form of public interference with the freedom of expression of online users. Section 5 sets out the key passages of this contribution, discussing the challenges posed by the public-private cogeneration of content moderation policies for online harmful content in relation to transparency and accountability of public action, and to the redress mechanisms against interferences with harmful but legal content. Finally, Section 6 reflects upon the challenges of the hybrid speech governance model of the DSA, discussing potential solutions.

B. Mitigation of Systemetic Risks in the DSA: Articles 34 and 35

I. The Regime for Systemic Risk Assessment and Mitigation in the DSA

12 Articles 34 and 35 DSA feature a scheme for systemic risk assessment and mitigation which, on the one hand, give obliged entities wide discretion in assessing risks and designing measures to address them and, on the other hand, provides for mechanisms of continuous supervision and evaluation over the conduct of such entities.

13 Article 34 DSA requires VLOPs and VLOSEs to identify and assess the systemic risks arising in the Union

from the design, functioning and use of their services and related systems, carrying out risk assessments at least once a year.[10] Based on the systemic risks thus identified, VLOPs and VLOSEs shall put in place risk mitigation measures pursuant to Article 35 DSA.

14 The DSA provides for an articulate system of supervision over the conduct of VLOPs and VLOSEs. The European Commission is entrusted with the role of supervising the assessment and mitigation of systemic risks by VLOPs and VLOSEs, with pervasive supervisory and enforcement powers

15 The model embraced in the DSA combines the conferral of significant discretion to regulated entities with continuous supervision from a public body. It has been referred to as co-regulation[11] and meta-regulation.[12] The DSA is not the first piece of legislation to put in place a co-regulatory model, but it presents innovative features in relation to content moderation. Recital 104 of the DSA explicitly states that self and co-regulatory agreements, such as codes of practice, should be pursued to design risk mitigation measures, and the explanatory memorandum accompanying the legislative proposal of the DSA mentions the creation of a co-regulatory backstop in relation to the due diligence obligations for VLOPs and VLOSEs.[13]

16 It is beyond the scope of this paper to attribute a specific terminology to the regulatory approach of the DSA for VLOPs and VLOSEs. It suffices to note that the mixed public-private participation in the definition of rules governing the circulation of online content has been highlighted under different conceptualisations.

17 The *fil rouge* of such conceptualisations lies in the fact that, under the DSA, VLOPs and VLOSEs are under the responsibility to put in place self-regulatory measures to manage risks, whether in the form of implementing codes of conduct or other risk mitigation measures, while being under the supervision of another regulator that has the enforcement powers necessary to guide their conduct where appropriate.

II. Providers of Very Large Online Platforms and Search Engines as Risk Regulators for Online Content

18 In the regulatory scheme of the DSA for the mitigation of risks posed by the dissemination of illegal and harmful content, VLOPs and VLOSEs are attributed the role of risk regulators.[14] They are subject primarily to the oversight and enforcement by the European Commission, but also by the national Digital Services Coordinators (''DSCs'') and the European Board for Digital Services to a more limited extent.

19 Under Articles 34 and 35 DSA, VLOPs and VLOSEs have significant discretion in both phases of the systemic risk mitigation process, i.e. risk identification and mitigation. In particular, in recognition of their better-placed position to understand systemic risks and how to mitigate them, VLOPs and VLOSEs are the

10 The systemic risks to be assessed are not exhaustively determined *ex ante* in the DSA. Article 34 only provides a list of systemic risks that shall be assessed in any case, without precluding the identification of additional risks where appropriate.

11 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, p. 3; Joan Barata, Oliver Budzinski, Mark Cole, Alexandre de Streel, Michèle Ledger, Tarlach McGonagle, Katie Pentney, Eleonora Rosati, 'Unravelling the Digital Services Act package' (2021), IRIS Special, European Audiovisual Observatory, Strasbourg, pp. 53, 54, 129; David Morar, ''The Digital Services Act's lesson for U.S. policymakers: Co-regulatory mechanisms'' [2022] Commentary published on the Brookings website, <https://www.brookings.edu/articles/the-digital-services-acts-lesson-for-u-s-policymakers-co-regulatory-mechanisms/> accessed 20 March 2024.

12 Nicolo Zingales, ''The DSA as a paradigm shift for online intermediaries' due diligence: hail to meta-regulation'', in Joris van Hoboken, João Pedro Quintais, Naomi Appelman, Ronan Fahy, Ilaria Buri, Marlene Straub (eds), ''Putting the Digital Services Act Into Practice: Enforcement, Access to Justice, and Global Implications'' (2023) Amsterdam Law School Research Paper No. 13, 2023, Institute for Information Law Research Paper No. 03, 2023.

13 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, p. 3.

14 Nicolo Zingales (n 12) p. 216.

entities who bear primary responsibility for systemic risk identification and mitigation.

20 The risk-based approach provides a first legally binding tool to address the risks and harms of lawful but harmful content. VLOPs and VLOSEs must look both inward and outward, to identify and mitigate systemic risks caused not only by illegal content but also by other content.

21 In their role as risk regulators, VLOPs and VLOSEs may be called to take risk mitigation measures that have important consequences for freedom of expression. Article 35 of the DSA does not require, *per se*, to prohibit or restrict the dissemination of a specific category of content uploaded by recipients of the service, as the scope of its obligation is only the mitigation of any systemic risk identified pursuant to Article 34 of the DSA.

22 However, taking into account the rationale and the nature of the obligation in Article 35, its implementation can be expected to lead to content moderation policies that restrict speech protected by the right to freedom of expression. Besides the category of illegal content, Article 35 is aimed at addressing the risks posed by ''harmful'' content.

23 Harmful content is not defined in the DSA and is not a legal concept of EU law. It is a term widely used in policy discussions around platform regulation to indicate content that can create harm to a series of public and private protected interests, such as public security, public health, civic discourse and the physical and mental well-being of natural persons. A prominent example of content that may be legal but harmful is disinformation.

24 While the EU legislator purposefully avoided to define harmful content in the DSA, the connection between the systemic risk mitigation framework of the latter and the objective to regulate the dissemination of harmful content is evident.[15] This is clear from the recitals of the DSA that make reference to disinformation as information that may generate systemic risks[16] and, more generally, to content that may cause harm.[17]

25 In relation to harmful content, the DSA aims to address, *inter alia*, amplification-based harm that is caused when content is disseminated in a way that materialises a given level of systemic risks. The materialisation of systemic risks is the condition that triggers the application of Article 35 and, consequently, may justify the imposition of restrictions on harmful content.

26 The risk-based approach adopted by the EU legislator in the DSA, and the newly assumed role of risk regulators of certain providers of intermediary services, are a novelty in EU law that have been subject to criticism, especially for the risks they engender to freedom of expression. Concerns have been voiced in multiple respects.

27 First, the wording used by DSA provisions in describing the scope of application of Articles 34 and 35 of the DSA has been described as too vague. There has been criticism in relation to key terms such as ''systemic risks'', ''reasonable'' and ''proportionate'',[18] with potential deficiencies in meeting the legality test for the restriction of fundamental rights, in particular as concerns the foreseeability of future restrictions for online users.[19] As users must be able to foresee how their speech might be restricted to mitigate systemic risks, the wording of DSA provisions must satisfy minimum standards of clarity as to when content is deemed unacceptable and how it may be restricted.

15 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, p. 3.

16 See recitals 9, 83, 84 and 104 of the DSA.

17 See recitals 5, 63, 69, 79, 104, 137 and 140 of the DSA.

18 Article 19, ''ARTICLE 19 recommendations for the Digital Services Act Trilogue'' (Article 19 website 2022) <EU: ARTICLE 19's recommendations for the Digital Services Act trilogue - ARTICLE 19> accessed 11 March 2024, pp. 2-3; Joan Barata, ''The Digital Services Act and its impact on the right to freedom of expression: special focus on risk mitigation obligations'' (2021) publication on *Plataforma en Defensa de la Libertad de Información* (PDLI), pp. 19 – 21; Joan Barata et al. (n 11) pp. 16-18.

19 Article 19, ''ARTICLE 19 recommendations for the Digital Services Act Trilogue'' (Article 19 website 2022) <EU: ARTICLE 19's recommendations for the Digital Services Act trilogue - ARTICLE 19> accessed 11 March 2024, pp. 2-3.

28 Second, the bestowal of regulatory functions, with wide discretion, to VLOPs and VLOSEs for the delicate task of moderating harmful but legal content has been criticised by the Committee on Civil Liberties, Justice and Home Affairs of the European Parliament as posing significant risks to freedom of expression. For this reason, during the legislative procedure for the adoption of the DSA the Committee proposed an amendment to delete the risk management framework.[20]

III. Article 35 of the DSA as Conducive to Restrictions on the Dissemination of Legal Content

29 The adoption of risk mitigation measures under Article 35 may lead to new types of interferences with freedom of expression targeting content that is legal and that is not restricted under any other legal basis than Article 35 itself. For illegal content, the boundaries of free speech have already been defined by national legislation or other legally binding acts, and the nature and scope of the restriction is clear as illegal content is plainly not acceptable.

30 Legal content whose dissemination generates systemic risks may instead be restricted under the aegis of Article 35 for the sole reason that it is conducive to such risks. Risk mitigation measures to be adopted under Article 35 are an open category, with the consequence that they may include anything deemed appropriate by VLOPs and VLOSEs.

31 For example, the prohibition of content is already foreseen as a possible measure to address disinformation in the Code of Practice on Disinformation.[21] Adherence to the Code may in turn constitute an adequate risk mitigation measure within the meaning of Article 35.[22] Another example is the demotion of content deemed harmful, which would fall under one of the measures listed in Article 35 regarding the adaptation of algorithmic systems, including recommender systems[23], and is equally foreseen as an action under the Code to tackle disinformation.[24]

32 Guidelines and reports published by the Commission to date in relation to systemic risks and the implementation of the DSA clearly show that the regulatory expectations towards Article 35 envisage the restriction of legal but harmful content. The Guidelines of the Commission on the mitigation of systemic risks for electoral processes recommend as mitigation measures, *inter alia*, disrupting the algorithmic amplification and spread of viral harmful content,[25] demonetisation[26] and the measures already foreseen in the Code on disinformation.[27] Furthermore, the report by the Commission on the application of the DSA risk management framework to Russian disinformation suggests in multiple points that restriction of legal speech may be warranted, especially as concerns the imposition of bans and demotions on Kremlin-aligned accounts.[28]

20 The Committee stated that the DSA "*should address illegal content only and not "harmful content" as targeting legal content could put the freedom of expression at serious risk (i.e. annex to resolution 2020/2019(INL) as well as LIBE opinion PE650.375v02, par. 15), whereas the proposed Article 26 would go far beyond illegal content where mere vaguely described allegedly "negative effects" are concerned*". See: Draft Opinion of the Committee on Civil Liberties, Justice and Home Affairs for the Committee on the Internal Market and Consumer Protection on the proposal for a regulation of the European Parliament and of the Council Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (COM(2020)0825 – C9-0418/2020 – 2020/0361(COD), Amendment 91, pp. 63-65.

21 The Strengthened Code of Practice on Disinformation [2022] measure 18.2, p. 20.

22 Article 35(1)(h) of the DSA, and preamble j) of the Code which states that signing up to all the commitments of the Code should be considered as a possible risk mitigation measure under the DSA.

23 Article 35(1)(d) of the DSA.

24 The Strengthened Code of Practice on Disinformation of 2022, measures 18.1 and 18.2, p. 20.

25 Commission, 'Commission Guidelines for providers of Very Large Online Platforms and Very Large Online Search Engines on the mitigation of systemic risks for electoral processes pursuant to Article 35(3) of Regulation (EU) 2022/2065', C/2024/2537, Section 3.2.1.

26 Ibid, p. 8.

27 Ibid, p. 5.

28 Commission, 'Digital Services Act: Application of the Risk Management Framework to Russian disinformation campaigns', <https://op.europa.eu/en/publication-

33 VLOPs and VLOSEs have already been moderating legal content before the DSA started to apply, in many cases on a voluntary basis.[29] Moreover, a search on the statements of reasons in the transparency database shows that some VLOPs demoted legal speech deemed harmful for civic discourse or elections relying on fully automated means.[30]

34 Under the DSA, VLOPs and VLOSEs may mitigate systemic risks by actively moderating legal content, and will be allowed to take a more proactive stance over monitoring content under Article 7 of the DSA. Compliance with Article 34 and 35 may require a rather systematic monitoring of the content being disseminated online. This could take place using online tools such as the demotion mechanisms in the ''Explore'' recommender system of Instagram,[31] where items may be filtered out or downranked by automated means based on integrity-related scores.[32]

C. Cogeneration of Content Moderation Policies in the DSA: Interaction Between the Commission and Supervised Intermediaries

35 As the entities in the best position to control the flow of online content, VLOPs and VLOSEs have been assigned important responsibilities for *ex ante* and *ex post* moderation of speech. The biggest change can be noted with regard to legal but harmful content, as for illegal content this was already the case before the DSA.[33]

36 When VLOPs and VLOSEs will continue to moderate legal content in compliance with Articles 34 and 35 of the DSA, the measures taken to this end cannot be deemed as merely private content moderation policies under their exclusive responsibility.[34] On the contrary, public authorities have the means and the duty to influence content moderation policies of obliged entities on a regular basis, where appropriate.

37 Thus, this article argues that the systemic risk mitigation framework of the DSA has set up a mechanism for the co-generation of the legal and technological rules that govern content moderation of online content, including legal content. On a legal level, cogeneration processes influence the terms and conditions on which VLOPs and VLOSEs rely as the contractual basis to restrict the content uploaded by service recipients. On a technological level, public actors can participate in shaping the algorithms governing the dissemination of online content by setting certain regulatory expectations on the implementation of Articles 34 and 35 of the DSA.

38 The public-private cogeneration of norms governing content moderation is a trend that has already emerged in recent years on an international level.[35]

detail/-/publication/c1d645d0-42f5-11ee-a8b8-01aa75ed71a1/language-en> accessed on 2 February 2024, pp. 45-46.

29 See the dashboard of the DSA transparency database, accessed at https://transparency.dsa.ec.europa.eu/dashboard on 2 February 2024.

30 See the results available at the following search on the DSA transparency database of the Commission: https://transparency.dsa.ec.europa.eu/statement?automated_decision%5B0%5D=AUTOMATED_DECISION_FULLY&category%5B0%5D=STATEMENT_CATEGORY_NEGATIVE_EFFECTS_ON_CIVIC_DISCOURSE_OR_ELECTIONS&platform_id%5B0%5D=36&platform_id%5B10%5D=31&platform_id%5B11%5D=34&platform_id%5B12%5D=30&platform_id%5B13%5D=22&platform_id%5B14%5D=27&platform_id%5B15%5D=29&platform_id%5B1%5D=28&platform_id%5B2%5D=23&platform_id%5B3%5D=37&platform_id%5B4%5D=32&platform_id%5B5%5D=24&platform_id%5B6%5D=25&platform_id%5B7%5D=26&platform_id%5B8%5D=33&platform_id%5B9%5D=35&page=19, accessed on 5 February 2024.

31 See the information available at the following link: https://engineering.fb.com/2023/08/09/ml-applications/scaling-instagram-explore-recommendations-system/, accessed on 6 February 2024.

32 For more information about how Meta uses AI to rank harmful content, see: https://ai.meta.com/blog/harmful-content-can-evolve-quickly-our-new-ai-system-adapts-to-tackle-it/, accessed on 6 February 2024.

33 Marco Bassini, 'Fundamental Rights and Private Enforcement in the Digital Age' (2019) European Law Journal 182.

34 Joan Barataet et al (n 11) p. 21.

35 Michael D. Birnhack, Niva Elkin-Koren (n 7); Derek E.

In the EU, it has been discussed more in detail in relation to the moderation of terrorist content,[36] under Regulation (EU) 2021/784.[37] Moreover, also the EU Code of Conduct on countering illegal hate speech online[38] introduced a collaboration between public and private entities for the moderation of illegal speech. This article aims to analyse this phenomenon with specific regard to the cogeneration of content moderation policies for content that is legal but can be restricted due to the systemic risks it poses. This scope of analysis thus warrants different considerations from content moderation policies that restrict content which is illegal under another national or EU law.

39 Private content moderation policies can be influenced by the European Commission and DSCs both *ex ante* and *ex post* under the DSA. The European Commission has exclusive competence to enforce the provisions on systemic risk assessment and mitigation for VLOPs and VLOSEs, while the competence is shared with the DSCs for enforcing compliance with the majority of the DSA provisions in relation to VLOPs and VLOSEs.

40 Articles 34 and 35 already define *ex ante* the basic rules governing content moderation for the purposes of mitigating systemic risks. They indicate how systemic risks must be assessed and lay down the high-level principles that should be respected when adopting mitigation measures, i.e. reasonableness, proportionality, effectiveness and consideration of the impact to fundamental rights.

41 However, due to the vagueness of the DSA provisions on systemic risk assessment and mitigation, the more concrete, and possibly consequential, *ex ante* guidance on how to implement them is likely to be provided by guidelines from, and dialogue with, the regulators.

42 First, the Commission, in cooperation with DSCs, can issue guidelines that provide more detail on how VLOPs and VLOSEs should mitigate systemic risks.[39] The first guidelines drafted under this legal basis have already been published, and they provide detailed guidance on how risks to electoral processes should be assessed and mitigated.[40]

43 Second, the Commission can invite VLOPs and VLOSEs to draw up codes of conduct on how to mitigate specific systemic risks.[41] The implementation of these codes can in turn qualify as a risk mitigation measure compliant with Article 35 of the DSA. The Commission has the means under the DSA to significantly influence the content of codes of

Bambauer (n 7); Christopher T. (n 7); Paddy Leerssen (n 7); Kylie Langvardt, 'Regulating Online Content Moderation' [2017] Georgetown Law Journal 1353; Daphne Keller (n 7); Julie E. Cohen, *Between Truth and Power* (Oxford University Press, 2019); Chris Marsden, Trisha Meyer, Ian Brown (n 7); Evelyn Douek, 'The Rise of Content Cartels' (publication on the website Knight First Amendment Institute at Columbia University, 2020) <The Rise of Content Cartels | Knight First Amendment Institute (knightcolumbia.org)> accessed on 7 February 2024.

36 Rocco Bellanova, Marieke de Goede, 'Co-Producing Security: Platform Content Moderation and European Security Integration' (2022) Journal of Common Market Studies 1316.

37 Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online (Text with EEA relevance) (2021) OJ L 172/79.

38 Code of conduct on countering illegal hate speech online (2019).

39 Article 35(3) reads as follows: ''*the Commission, in cooperation with the Digital Services Coordinators, may issue guidelines on the application of paragraph 1 in relation to specific risks, in particular to present best practices and recommend possible measures, having due regard to the possible consequences of the measures on fundamental rights enshrined in the Charter of all parties involved. When preparing those guidelines the Commission shall organise public consultations*".

40 Commission, 'Commission Guidelines for providers of Very Large Online Platforms and Very Large Online Search Engines on the mitigation of systemic risks for electoral processes pursuant to Article 35(3) of Regulation (EU) 2022/2065', C/2024/2537, Section 3.2.1.

41 Article 45(2) of the DSA reads as follows: ''*where significant systemic risk within the meaning of Article 34(1) emerge and concern several very large online platforms or very large online search engines, the Commission may invite the providers of very large online platforms concerned or the providers of very large online search engines concerned, and other providers of very large online platforms, of very large online search engines, of online platforms and of other intermediary services, as appropriate, as well as relevant competent authorities, civil society organisations and other relevant stakeholders, to participate in the drawing up of codes of conduct, including by setting out commitments to take specific risk mitigation measures, as well as a regular reporting framework on any measures taken and their outcomes.*"

conduct, not only by encouraging their drawing up but also by monitoring how they are drafted[42] and how they are implemented.[43] In concrete terms, codes of conduct can become a set of rules implementing the DSA.

44 Third, the Commission may rely on Article 72(1) of the DSA to establish regular dialogue with VLOPs and VLOSEs on the mitigation of systemic risks.[44] In the context of this dialogue, the Commission can communicate regulatory expectations that may shape *ex ante* the measures to be adopted under Article 35.

45 Finally, the Commission and DSCs can influence the content and structure of terms and conditions in the context of their supervision over compliance by VLOPs and VLOSEs with Article 14 of the DSA, setting specific expectations on, for instance, clarity of the language and respect of fundamental rights.

46 *Ex post* intervention can take place thanks to the enforcement powers of public bodies that shape and constrain how VLOPs and VLOSEs deal with systemic risks.[45] Under Section 4 of Chapter IV of the DSA, the Commission has direct investigatory and enforcement powers over compliance of VLOPs and VLOSEs with the DSA. To this end, the Commission has a wide array of investigatory and enforcement powers at its disposal ranging from requests for information to inspections, interim measures, decisions of non-compliance and the imposition of fines.

47 Moreover, similarly to what is mentioned above regarding *ex ante* measures, Article 72(1) of the DSA can be relied on to have regular dialogue with supervised entities in order to correct and guide *ex post* their risk mitigation activities.

48 All of the enablers for *ex ante* and *ex post* intervention described above draw a picture of intricate relationships between EU public policy and private ordering of supervised entities. Public interference can affect the contractual freedom of private entities, as concerns the content of terms and conditions, as well as the freedom to structure the technological design of intermediary services. Contrary to other more subtle forms of government interference over content moderation induced through political or public opinion pressures,[46] the connection between private content moderation and public policy is made explicit in the DSA and stems from a legal requirement. While content moderation policies are ultimately determined by VLOPs and VLOSEs, lack of compliance with regulatory demands from the Commission or DSCs could lead to a decision of non-compliance and a fine. The enforcement activities of the Commission in the last year provide evidence of how subtly regulatory demands can be communicated to VLOPs and VLOSEs without the adoption of a formal decision. For example, in a letter dated 12 August 2024, former Commissioner Thierry Breton warned X owner Elon Musk about the dissemination of harmful content on X, with a specific mention of the upcoming live conversation with a US presidential candidate.[47] This shows that the *ex ante* and *ex post* avenues for intervention could also empower the Commission to put in place jawboning practices.

42 See Article 45(3) of the DSA.

43 See Article 45(4) of the DSA.

44 Article 72(1) of the DSA reads as follows: ''*for the purposes of carrying out the tasks assigned to it under this Section, the Commission may take the necessary actions to monitor the effective implementation and compliance with this Regulation by providers of the very large online platform and of the very large online search engines. The Commission may order them to provide access to, and explanations relating to, its databases and algorithms. Such actions may include, imposing an obligation on the provider of the very large online platform or of the very large online search engine to retain all documents deemed to be necessary to assess the implementation of and compliance with the obligations under this Regulation.*"

45 Joan Barata (n 11).

46 Niva Elkin-Koren, 'Government–Platform Synergy and its Perils' in Edoardo Celeste, Amelie Heldt, Clara Iglesias Keller (eds) *Constitutionalising Social Media* (Oxford: Hart Publishing, 2022), pp. 177–198.

47 The letter has been published by the X account of former Commissioner Thierry Breton on 12 August 2024. See: Thierry Breton on X: "With great audience comes greater responsibility #DSA As there is a risk of amplification of potentially harmful content in EU in connection with events with major audience around the world, I sent this letter to @elonmusk https://t.co/P1IgxdPLzn" / X.

49 The existence of legal obligations and a co-regulatory setting of dialogue with, and enforcement by, the Commission enables public policy considerations to affect private content moderation practice to a level that, before the DSA, was unprecedented in EU law. The extent to which public policy considerations seep into terms and conditions and technological design cannot be gauged from a reading of Article 35 of the DSA alone.

50 Obligations for systemic risk assessment and mitigation are defined in vague terms, and the concrete relationship between EU public policy and private ordering will become clearer only in the future when the Commission has consolidated its supervisory and enforcement practices. The Commission might issue detailed guidelines and encourage the drawing up of codes of practice to set out how harmful content should be moderated or have continuous dialogue with supervised entities indicating in a more informal manner which conducts are recommended.

51 After having described the setting that leads to the cogeneration of content moderation policies, a central aspect of this article is understanding the consequences of such setting for any restriction to harmful content. For illegal content, the nature of the restriction to free speech is clearly set out in the EU or national law that qualifies the content as illegal.

52 The nature and scope of the interference would result directly from the relevant legal provisions and their interpretation. The underlying constitutional calculus that justifies the illegality of certain speech has been made and rendered explicit by the authority that adopted such provisions, which in most cases would be the EU or national legislature. For instance, the terrorist content to be restricted under the Terrorist Content Regulation is clearly linked to the offences regulated by Directive 2017/541,[48] and many forms of hate speech are prohibited pursuant to the Council Framework Decision 2008/913/JHA.[49] In both of these examples the relevant constitutional calculus for the prohibition of certain categories of content has been made by the EU legislature.

53 For the restrictions to harmful content that may result from Article 35, the way the constitutional calculus takes place is more intricate and complex. Harmful and legal content is not prohibited as such by the DSA. For example, in the case of disinformation a single piece of false or misleading information is not per se the object of any legally-mandated restriction. However, if disseminated in a given manner and context that generates systemic risks of the type under the scope of Article 34 of the DSA, VLOPs and VLOSEs would be under an obligation to take mitigation measures that address this content, which may in turn involve measures that restrict its dissemination.

54 The manner and context of dissemination acquire central importance, as the same content may or may not have to be restricted depending on these factors. The example of amplification-based harm is instrumental in understanding the types of restrictions that may stem from Article 35 DSA. Certain content may become harmful only when amplified to a given extent that generates systemic risks, such as disinformation on health matters that may cause a public health crisis. The amplification-based harm caused by legal content is the element that may shift the constitutional calculus and induce the legislator to introduce an interference with freedom of expression.[50] This is the approach taken by the risk mitigation framework of the DSA, which only lays down the general principles governing risk assessment and mitigation without explicitly requiring restrictions to any category of content.

48 Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA [2017] OJ L 88/6.

49 Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law [2008] OJ L 328/55.

50 Daphne Keller, 'Amplification and its discontents: why regulating the reach of online content is hard' (Knight First Amendment Institute at Columbia University, section on essays and scholarship, 2021), <https://knightcolumbia.org/content/amplification-and-its-discontents> accessed on 3 March 2024.

55 The identification and mitigation of systemic risks becomes a crucial moment for the constitutional calculus under which an interference with freedom of expression is justified. Risk acts as a proxy for the balancing of conflicting constitutional interests:[51] the freedom of expression of users, public interests harmed by systemic risks, and the freedom to conduct a business of private entities. Therefore, to understand the role of cogeneration in shaping content moderation policies for legal content, it is essential to look at the decision-making process on the identification and mitigation of systemic risks. This process should be looked at taking into account the primary responsibility of VLOPs and VLOSEs in deciding how to assess and mitigate risks, but also the role of the Commission as meta-regulator to guide *ex ante*, and correct *ex post*, the actions of VLOPs and VLOSEs. This adds another venue of cogeneration besides content moderation policies, and it relates to the upstream task of systemic risk identification and mitigation.

56 Under the DSA, the Commission has a series of tools at its disposal to influence *ex ante* and *ex post* assessments of VLOPs and VLOSEs. In this context, Article 72 can be relied on to shape private assessments *ex ante*, whereas the investigatory and enforcement powers described above in relation to risk mitigation are equally used by the Commission to control *ex post* how systemic risks are identified and assessed.

57 Such intervention takes place *ex ante*, via the rules included in the DSA. It also takes place *ex post*, due to the capacity of the European Commission to shape and constrain the different ways platforms deal with systemic risks, which entail the dissemination of and access to far more types of content than merely illegal information.

58 Overall, a picture can be drawn where public and private actors cogenerate policies for the moderation of legal but harmful content. This cogeneration involves aspects of crucial constitutional relevance, notably the identification of the level of risk that may justify a restriction to freedom of expression and the determination of the nature and scope of such restriction.

59 As it determines the scope of the limitation on freedom of expression, the interplay between public influence and private ordering has important consequences for the freedom of expression of millions of recipients of VLOPs and VLOSEs' services. This interplay creates a new dimension of power and interference which may be difficult to categorise under traditional constitutional concepts. Thus, it creates new theoretical and practical challenges for the protection of the freedom of expression of users, as is discussed below.

D. Public Interferences with Freedom of Expression under the DSA: Article 35 and Public Supervision over Private Ordering

60 The rights recognised by the Charter of Fundamental Rights of the European Union are binding on the EU institutions and the Member States when they implement EU law, as provided for in its Article 51.[52] Whether the Charter can impose horizontal direct effects on individuals is an issue that has been settled in EU case-law in relation to certain rights,[53] but remains open as concerns other rights including freedom of expression.[54] Therefore, the most common and clear application of the Charter is as standard of review of public actions. For the Charter to be invoked against a public action, this action must qualify as a public interference with a fundamental right protected by the Charter.

51 Giovanni De Gregorio, Pietro Dunn, 'The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age' (2022) Common Market Law Review, pp. 17-18.

52 Article 51 of the Charter reads as follows: *''the provisions of this Charter are addressed to the institutions and bodies of the Union with due regard for the principle of subsidiarity and to the Member States only when they are implementing Union law. They shall therefore respect the rights, observe the principles and promote the application thereof in accordance with their respective powers."*

53 ECJ Case C-414/16 *Vera Egenberger v Evangelisches Werk für Diakonie und Entwicklung eV* [2018] EU:C:2018:257; ECJ Case C-569/16 *Stadt Wuppertal v Maria Elisabeth Bauer and Volker Willmeroth v Martina Broßonn* [2018] ECLI:EU:C:2018:871.

54 Paul Craig, Grainne de Búrca, *EU Law: Text, Cases, and Materials* (seventh edition, Oxford University Press, 2020), pp. 450-454.

61 The public influence on private content moderation policies raises the question of whether a risk mitigation measure taken under Article 35 of the DSA can qualify as a public interference under the Charter. To answer this question, it is necessary to look at the entire co-regulatory setting for systemic risk mitigation of the DSA, with the different layers of legislative norms, supervisory and enforcement actions and private conduct.

62 The case-law of the ECJ and of the European Court of Human Rights (ECtHR) offers a rather clear picture of what can constitute an interference with freedom of expression. The ECtHR has developed a broad interpretation of what could constitute an interference, including a large array of measures such as formalities, conditions, restrictions or penalties.[55] On the internet, restrictions on the means of dissemination are interferences with freedom of expression as much as restrictions on content per se,[56] especially when they target online content-sharing platforms that play a vital role for the dissemination of information.[57]

63 Therefore, restrictions that affect recommender systems and the algorithmic reach of online content may qualify as an interference with freedom of expression. According to the case-law of the ECtHR, an interference does not need to result from a legally binding act. It may also stem from other actions of a public authority which have the effect of restricting the enjoyment of freedom of expression, potentially also in the form of chilling effects.

64 The case-law of the ECJ sheds light on forms of public interference where the restriction to free speech stems indirectly from public action, even in the absence of a direct prohibition of a given content. The reasoning followed by the ECJ in Poland v EP and Council[58] shows that a provision can qualify as an interference with freedom of expression even if it does not directly prohibit content nor explicitly requires intermediaries to restrict content. It suffices that the provision generates a situation that would lead intermediaries to restrict content to comply with it. In particular, the ECJ held that, since Article 17 of Directive 2019/790[59] ("DSM Directive") created a situation where intermediaries would need to deploy content filtering tools that may block *ex ante* legal content, the limitation resulting from these tools would be attributable to the EU legislature.[60]

65 This attribution flows from the fact that the limitation is a direct consequence of the specific liability regime established in respect of online content-sharing service providers in Article 17(4) of the DSM Directive. As a consequence, the ECJ concluded that the specific liability regime of Article 17(4) of the DSM Directive entails a limitation on the exercise of the right to freedom of expression and information of users guaranteed in Article 11 of the Charter.[61]

66 The principles described above on the meaning of public interference provide convincing arguments to claim that there is a public interference with freedom of expression when the application of Article 35 leads to the moderation of legal content. At the legislative level, Articles 34 and 35 provide the basis and the metrics to put in place such restrictions. Since legal but harmful content is not restricted under other laws that declare its illegality, the only criteria that determine its restriction are those stemming from the risk management regime of the DSA, i.e. the

55 *Wille v. Liechtenstein* App no 28396/95 (ECtHR 28 October 1999), para. 43.

56 *Autronic AG v. Switzerland* App No 12726/87, (ECtHR 22 May 1990), para. 47; *Murphy v. Ireland* App No 44179/98 (ECtHR, 10 July 2003), para. 61; *Ahmet Yildirim v. Turkey* App No 3111/10 (ECtHR 18 December 2012), para. 50; *Pirate Bay: Neij and Sunde Kolisoppi v Sweden* App No 40397/12 (ECtHR 18 February 2013); *Pendov v. Bulgaria* App No 44229/11, (ECtHR 12 October 2020), para. 53.

57 *Cengiz and Others v. Turkey* Applications nos. 48226/10 and 14027/11 (ECtHR 1 December 2015), para. 52; *Vladimir Kharitonov v. Russia* App No 10795/14 (ECtHR 23 June 2020), para. 33 and the case-law cited therein.

58 ECJ Case C-401/19 *Republic of Poland v. European Parliament and Council of the European Union* [2022] EU:C:2022:297.

59 Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC [2019] OJ L 130/92.

60 ECJ Case C-401/19 *Republic of Poland v. European Parliament and Council of the European Union* [2022] EU:C:2022:297, para. 56.

61 ibid para. 58.

capacity to create systemic risks. And while Article 35 does not directly restrict content, it establishes duties of care that oblige intermediaries to impose limitations on legal speech in certain circumstances. The limitation is indirect but directly attributable to the EU legislature, following the same logic of the ECJ in Poland v EP and Council.

67 At the supervisory and enforcement level, the Commission has the means to influence private policies interfering with freedom of expression in various ways. The Commission can contribute to the definition of content moderation policies by providing *ex ante* guidance and by correcting private actions *ex post*. The high-level and vague wording of Articles 34 and 35 of the DSA provide the basis and metrics to restrict harmful content, but the Commission can shape the rules that govern the moderation of legal content in practice. The actual decisions on which risks are acceptable, and which should be mitigated and how, is a result of the intricate relationship between public supervision/enforcement and private ordering. As discussed above, VLOPs and VLOSEs as risk regulators carry out a balancing exercise of fundamental importance together with the Commission.

68 In light of the above, there are elements to argue for the existence of a mediated public interference with freedom of expression. This interference would result from Article 35 of the DSA and, possibly, from the supervisory and enforcement action of the Commission. If this is the case, the Charter would apply. The existence of a public interference can therefore not be excluded solely for the fact that private entities are ultimately responsible for moderating content that generates systemic risks.

E. Transparency, Accountability and Redress for Public Interferences with Freedom of Expression

69 This article argues that the mix of private and public participation in the definition of content moderation policies for online legal but harmful content raises specific concerns for the effective protection of the freedom of expression of users. This conclusion is based on an assessment that relies on two evaluative criteria: i) transparency and accountability in relation to public interferences with freedom of expression, and ii) judicial redress channels available against such interferences. These two concerns are described below.

I. Transparency and Accountability of Public Interferences with Freedom of Expression under the DSA

70 Transparency and accountability are widely recognised as foundational principles of good governance, essential to build trust in public actors.[62] They are also guiding principles of pervasive importance for the actions of the European Commission,[63] and recognised pillars of the rule of law in EU legislation[64] and policy[65] and in the Council of Europe.[66] Transparent and accountable actions by

62 Michael Johnston, 'Good governance: Rule of law, transparency, and accountability' (United Nations Public Administration Network, 2006), <Good governance: rule of law, transparency, and accountability | IIEP Unesco - Etico | Platform on ethics and corruption in education> accessed 6 March 2024; European Parliament, 'Transparency, integrity and accountability in the EU institutions' (briefing for the PETI Committee, 2019) <Transparency, integrity and accountability in the EU institutions (europa.eu)> accessed on 10 January 2024, p. 1; Council of Europe, '12 principles of good democratic governance', (online brochure, 2019), <https://rm.coe.int/brochure-12-principles-of-good-governance-and-current-tools-on-good-go/16808b1687> accessed on 10 January 2024; Janos Bertok, 'Public Sector Transparency and Accountability: Making it Happen' (OECD/OAS, OECD publishing Paris, 2002).

63 Commission, ''Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Better regulation for better results - An EU agenda'', COM(2015)215 final.

64 According to Article 2(a) of Regulation 2020/2092, the 'rule of law' includes ''*the principles of legality implying a transparent, accountable, democratic and pluralistic law-making process*''.

65 Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 2020 Rule of Law Report, The rule of law situation in the European Union', COM(2020) 580 final.

66 European Commission for Democracy through Law (Venice Commission), 'Rule of law checklist' (publication of the

the EU public administration are also instrumental to enable citizens to effectively exercise their rights, by monitoring how they may be affected by public action.

71 The DSA provides for increased transparency about the activities of intermediary service providers and enhances their accountability vis-à-vis recipients of their services.[67] As concerns content moderation, the DSA represents a significant step forward towards transparency and accountability regarding the restrictions on content put in place by providers of intermediary services and the underlying reasons for such restrictions.[68]

72 The DSA provides for articulated transparency safeguards provided against private restrictions on content. However, there are no mechanisms to ensure that users can clearly distinguish between measures that are purely private and measures that providers are obliged to adopt to tackle systemic risks under the DSA. Ultimately, it seems that the DSA does not fare as well when it comes to providing for transparency and accountability over public intervention in the dissemination of information on online platforms and search engines. In particular, issues can be identified regarding the foreseeability of interferences with freedom of expression from the perspective of online users. Even though Article 35 does not create obligations for users, but only for platforms, it is the legal basis for interferences with freedom of expression that may be imposed on the harmful but legal content of users. Therefore, foreseeability should be looked at from the perspective of online users whose legal content may be restricted as a consequence of Article 35.[69] Foreseeability is an essential quality that any legal basis providing for an interference with fundamental rights should have,[70] in order to be compliant with the requirement under the Charter that such interference be 'provided for by law'.[71]

73 While the difficulty to distinguish private and public censorship in contemporary trends of content moderation has already been observed[72], the DSA creates new and more concerning challenges in relation to the moderation of legal but harmful content. Article 14(1) of the DSA does not require

Council of Europe, 2016).

67 The DSA has provisions on both *ex ante* and *ex post* transparency. The former is ensured by Article 14(1) of the DSA, according to which terms and conditions must inform users of any restrictions that may be imposed in relation to the use of an intermediary service, including information on how content moderation takes place for any content that is illegal or incompatible with terms and conditions. The same provision also lays down requirements over how this information should be communicated, i.e. that it be in clear, plain, intelligible, user-friendly and unambiguous language, publicly available in an easily accessible and machine-readable format. The latter is enabled by provisions on statements of reasons accompanying decisions that restrict online speech, by the obligation to publish reports with information on the content moderation activities that intermediaries engaged in, and by the obligation to make publicly available the specific mitigation measures put in place to address systemic risks.

68 Giancarlo Frosio, Christophe Geiger, 'Taking Fundamental Rights Seriously in the Digital Services Act's Platform Liability Regime' [2023] European Law Journal 31; Joao Pedro Quintais, Naomi Appelman, Ronan Fahy, 'Using Terms and Conditions to apply Fundamental Rights to Content Moderation' [2023] German Law Journal 881.

69 This is, in essence, the perspective adopted by the ECJ in assessing whether the liability regime in Article 17 of Directive 2019/790 imposes a limitation on the exercise of the right to freedom of expression and information that is compliant with the Charter. See: ECJ Case C-401/19 *Republic of Poland v. European Parliament and Council of the European Union* [2022] EU:C:2022:297.

70 European Union Agency for Fundamental Rights, 'Applying the Charter of Fundamental Rights of the European Union in law and policymaking at national level' [2020], pp. 71-72; ECJ Case C-401/19 *Republic of Poland v. European Parliament and Council of the European Union* [2022] EU:C:2022:297, para. 67; ECJ joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB and Secretary of State for the Home Department* [2016] EU:C:2016:970, para. 117; Opinion of Advocate General Cruz Villalón in ECJ Case C-70/10 *Scarlet Extended SA v SABAM* [2011] EU:C:2011:255, paras. 94-96. Opinion in ECJ Case C-401/19 *Poland v. Parliament and Council* [2022] ECLI:EU:C:2022:297, para 90.

71 According to Article 52(1) of the Charter, any interference with the enjoyment of the rights and freedoms recognised by the Charter must be 'provided for by law'. This requirement is also known as the legality principle, and is one of the conditions that must be met for an interference with a fundamental right to be compliant with the Charter.

72 Rachel Griffin, 'The Politics of Algorithmic Censorship: Automated Moderation and its Regulation', in James Garratt, *Music and the Politics of Censorship: From the Fascist Era to the Digital Age*, Brepols.

providers of intermediary services to inform users *ex ante* about which restrictions may apply specifically for the purposes of mitigating systemic risks under the DSA. Moreover, it does not require to indicate whether any specific measure applied has been required by the Commission through guidelines or informal supervisory requests. While this provision safeguards the foreseeability of the restrictions that may be imposed because of the contractual document governing the relationship with providers, i.e. terms and conditions, it does not ensure full transparency in relation to the restrictions that derive from an application of Article 35.

74 When reading terms and conditions, a user may not be able to distinguish between restrictions that result from the contractual freedom of providers or from demands of public policy. All interferences with content that is legal may be equally enforceable and justified as incompatible with terms and conditions. Therefore, any restriction with harmful content would fall under the same contractual ground and might, *prima facie*, appear as resulting from a decision solely of the service provider. Moreover, Article 17 on statements of reasons only obliges providers to indicate the contractual ground relied on for the restriction of legal content. It does not require an indication of whether the interference is a risk mitigation measure implemented in compliance with Article 35 of the DSA. While for illegal content the basis of the restriction would be clearly set out in law, and would have to be specifically indicated in statements of reasons, for legal content there is no transparency on the nature of the public interference behind private content moderation.

75 Not only is there no guarantee of transparency from VLOPs and VLOSEs on this point, but also the text of Article 35 is excessively vague to predict *ex ante* which content may be restricted for reasons of public policy due to the fact that it generates systemic risks,[73] as there is no clear criteria to determine when a risk becomes too risky.[74]

76 As discussed above, the public-private cogeneration of content moderation measures is the context where conflicting constitutional interests in relation to harmful but legal content are balanced. These reasons may not be made public, and the user may not have means to understand to which extent public policy considerations are behind what is and is not accepted on online fora.

77 The biggest promise for transparency may lie in Article 42(4)(b), according to which VLOPs and VLOSEs must make publicly available, at least once a year, the specific mitigation measures put in place pursuant to Article 35(1). However, the level of granularity in which information on mitigation measures is disclosed will be the key factor in effectively enabling users to be aware of which restrictions applied to them stem from such measures. Moreover, the requirement to publish information on mitigation measures once a year does not enable *ex ante* foreseeability of legally mandated censorship over legal content, but only provides *ex post* reporting. Overall, a mechanism where private entities formally take decisions that *de facto* have been required by law and influenced by public bodies does not provide for transparency over public interferences with freedom of expression. As a consequence, it may enable public bodies to evade accountability for their online speech policies. Online users, and society at large, would not be able to have detailed information about how systemic risks have been assessed, how the appropriate mitigation measures to be implemented have been determined, and which restrictions to harmful content provided for in the terms and conditions of VLOPs and VLOSEs are mitigation measures put in place according to Article 35(1).

73 Article 19, ''ARTICLE 19 recommendations for the Digital Services Act Trilogue'' (Article 19 website 2022) <EU: ARTICLE 19's recommendations for the Digital Services Act trilogue - ARTICLE 19> accessed 11 March 2024, pp. 2-3; Joan Barata (n 11) pp. 19–21; Joan Barata et al. (n 11) pp. 16-18.

74 Joan Barata, ''The Digital Services Act and its impact on the right to freedom of expression: special focus on risk mitigation obligations'' (2021) publication on *Plataforma en Defensa de la Libertad de Información* (PDLI), p. 20.

78 While not desirable for reasons of transparency and accountability, it is not clear to which extent this mechanism is also in violation of EU law provisions governing public action. While the delegation of public tasks to private entities can be criticised from the perspective of constitutional legitimacy,[75] a sharing of responsibilities between public and private entities is also widely regarded as essential in a complex world.[76] This is especially the case where private entities are in the best position to address certain societal issues such as harmful content.

79 From the perspective of the requirement that any interference with fundamental rights be ''provided for by law'', the legal basis providing for an interference with fundamental rights does not need to be adopted by a democratically legitimised body.[77] It suffices that it is an act of general application with the requisite quality of ''law''.[78] Moreover, it is not precluded that norms of private entities provide for the interference insofar as there is a delegation from public bodies to this end and there is appropriate public oversight over how the delegated powers are exercised.[79]

80 Nonetheless, it can be argued that the blurring line between public and private censorship for legal content is problematic for both legality *stricto sensu*, on the one hand, and for accountability on the other. The two aspects are interconnected, as they are both essential components of the rule of law.[80]

81 Lack of transparency over public action in content moderation does not enable users to fully understand the nature of the limitations to their fundamental rights and, consequently, it creates a gap in the accountability of public bodies. The lack of accountability and transparency may in turn increase the risks of an arbitrary exercise of power by public bodies, whose actions entailing a public interference with freedom of expression may not be recognisable and such. This may ultimately thwart the objective of the legality principle to function as a safeguard against arbitrariness of public action, which implies that public interferences are clearly recognisable as such and foreseeable in relation to their effects.

II. Redress channels against interferences with legal speech

82 The DSA is a real breakthrough when it comes to the protection of online users through procedural safeguards and redress mechanisms. It translates rule of law principles to the governance of online platforms, recognising the role of large providers of intermediary services as *de facto* rule setters with powers comparable to that of a state entity, as theorised by multiple scholars to date.[81] Examples

75 Rikke Frank JØrgensen (ed.), *Human Rights in the Age of Platforms* (The MIT Press, 2019).

76 Robert Baldwin, 'Better Regulation: The Search and the Struggle' in Robert Baldwin, Martin Cave, Martin Lodge (eds), *The Oxford Handbook of Regulation* (Oxford, Oxford University Press 2010), pp 259–278; Neil Gunningham, Darren Sinclair, 'Smart Regulation' in P Drahos (ed.), *Regulatory Theory: Foundations and Applications* (Canberra, ANU Press 2017); Christine Parker, 'Twenty Years of Responsive Regulation: An Appreciation and Appraisal' (2013), Regulation & Governance 2; Almada Marco, 'Regulation by Design and the Governance of Technological Futures' (2023) European Journal of Risk Regulation.

77 Robert Schutze, *European Union Law* (Oxford University Press, 2015), pp. 446-447; Koen Lenaerts, 'Exploring the Limits of the EU Charter of Fundamental Rights' (2021) European Constitutional Law Review, pp. 388-391;

78 Ibid.

79 *Barthold v Germany* App No 8734/79 (ECtHR 25 March 1985), para. 46; Hans-Bredow-Institut for Media Research, 'Study on Co-Regulation Measures in the Media Sector' (University of Hamburg, Final Report, Study for the European Commission, Directorate Information Society and Media, 2006) pp. 147-152.

80 Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 2020 Rule of Law Report, The rule of law situation in the European Union', COM(2020) 580 final; European Commission for Democracy through Law (Venice Commission), 'Rule of law checklist' (publication of the Council of Europe, 2016).

81 Nicolas Suzor, 'The Role of the Rule of Law in Virtual Communities' (2010) Berkeley Technology Law Journal 1817; Niva Elkin-Koren, Maayan Perel, 'Guarding the Guardians: Content Moderation by Online Intermediaries and the Rule of Law' in Giancarlo Frosio (ed.), *Oxford Handbook of Online Intermediary Liability* (Oxford University Press, 2020); Stephan Kolo ßa, 'Facebook and the Rule of Law' (2020) Zeitschrift für ausländisches öffentlichesRecht und Völkerrecht 509;

of procedural safeguards and redress mechanisms include transparency requirements,[82] the obligation to state reasons,[83] the internal complaint-handling system[84] and out-of-court dispute settlement.[85] These safeguards aim at protecting users against arbitrary and non-transparent content moderation practices, and at holding providers of intermediary services accountable for their actions.

83 Nonetheless, the remedies available to users against content moderation actions of private entities are different from those that would be available if the restriction of content were the clear result of public action.

84 If VLOPs and VLOSEs are enabled by the terms and conditions governing their services to restrict the dissemination of legal but harmful online content, users may only be able to act against such restriction by claiming that it is in violation of the terms and conditions. For example, there may be cases where online content is restricted on the basis of it being incompatible with terms and conditions. Should users believe that the lawful content was wrongfully labelled as incompatible, they may submit a complaint to the provider, or alternatively act before an out-of-court dispute settlement body or a judge. However, any such claim of the user against VLOPs and VLOSEs may only be based on contractual grounds, and in particular on the terms and conditions that regulate their private relationship.

85 Besides any claim based on the contractual norms governing the relationship between users and providers, it is not clear whether users could demand that VLOPs and VLOSEs respect their fundamental right to freedom of expression. In particular, if they could require that any interference with legal speech be justified in accordance with the criteria laid down in Article 52(1) of the Charter. Admitting this type of legal action would be tantamount to recognising the horizontal direct applicability of the right to freedom of expression in private relationships.

86 In legal doctrine, the horizontal direct effect of a provision denotes its ability to find application in cases between private parties, with the consequence that a private party may rely directly on that provision in judicial proceedings against another private party.[86]

87 Giving direct effect to fundamental rights in contractual relationships means that they apply directly in such relationship in the same way they do in a state (or EU institution or body) – citizen relationship,[87] and therefore that fundamental rights act as a direct limitation to the freedom of contract of the parties. The ECJ has explicitly stated that Article 51(1) of the Charter should not be interpreted as systematically precluding the horizontal effect of fundamental rights,[88] thus leaving the question open for the future.

88 Despite the fact that the Charter is not addressed to private parties, the ECJ has recognised the

Nicolas Suzor, 'Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms' (2018) Social Media and Society 1; Edoardo Celeste, 'Digital Constitutionalism: A New Systematic Theorisation' (2019) International Review of Law, Computers & Technology 76; Giovanni de Gregorio, *Digital Constitutionalism in Europe: reframing rights & powers in the algorithmic society* (Cambridge University Press 2022); Oreste Pollicino, 'The quadrangular shape of the geometry of digital power(s) and the move towards a procedural digital constitutionalism' (2023) European Law Journal.

82 See Article 14(1) of the DSA.

83 See Article 17 of the DSA.

84 See Article 20 of the DSA.

85 See Article 21 of the DSA.

86 Paul Craig, Grainne de Búrca, *EU Law: Text, Cases, and Materials* (seventh edition, Oxford University Press, 2020), pp. 225-232.

87 Chantal Mak, 'Fundamental rights in European Contract Law' (Dphil thesis, University of Amsterdam 2007), p. 49.

88 ECJ joined cases C-569/16 and C-570/16 *Stadt Wuppertal v Maria Elisabeth Bauer and Volker Willmeroth v Martina Broßonn* [2018] ECLI:EU:C:2018:871, para 87. In particular, the ECJ held in para 87 that: *''although Article 51(1) of the Charter states that the provisions thereof are addressed to the institutions, bodies, offices, and agencies of the European Union ... and to the Member States only when they are implementing EU law, Article 51(1) does not, however, address the question of whether those individuals may, where appropriate, be directly required to comply with certain provisions of the Charter and cannot, accordingly, be interpreted as meaning that it would systematically preclude such a possibility".*

horizontal direct effect of certain fundamental rights in private relationships on account of their mandatory and unconditional nature,[89] namely the right to non-discrimination,[90] the right to effective judicial protection[91] and the right to paid annual leave.[92] Therefore, it appears that the recognition of direct horizontal applicability is specific to each fundamental right based on its nature.

89 The horizontal application of freedom of expression has for long been a controversial issue, and it has been discussed, among others, specifically in relation to the contractual relationship between platforms and users.[93] To date, however, there is no judgement of the ECtHR or of the ECJ in legal proceedings brought by a user against an online platform for restrictions on content. Thus, there is no recognition of the horizontal effect of freedom of expression in such a relationship.

90 In the absence of a clear judicial recognition of the horizontal effect of freedom of expression in contractual relationships in the EU,[94] it cannot be claimed with sufficient certainty that online users would be able, at the EU level, to act against any content moderation decision that VLOPs and VLOSEs implement to mitigate the systemic risks caused by harmful but legal content under Article 35 of the DSA. At the national level, there is no common trend among Member States to recognise the horizontal effect of freedom of expression in private relationships, despite the ruling by the German Federal Court of Justice that online intermediaries face constitutional obligations vis-à-vis their users.[95]

91 If an interference with freedom of expression resulted from a public action, however, users would be able to directly invoke their right under the Charter in a legal action against a public body. For example, a user may bring action against a legal act of the European Commission that imposes a restriction on their online speech. To this end, they may claim that there is an unjustified interference with their right to freedom of expression, e.g. because the interference is in violation of the principle of proportionality. In this case, users would act in a terrain with significant legal certainty, given that the fundamental rights of the Charter have been primarily applied in private-public relationships. There is ample case-law of the ECJ and the ECtHR clarifying under which conditions an interference by public bodies with freedom of expression may be considered lawful.

92 In relation to harmful but legal content, any restriction that can be attributed to a public body may be challenged by users on multiple grounds, including that the systemic risks caused by the content in question do not justify an interference with its dissemination.

93 When VLOPs and VLOSEs restrict the dissemination of harmful but legal content to mitigate systemic risks in compliance with Article 35 of the DSA, the source of the interference is private contractual law, and in particular terms and conditions. Even when the regulatory dialogue between the European Commission and VLOPs and VLOSEs leads to the coproduction of content moderation decision, as described above, the interference would still stem from a private measure. There is no public action that can be *prima facie* connected to it. There would be no act from the European Commission that specifically mandates the restriction of specific content, as the

89 Paul Craig, Grainne de Búrca (n 87) pp. 225-232.

90 ECJ Case C-414/16 *Vera Egenberger v Evangelisches Werk für Diakonie und Entwicklung eV* [2018] EU:C:2018:257, paras 76-82.

91 Ibid.

92 ECJ joined cases C-569/16 and C-570/16 *Stadt Wuppertal v Maria Elisabeth Bauer and Volker Willmeroth v Martina Broßonn* [2018] ECLI:EU:C:2018:871, para 85.

93 Matthias C. Kettemann, Anna Sophia Tiedeke 'Back up: Can users sue platforms to reinstate deleted content?' (2020) Internet Policy Review 1.

94 It is worth recalling that, as far as the EU legal order is concerned, the horizontal applicability of fundamental rights in the relationship between online platforms and users is an open question, as explicitly stated by Advocate General Saugmandsgaard Øe in his Opinion in ECJ Case C-401/19 *Poland v. Parliament and Council* (2022) ECLI:EU:C:2022:297, para 90.

95 German Federal Supreme Court, Judgements of 29 Jul 2021, III ZR 179/20 and ZR 192/20; see also Matthias C Kettemann, Torben Klausa, 'Regulating Online Speech: Ze German Way' (Lawfare, 20 September 2021) https://www.lawfareblog.com/regulating-online-speech-ze-german-way accessed 15 March 2024; Matthias C. Kettemann, Anna Sophia Tiedeke (n 93).

ultimate decision on how to mitigate systemic risks would be made by VLOPs and VLOSEs.

94 To draw a distinction that clarifies this point, the situation is different under Article 36 of the DSA where the Commission adopts a decision[96] requiring one or more VLOPs or VLOSEs to take action in order to address a crisis.[97] While Articles 35 and 36 pursue similar objectives, i.e. to require VLOPs and VLOSEs to address risks posed by their services, they function according to different mechanisms that in turn lead to different remedies available to any user that may want to challenge a content moderation decision.

95 In both cases the measure that restricts online content is taken by a VLOP or VLOSE, but Article 36 requires the Commission to adopt a legally binding decision that potentially mandates the implementation of content moderation measures. In this case, the decision of the European Commission could be clearly identified as the source of any interference with the freedom of expression that may be adopted by VLOPs and VLOSEs. This leaves online users who are directly and individually concerned by the decision to bring action before the ECJ and seek its annulment under Article 263(4) of the Treaty on the Functioning of the European Union (''TFEU'')[98], insofar as they have *locus standi* for this action under the ''Plaumann test''.[99]

96 On the contrary, risk mitigation measures adopted under Article 35 of the DSA cannot be linked to a legally binding decision of the European Commission. The Commission participates in shaping private content moderation measures through regulatory dialogue, non-binding guidance and informal discussions. Therefore, there is no act of direct and individual concern against which users can bring action. Any action under Article 263(4) against Article 35 of the DSA is likely to be dismissed, for two reasons. First, the vague wording of Article 35 that does not prescribe any specific interference with freedom of expression.[100] Second, the fact that a reading of the Article does not allow to foresee with sufficient certainty in which specific cases it may require restrictions on the dissemination of legal content.[101]

97 Further to Article 263 of the TFEU, users may also not be able to bring action under Article 265(3) of the TFEU by claiming that the Commission has failed to act and protect the freedom of expression of online users in the exercise of its powers while supervising and orienting the conduct of VLOPs and VLOSEs. There are two reasons to conclude that Article 265(3) of the TFEU is not actionable in this case.

98 First, Article 265 would apply to cases where the EU institutions, bodies, offices and agencies have a clear obligation to take a specific action aimed at ensuring the VLOPs and VLOSEs do not violate the fundamental rights of online users when complying with Article 35 of the DSA. This does not seem to be the case under the DSA as the Commission enjoys

96 See Article 36(1) of the DSA.

97 For the purposes of Article 36 of the DSA, a crisis shall be deemed to have occurred where extraordinary circumstances lead to a serious threat to public security or public health in the Union or in significant parts of it. See Article 36(2) of the DSA.

98 See Article 263(4) of the DSA.

99 As formulated by the ECJ in Case 25/62 *Plaumann & Co v Commission* [1963] ECLI:EU:C:1963:17, p. 107. In this judgement, the ECJ set out the criteria to determine in which cases a natural or legal person can be considered to be ''individually concerned'', which is one of the conditions for *locus standi* under Article 263(4) of the TFEU. In particular, the ECJ held at p. 107 of the judgement that *''persons other than those to whom a decision is addressed may only claim to be individually concerned if that decision affects them by reason of certain attributes which are peculiar to them or by reason of circumstances in which they are differentiated from all other persons and by virtue of these factors distinguishes them individually just as in the case of the person addressed. In the present case the applicant is affected by the disputed Decision as an importer of clementines, that is to say, by reason of a commercial activity which may at any time be practised by any person and is not therefore such as to distinguish the applicant in relation to the contested Decision as in the case of the addressee''.*

100 In its judgement on the Plaumann case, the ECJ held that *''persons other than those to whom a decision is addressed may only claim to be individually concerned if that decision affects them by reason of certain attributes which are peculiar to them or by reason of circumstances in which they are differentiated from all other persons and by virtue of these factors distinguishes them individually just as in the case of the person addressed''.* See p. 107 of the OJ publication.

101 The formulation in abstract terms of the obligation in Article 35, and the impossibility to single out affected persons, are factors that render unlikely the fulfilment of the criteria affirmed by the ECJ in Plaumann.

significant discretion in deciding how to exercise its supervisory and enforcement powers and is not required to take specific actions.

99 Second, a natural or legal person can bring action under Article 265(3) where an EU institution, body, office or agency has failed to adopt an act to be addressed specifically to that natural or legal person. This Article is therefore not actionable in instances of failure to protect fundamental rights in a 'mediated' manner through supervision and enforcement over VLOPs and VLOSEs by the Commission.

100 Finally, in addition to actions before the ECJ against the Commission, users would also have no effective redress against the actions of the European Commission as a supervisor and enforcer under the DSA by relying on their rights conferred by the ECHR. The EU is not yet a signatory of the ECHR,[102] therefore proceedings against the European Commission cannot be brought before the ECtHR.

101 The lack of redress channels available to users in such cases appears problematic especially in light of the more 'informal' enforcement history of the European Commission in the past year. For example, in the letter sent by Thierry Breton on 12 August 2024, X was effectively requested to take specific actions in relation to clearly identified content. These actions could result in restrictions on the dissemination of legal but harmful content. This is an episode of 'jawboning' by the European Commission that clearly shows how regulatory expectations can be set without the adoption of acts that can be appealed before a court. While not formalised in an official act, these regulatory expectations can be conducive to concrete restrictions on legal content via the obligations laid down in the DSA. While this can take place across different areas where the European Commission has enforcement powers, such as antitrust enforcement, it presents unique problems under the DSA due to the potential consequences for users' freedom of expression.

102 In conclusion, users have multiple options for redress against content moderation decisions that violate the terms and conditions they adhered to. However, they have no means to obtain redress against interferences affecting the legal content they disseminate online that are put in place by online intermediaries in pursuit of public policy objectives, and indirectly mandated by legal requirements and regulatory demands. Similarly, VLOPs and VLOSEs would not have standing against disproportionate regulatory demands on the restriction of harmful but legal content, since they are not directly and individually concerned by interferences with the freedom of expression of users.

103 This gap in the redress solutions available to online users is particularly problematic for legal but harmful content, since the source of the interference with this category of content is precisely the regulatory dialogue between the Commission and VLOPs/VLOSEs, where it is determined in which cases the level of systemic risks created by harmful content justifies restrictions on its dissemination.

F. Discussion: Gaps in the Legal Framework to Adress a Hybrid Speech Governance Model

104 Based on the two problems highlighted above, a broader overarching issue can be identified. The new mechanism of public-private cogeneration of policies for the moderation of harmful but legal content in the DSA challenges an approach based on the dichotomy between public and private actors, and the different requirements that apply to them. The constitutional ambiguities of public-private cooperation for online speech moderation have already been discussed in relation to other regulatory schemes and provisions.[103] However, they present peculiar and unique issues under the DSA in relation to the moderation of harmful but legal content. The central role of systemic risk assessment

102 The obligations that arise under the ECHR, and the jurisdiction of the ECtHR, are limited to its signatories, i.e. the Member States of the Counsil of Europe. The EU shall accede to the ECHR according to article 6(2) of the TEU, but the accession has not yet taken place.

103 Niva Elkin-Koren, 'Government–Platform Synergy and its Perils' in Edoardo Celeste, Amelie Heldt, Clara Iglesias Keller (eds) *Constitutionalising Social Media* (Oxford: Hart Publishing, 2022); Rocco Bellanova, Marieke de Goede, 'Co-Producing Security: Platform Content Moderation and European Security Integration' [2022] Journal of Common Market Studies 1316.

and mitigation in balancing conflicting interests, and in constituting the basis for an interference with otherwise legal speech, would warrant more safeguards in relation to transparency, accountability and redress for legally mandated interferences with legal speech.

105 This interaction is not captured in EU human rights law, where different obligations are traditionally imposed on public and private actors. This interaction seems to be equally not addressed in the DSA.

106 First, the DSA does not require transparency on the dialogue between the European Commission and supervised intermediaries, nor on how regulatory demands shape private content moderation policies. External observers should be able to clearly understand which private content moderation policies are informed by legal requirements and regulatory demands, and which are merely choices of the intermediary.

107 Second, VLOPs and VLOSEs are under no obligation to indicate in their terms and conditions whether a given restriction is a risk mitigation measure put in place to comply with Article 35 of the DSA. A simple mention in this regard would ensure foreseeability for users of the restrictions stemming from a legal requirement, in line with the conditions in Article 52 of the Charter.

108 Third, despite the numerous procedural and transparency requirements laid down in the DSA for providers of intermediary services, the activities of VLOPs and VLOSEs are not subject to the same constraints to which public actors are, especially as concerns fundamental rights protection. Nonetheless, it would be challenging to identify a clear solution to this shortcoming in the absence of a recognition of full horizontal effects for freedom of expression.

109 In this regard, the question arises as to whether the obligation of Article 14(4) DSA to have due regard for the fundamental rights of the recipients of the service should be interpreted as introducing a direct or indirect horizontal effect of such rights in contractual relationships. Article 14(4) of the DSA, together with Article 5(1) of Regulation (EU) 2021/784, represent an unconventional and innovative legislative technique due to their reference to the Charter to frame the obligations of private entities.[104]

110 The explicit requirement on private actors to respect the fundamental rights of the Charter in the context of their contractual practices is a novelty in EU legislation. If observed through the lens of the conceptual framework on digital constitutionalism, it could be seen as an affirmation of constitutional responsibilities for private actors, with the establishment of a quasi-constitutional framework for content moderation practices. This legislative technique raises several questions on multiple fronts, including on whether the EU has competence to enact rules on fundamental rights protection beyond what is already foreseen in the Charter. In this regard, the question to answer is the meaning that should be ascribed to the fundamental rights obligations of Article 14(4). Article 14(4) operates a vague reference to the fundamental rights of the Charter and does not provide guidance on which could be its legal consequences.[105]

111 For this reason, a clear answer cannot be found in the text alone. Different alternative interpretations have been advanced so far on the meaning of Article 14(4),[106] with three ultimately advocating for the recognition of horizontal direct or indirect effects in connection to the provision.[107] These interpretations

104 Tobias Mast, Christian Ollig, 'The Lazy Legislature. Incorporating and Horizontalising the Charter of Fundamental Rights through Secondary Union Law' (Working Papers of the Hans-Bredow-Institut, Project Results No. 70, 2023), p. 5.

105 Mattias Wendel, 'Taking or Escaping Legislative Responsibility? EU Fundamental Rights and Content Regulation under the DSA', in Antje von Ungern-Sternberg (ed.) *Content Regulation in the European Union* (Trier University and Verein für Recht und Digitalisierung e.V., Institute for Digital Law Trier (IRDT), Volume I, 2023) pp. 81-82; Tobias Mast, Christian Ollig (n 104) p. 1.

106 For an overview of the authors that discussed the interpretation of Article 14(4) of the DSA, see: Tobias Mast, Christian Ollig (n 104); Joao Pedro Quintais, Naomi Appelman, Ronan Fahy, 'Using Terms and Conditions to apply Fundamental Rights to Content Moderation' (2023) German Law Journal 881; Mattias Wendel (n 105).

107 Authors have argued that Article 14(4) could have either a declaratory effect, i.e. merely declaring the horizontal applicability of fundamental rights which stems directly

offer potential solutions to the problem that EU fundamental rights obligations do not fully apply to at least one of the actors involved in the public-private cogeneration of content moderation policies for harmful but legal content.

112 On the one hand, the recognition of the direct horizontal application of freedom of expression would enable to fill a gap in the protection of the freedom of expression of users whose legal but harmful speech is moderated under Article 35 of the DSA. However, further research is needed to operationalise the right to freedom of expression in a horizontal setting, which would prove a difficult task. Due to its traditionally vertical application in binding state action, public law concepts (e.g. legitimacy) would need to be translated to a private setting. Scholars have endeavoured to provide a conceptual framework for the horizontal application of fundamental rights,[108] but it would need to take into account the specificities of each fundamental right in its operationalisation.

113 On the other hand, the indirect horizontal effect of fundamental rights[109] in the contractual relationship between intermediaries and users could at least ensure that contractual provisions are interpreted in light of the Charter. This would enhance the overall level of protection of EU fundamental rights, but it would not lead to a situation where fundamental rights fully constrain the content moderation actions of intermediaries. Thus, a gap would still be left in relation to the moderation of harmful but legal content.

114 Further to Article 14(4), VLOPs and VLOSEs are required to have '*particular consideration*' of the impact of their mitigation measures on fundamental rights, under Article 35(1) of the DSA. This provision is not phrased as laying down a fully-fledged obligation to respect fundamental rights, but rather to take them into consideration in the risk mitigation activities as a procedural requirement.

115 It is unlikely that this provision leads to any horizontal application of fundamental rights that users can rely on, in consideration of both its wording and the observations made above on the hurdles to recognise the horizontal effect of freedom of expression in the EU legal order. The European Commission may rely on this provision to ensure that risk mitigation measures are in line with fundamental rights. However, this does not provide for safeguards against public interferences with freedom of expression, as the European Commission would have the final word.

G. Conclusion

116 Hybrid or meta-regulatory forms of governance have become increasingly popular in EU digital regulation. They present undeniable advantages by giving significant discretion to the same entities that are in the best position to understand and address the risks posed by their services.

117 This contribution does not intend to label these regulatory arrangements as negative or unacceptable, nor to outrightly criticise the DSA. While recognising the positive developments introduced by the DSA, this contribution highlights the preconditions that could, but not necessarily would, allow for non-transparent and unaccountable backdoor entries

from the Charter, or a constitutive effect, i.e. being the source, with constitutive force, of the horizontal effects of the fundamental rights protected by the Charter. For a discussion on the hypothesis that sees Article 14(4) as constitutive of horizontal direct effects, see: Tobias Mast, Christian Ollig (n 104). For a discussion on the hypothesis that sees Article 14(4) as declaratory of pre-existing horizontal direct effects stemming directly from the Charter, see: Mattias Wendel (n 105).

108 David Bilchitz, *Fundamental Rights and the Legal Obligations of Business* (Cambridge University Press 2021).

109 Indirect effect is a doctrine used both in EU institutional law and in national contract law to indicate a situation where a provision or principle has indirect effect because it acts as a source of interpretation of another provision of principle. In EU law, the doctrine of harmonious interpretation (or indirect effect) was developed by the ECJ to require, in certain circumstances, that national law is interpreted in light of EU directives. In the context of contractual relationships, the indirect effect of fundamental rights indicates the role of fundamental rights to act as source of inspiration for interpreting and applying norms of contract law. The indirect effect of fundamental rights in contractual relationships has been mostly discussed at the level of EU Member States' law, especially in German case-law through the doctrine of *mittelbare Drittwirkung*.

of public policy considerations into private policies for the moderation of legal but harmful content. Moreover, it intends to hint at the necessity to discuss possible solutions. As new regulatory models emerge, it is necessary to conceive new solutions to ensure that public functions are performed in a way that is consonant with a democratic system based on the rule of law.

Towards an Optimal Regulatory Strategy for Data Protection: Insights from Law and Economics

by **Donatas Murauskas and Raminta Matulytė ***

Abstract: In this paper, we examine data protection regulation from the standpoint of Law & Economics. Specifically, we analyze the advantages and disadvantages of the two distinct data protection regulation frameworks in the EU and the US. We compare these regulatory frameworks based on the criteria set by S. Shavell in his seminal work "Liability for Harm Versus Regulation of Safety". We utilize Shavell's model to compare the *ex ante* regulatory approach to data protection in the EU with the *ex post* liability approach of the US. This comparative analysis helps us explore whether the focus in the field of data protection should be on proactive (*ex-ante*) regulation or reactive (*ex-post*) liability. We find difficulties in comparing the regulatory frameworks, considering the dominant conceptual framework of human rights in the data protection field. However, the comparison provides valuable efficiency-based arguments on ways to optimize both regulatory frameworks.

Keywords: Data Protection Regulation; GDPR; Law & Economics; Ex-ante Regulation; Ex-post Liability

Recommended citation: Donatas Murauskas and Raminta Matulytė, Towards an Optimal Regulatory Strategy for Data Protection: Insights from Law and Economics, 15 (2024) JIPITEC 269 para 1

A. Introduction

1 The dawn of the internet promised the loss of control of our privacy – "You have zero privacy anyway," according to the CEO of Sun Microsystems in 1999.[1] Yet, political and civil mobilisation has tried to 'get our privacy back'[2]. The emergence of AI-based tools focuses discussions on the privacy price paid to receive AI-based services. The European supervisory authorities target tech-giant Meta for non-compliant data protection practices, including unjustified data transfers to the US.[3] How can we reconcile the demand for privacy in the

* Donatas Murauskas is Associate Professor at Vilnius University Law Faculty, donatas.murauskas@tf.vu.lt. Raminta Matulytė is PhD student at Mykolas Romeris University, raminta.matulyte@stud.mruni.eu.

1 Polly Sprenger, 'Sun On Privacy: "Get over It"' (Wired, 26 January 1999) < https://www.wired.com/1999/01/sun-on-privacy-get-over-it/> accessed 19 December 2023.

2 Timothy Garton Ash, *Free Speech: Ten Principles for a Connected World* (Yale University Press; Reprint edition, 2017).

3 European Data Protection Board, '1.2 Billion Euro Fine for Facebook as a Result of EDPB Binding Decision' (EDPB, 22 May 2023) <https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en accessed> 14 August 2024.

age of AI with the growing need for data-driven services and international data flows?

2 The normative analysis sometimes ignores one of the crucial features of 'good' regulation: its efficiency.[4] In this paper, we do not want to analyse the advantages and disadvantages of data protection regulatory frameworks by looking at the wording of norms of legal acts. On the contrary, we aim to consider whether regulators should rely on economic efficiency in deciding which data protection regulatory approach is more preferred by society. Using Steven Shavell's economic analysis of law, which contrasts *ex-ante* regulation with *ex-post* liability, we assess the efficiency of the US and the European regulatory approach in protecting data rights.

3 First, we examine the concept of economic analysis of law and what models may be useful for lawmakers to measure the economic efficiency of planned regulation. Then we provide introductory insights to privacy economics, which is important considering our goal to discuss particular human rights (i. e. the right to private life and the right to data protection) in the context of efficiency (i. e. economic domain). Third, we chose the data protection regulatory frameworks in the EU and the US to show how economic analysis of law may be applied in practice to determine economic efficiency and to compare the chosen regulatory approaches in different jurisdictions. Finally, we discuss recent developments in the field of data protection that show the search for a balance between economic efficiency and the need to set data protection standards while maintaining constitutional national security and data privacy safeguards.

B. Economic Analysis of Law and Its Applicability to Emerging Regulatory Fields

4 Among other significant ideas in the realm of law and economics, scholars develop models to determine the social costs of selected regulatory approaches. In the field of social preference for *ex-ante* regulation and *ex-post* liability, S. Shavell's model depicted in his seminal work "Liability for Harm Versus Regulation of Safety"[5] is the most suitable to measure the economic efficiency of chosen data protection regulation frameworks.

5 Shavell analyses why society prefers to strictly regulate some fields or leave others unregulated, ensuring tort liability. He describes that tort liability (*ex-post* liability) is private in nature and works not by social command, but by the effect of legal damage actions that may be brought once harm occurs. Standards, prohibitions, and other types of safety regulation (*ex-ante* regulation), on the other hand, are public in nature and modify behaviour immediately through requirements imposed before, or at least independently, of the occurrence of harm.[6]

6 Are there any factors implying a preference for one or the other model? Shavell indicates four determinants of the relative desirability of *ex-post* liability and *ex-ante* regulation. According to Shavell, to identify and assess the factors determining the social preference for liability and regulation, one should set out a measure of social welfare. He assumes that this measure equals the benefits that parties derive from engaging in their activities, less the sum of the costs of precautions, the harms done, and the administrative expenses associated with the means of social control. The formal issue is to employ control mechanisms to maximise the welfare measure. Shavell outlines four factors that impact the solution to this issue (Image 1).[7]

4 Robert Baldwin, Martin Cave, Martin Lodge, 'Understanding Regulation. Theory, strategy, and Practice' (Oxford University Press; 2nd edition, 2012, 31.

5 Steven Shavell, 'Liability for Harm versus Regulation of Safety' (1984) 13(2) The Journal of Legal Studies 357.

6 Ibid 357.

7 Ibid 358-359.

Image 1. Shavell's Determinants Defining Social Preference for *Ex-Ante* Regulation and *Ex-Post* Liability[8]

7 Shavell considers that giving the regulator the power of control when private parties have complete information about risky behaviour about which the regulator has little knowledge will lead to a high probability of regulation errors. The regulator's standard will be excessively strict if it overestimates (1) **the possibility of harm caused by risky activity**. In the opposite case, if the regulator makes contrary errors, its requirements may be overly lenient.[9] Shavell suggests that because the private parties are the ones who are engaged in and benefit from their actions, they should have an inherent advantage in knowledge. Obtaining such information for a regulator would usually need near constant surveillance of parties' conduct, which would be practically impossible. However, in some specific fields, information about risks may not be evident and will take effort or particular competence to analyse, which the regulator may supply in these situations by dedicating social resources to the task.[10]

8 Next, (2) **the capacity to pay for the harm caused** would be irrelevant under regulation, assuming that parties would take steps to reduce risk as a precondition for engaging in their activities; therefore, any harm will be less likely to occur.[11]

9 (3) **The possibility of avoiding a lawsuit** for the damage done might be another important factor. First, a defendant may avoid *ex-post* liability because the harms caused are widely dispersed, making it difficult for any single victim to pursue legal action. Second, there could be a significant period of time before any harm occurs; therefore, it could be impossible to gather the evidence needed for a successful suit. Third, it is challenging to assign guilt for harm to those actually accountable for it, as actual harm often may not be directly linked to certain actors.[12]

10 Finally, (4) **the tort system's costs** must be widely defined to cover private parties' time, effort, legal fees, and public expenses such as trial costs. Similarly, administrative costs of regulation encompass expenses of maintaining the regulatory establishment and the private costs of compliance. In this scenario, liability has the benefit because, in such cases, most administrative expenses are incurred only if harm occurs, while administrative costs are always incurred under regulation.[13]

11 In conclusion, administrative expenses and difference in knowledge, according to Shavell, favour social preference for *ex-post* liability. The inability to pay for the harm done and the opportunity to avoid lawsuits, on the other hand, support *ex-ante* regulation. Shavell argues that these two approaches should not be seen as mutually exclusive. Instead, a comprehensive legal solution to any social problem should include *ex-post* liability and *ex-ante* regulation, with the balance reflecting the significance of the determinants.[14] In this article, we consider whether Shavell's model can suggest the most efficient methods for balancing regulatory approaches, especially in the data protection field.

C. The Economics of Privacy

12 Before exploring a comparison of different data protection regulatory frameworks, it is imperative to first address the challenge of discussing human rights – such as the right to private life and the right to data protection—within the context of economic considerations. This interplay often raises complex

8 Compiled by the authors based on Shavell (n 5).

9 Shavell (n 5) 359.

10 Ibid 360.

11 Ibid 360-361.

12 Ibid 363.

13 Ibid 363-364.

14 bid 365.

questions about the monetary value that may be ascribed to human rights.

13 The discussion of rational individual decision-making can be situated within the context of human rights. While human rights involve inherent trade-offs between individual autonomy and public needs, their monetary value is inherently challenging to quantify. Human rights are fundamental, universal, and inviolable, representing intrinsic values grounded in respect for human autonomy and dignity. Privacy and data protection, in particular, are enshrined as fundamental rights under Articles 7 and 8 of the Charter of Fundamental Rights of the EU. This raises the question: what are the conceptual foundations for examining human rights within the framework of economic analysis of law?

14 Similar to other goods and services, individuals hold preferences and make assessments regarding human rights. While it is impossible to objectify human rights in purely monetary terms, this does not preclude the possibility of determining their relative value. Human rights safeguard specific aspects of human autonomy and can be viewed as both final and instrumental goods.[15]

15 Economic studies imply that no definitive conclusions can be made about whether there are actual costs / benefits of individuals or societal privacy protection.[16] If we imagine data protection rights as property rights, with personal data as an object of transactions, it enables a more economically driven approach to assessing data protection. This perspective allows for the examination of trade-offs between maintaining privacy and sharing data with service providers.

16 If companies are collecting data of private individuals, they can make their goods and services better aligned to the preferences of these individuals. In this context, collected data that includes individual attributes might be regarded as business asset "that can be used to target services or offers, provide relevant advertising, or be traded with other parties."[17] Individuals may incur various costs as a result of sharing excessive amounts of data. For instance, reputational damage could occur due to the loss of sensitive information. Additionally, individuals may suffer financial losses stemming from information asymmetry, where a service provider, leveraging collected data, charges personalised prices aligned with the individual's aggregated preferences. Acquisti et al. also provide examples of positive externalities in cases of data sharing such as personalized services and discounts.[18] They also underline the specific nature of information privacy as maintaining characteristics of public and private goods.[19]

17 Privacy, like other human rights, is sometimes conceptualized as a public good due to its characteristics of non-excludability and non-rivalry. These rights are non-rivalrous because one person's enjoyment of them does not diminish the ability of others to enjoy them as well. However, they are only partially non-excludable, as access to these rights can be restricted or obstructed by legal or social discrimination or a lack of economic resources.[20]

18 Individuals maintain specific preferences regarding their privacy and behavioural constraints such as bounded rationality.[21] Farell underlines that "there is also a dysfunctional equilibrium in which few consumers devote much attention to disclosures, disclosures are vague, noncommittal, or even if explicit, mostly ignored; and the privacy policies chosen are

15 "[H]uman rights can be final goods (that is, goals to be achieved for themselves) or intermediate goods (that is, means to realize other goods or rights)." (Georges Enderle, 'Human Rights as Public Goods'. In: *Corporate Responsibility for Wealth Creation and Human Rights* (Cambridge University Press, 2021 152). Farrel suggests that privacy has elements of both (Joseph Farrell J, 'Can Privacy Be Just Another Good?' 10 Journal on Telecommunications and High Technology Law, 2012 252).

16 Alessandro Acquisti; Curtis Taylor; Liad Wagman, 'The Economics of Privacy', 54(2) Journal of Economic Literature 2016, 444.

17 Ibid 444.

18 Ibid 445.

19 Ibid 446.

20 Enderle, (n 15) 151–152.

21 Wolfgang Kerber, 'Digital markets, data and privacy: competition law, consumer Law and data protection', 11(11) *Journal of Intelectual Property Law & Practice*, 2016 849.

inefficiently non-protective".[22]

19 Therefore, while a traditional law and economics approach would seek the economically efficient (i.e., welfare-maximising) specifications of these property rights, the normative choice to regard privacy as a fundamental individual right might result in stronger protection of privacy and personal data than what would be justified by an economic efficiency standard.[23]

20 Determining the economic value of data or privacy remains a challenging task. Our attempt to apply the Shavell framework to data protection regulation inevitably raises questions about the appropriate conceptual framework for data protection. While we endeavor to treat data protection as an asset within the law and economics paradigm, this approach offers limited contributions to the broader and more complex discourse on the value of data and privacy within the context of fundamental rights. This is the trade-off of maintaining a consistent yet narrow focus—restricting the analysis to a single dominant framework, namely law and economics. With this limitation in mind, we now turn to the search for a more efficient standard in data protection.

I. Example of Data Protection Regulation Models

21 Almost no technology-driven field nowadays can operate without at least some kind of relation to the processing of personal data. Over the last few decades, rapid technological development has resulted in the need to search for options for data protection regulation. However, with the introduction of different data protection standards, discussions on which standard to follow or how to improve existing ones are as relevant as ever.

22 The General Data Protection Regulation (GDPR)[24] is the EU data protection standard that sets numerous obligations to companies and a list of rights of individuals. The opposite of such comprehensive and strict regulation enshrined in one legal act is the US data protection framework, that is fragmentary and does not foresee obligations for organisations or rights to individuals in every case concerning data processing. These different jurisdictional approaches are the subject of our further analysis. In the table below (Table 1), we summarised the main features of data protection regulation models in the EU and US.

22 Farell, (n 15) 259.

23 Kerber, (n. 21) 864.

24 Regulation of the European Parliament and of the Council 2016/679 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 [2016] OJ L 119/1.

Jurisdiction	Legislation	Centre of the regulatory framework	Supervisory authority	Enforcement
EU	One comprehensive personal data protection regulation - GDPR	A data subject who is granted a list of certain rights	A well-established network of supervisory authorities in the EU member states	Administrative fines for infringement up to 20 million euros or 4 % of the annual turnover GDPR allows individuals to seek damages
US	Sectoral federal legislation; comprehensive legislation adopted on a state-level	Business freedom and its right to choose the best way to protect individuals' data by way of contractual obligations	No clearly designated supervisory authority on a federal level (Federal Trade Commission operating as *de facto* authority)	No unified system of administrative fines Allowed possibilities to bring claims before courts regarding privacy infringements

Table 1. Main features of the EU and the US data protection regulation frameworks

23 While the EU and US have different approaches to data protection, both jurisdictions attempt to combine *ex-ante* regulation and *ex-post* liability in their data protection regulation models. We further analyse the social costs of the EU's and US's data protection regulation models and preference for either *ex-ante* regulation or *ex-post* liability based on the previously described Shavell's economic approach, by applying the four determinants that, according to Shavell, influence preference for *ex-ante* regulation and *ex-post* liability.

1. Difference in Knowledge about Risky Activities

24 We consider the data protection field to be a good example of how private parties and state institutions can have very different understandings, knowledge, and approaches towards personal data and the necessary level of protection. In his model Shavell refers to regulatory authorities, which in the data protection field should also include Supervisory Authorities.[25] Supervisory Authorities interpret the data protection legislation and can *de facto* expand or narrow down the data protection rules. Technological neutrality of the data protection laws results in their equal applicability to big-tech companies and organisations that process data in a non-complex manner. This presupposes that while it is not too difficult to have knowledge of basic operation principles and set standard rules for simple cases, this is not true if we talk about processing data using emerging tech-

25 Referring to Article 51(1) of the GDPR ("Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority')").

nologies. The complicated technological solutions used for data processing may cause a significant difference in the information that companies and state actors possess. Additionally, the human rights lens taken by regulatory authorities could be considered a difference in knowledge because private parties in the data protection field often follow the approach that consumers choose to give up their data to receive services or purchase goods. Therefore, companies consider themselves the ones that should know better, how to efficiently serve their customers.

25 **Europe**. The GDPR is constructed as a technologically neutral legislation.[26] Hence, the abstract provisions apply to different actors operating in different business fields. The neutral nature of the GDPR causes Supervisory Authorities to possess different knowledge on the applicability of the GDPR depending on differences in data processing performed by various actors. Big-tech companies often process data in a complex way; for example, technical characteristics may not directly indicate whether particular data may be related to an identified or identifiable natural person in the way that is defined under Art. 4(1) of the GDPR (e.g., data logs, encrypted data). These technical characteristics may become an issue when Supervisory Authorities investigate organisations and apply GDPR principles to specific data processing operations. In such cases, the Supervisory Authority may lack expertise and resources to thoroughly analyse and understand the actual technical setting. This may result in fines that do not necessarily ensure the factual protection of personal data.

26 Another factor proving the differential knowledge is the asymmetry of the burden that lies with global corporations and small and medium enterprises. The latter, in most cases, are obliged to comply with requirements that are exactly similar to those imposed on the big companies. However, they often do not extensively process massive datasets or cause a significant threat to individuals. Such regulatory asymmetry may be considered what Shavell describes as "a chance of regulatory error", where the EU regulation overestimates the potential for harm in small and less intrusive data processing operations and sets too stringent data protection standards.

27 **The US.** The US model is based on the premise that private parties should generally enjoy an inherent advantage in knowledge of their risky activities. For a regulator to obtain the same information would often be practically impossible, especially when the information concerns complex technological solutions. The US approach corresponds with the fact that regulators usually possess less information than private parties in the data protection field. However, the fragmented sectoral regulation is an example of what Shavell describes as better knowledge possessed by the regulator due to the specifics of the field that require special protection. For example, children's privacy protection under the Children Online Privacy Protection Act[27] or health data protection under the Health Insurance Portability and Accountability Act[28] shall be considered areas where private parties do not enjoy the same knowledge as the regulator – the areas are so sensitive that the regulator is considered as a greater incentive to ensure data protection compliance due to the ease of ensuring a higher level of expertise in very specific fields. Following Shavell's notions in these areas, substantial regulation is not a coincidence but rather a need, both because liability alone would not adequately reduce risks and because the usual disadvantages of regulation are not as severe as in the tort context.

28 It is fair to state that the US model reflects the difference in knowledge about risky activities better than the EU model as it leaves most data protection-related decisions[29] to organisations and to liability, accordingly. The US fragmentary approach to federal regulation reflects specific fields that require a higher standard of protection and provides examples where the regulator possesses more knowledge than private parties. On the opposite note, with technological neutrality, the GDPR obliges Supervisory Authorities to possess more information than private parties on technological aspects to enforce the regulation. This often is impossible due to limited resources and expertise. At the same time, the GDPR

26 GDPR (n 24) recital §15.

27 Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. §§ 6501–6506 (Pub. L. 105–277), 112 Stat. 2681-728.

28 Health Insurance Portability and Accountability Act of 1996 (HIPPA), Pub. L. 104–191, 110 Stat. 1936.

29 Shavel (n 5) 369.

does not provide specific implementation guidelines, making it difficult for companies to interpret the regulation and establish appropriate data management practices to ensure compliance.[30]

2. Incapability to Pay for the Full Harm Done

29 Harm under the data protection regulation is not straightforward to define. Possible administrative fines influence preference for regulation or liability even greater than the risk of paying damages. This determinant shall be adjusted for the data protection field as data actors often measure risks relating to imminent administrative fines and not harm-related costs. Shavell states that the party's assets are crucial in establishing whether this determinant favours more regulation or liability – the greater the likelihood of harm being much larger than assets, the greater the appeal of regulation. However, such presumptions shall be altered considering the importance of fines in the data protection field.

30 It is crucial to consider how harm is interpreted under the data protection legislation. While it is relatively easy to determine harm in cases of data breaches when a financial loss occurs (e.g., cases of identity theft), there are difficulties in measuring such harm when the loss is intangible (e.g., mere disclosure of personal data) or not related to data breaches (e.g., refusal to grant access to personal data held by an organisation) – although the claimants could invoke a non-pecuniary loss, "there is hardly any other issue in tort law which is assessed so differently throughout Europe".[31]

31 What we can agree upon is that privacy, in general, and data, in particular, hold certain economic value. If privacy is regarded as a specific type of property owned by an individual, a market emerges that defines the value of privacy (or data) loss. In this context, it is reasonable to conclude that various combinations of regulatory interventions, technological solutions, and economic incentives could effectively balance protection and sharing, thereby enhancing both individual and societal welfare.[32] However, the content of such 'balance' is not certain due to too divergent views on the value of privacy itself.

32 **Europe.** The inability to pay relates more to the failure to pay a fine than to pay for the harm done in the context of the GDPR. Usually, when organisations to whom the GDPR applies assess the risk, they consider the possibility of being fined, not the damages that could be required to pay for the harm caused. However, the GDPR allows a Supervisory Authority to impose a fine for up to 20 million EUR or 4 % of the annual turnover, whichever is higher.[33] The second limit proved useful for fining major corporations – the top 10 fines imposed under the GDPR exceed the 20-million limit, with 1.3 billion EUR being the highest fine imposed.[34]

33 Some national jurisdictions in the EU may be considered stricter than others. For example, in 2023, the French Supervisory Authority issued 42 sanctions, including 36 administrative fines for a total amount of 89 million EUR,[35] the Irish Supervisory Authority issued 19 fines for a total amount of 1.55 billion EUR,[36] the Spanish Supervisory Authority issued 367 decisions, including the imposition of fines for a total amount of more than 29 million EUR.[37] In

30 Clément Labadie and Christine Legner, 'Building data management capabilities to address data protection regulations: Learnings from EU-GDPR,' 38(1) *Journal of Information Technology*, 2023, 17.

31 Jonas Knetsch, 'The Compensation of Non-Pecuniary Loss in GDPR Infringement Cases', 13(2) *Journal of European Tort Law*, 2022, 135.

32 Acquisti et al., (n 16) 484.

33 GDPR (n 24) Article 83(5).

34 Until 23 August 2024, more than 2100 fines, reaching more than 4.5 billion euros overall, were imposed by Supervisory Authorities across Europe (GDPR Enforcement Tracker, 2023) <https://www.enforcementtracker.com/?insights> accessed 23 August 2024.

35 *See* CNIL 'The 2023 Annual Report of the CNIL' <https://www.cnil.fr/en/cnil-publishes-its-annual-report-2023 > accessed 23 August 2024.

36 *See* Data Protection Commission 'Data Protection Commission Publishes 2023 Annual Report' < https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-publishes-2023-annual-report > accessed 23 August2024.

37 *See* AEPD 'The AEPD receives for the third consecutive year

comparison, in 2023, the Lithuanian State Protection Inspectorate issued 13 fines for a total amount of 64,060 EUR.[38] To date, in Lithuania only one major fine was issued for GDPR violations of almost 2.4 million EUR.[39] However, close cooperation between the Supervisory Authorities and the one-stop-shop principle allows to, in general, keep the enforcement practice unified. While some of the fines do not cause a significant burden, there are examples when even a small administrative fine under the GDPR is too hefty for small organisations.[40] The possibility for courts to reduce fines functions as a safeguard for organisations to receive fair sanctions. However, the GDPR imposed approach of rigorous fines could generally propose that Shavell's determinant – incapability to pay – favours the liability more than the regulation.

34 **The US.** In contrast to the EU's regulatory model, the US model presents challenges in assessing an organization's incapability to pay fines or compensation for harm. The Federal Trade Commission (FTC) has a mandate to charge organisations with violation of Section 5 of the FTC Act, which prohibits unfair and deceptive actions and practices in or affecting commerce. While the FTC also enforces various federal consumer privacy and security laws, such as COPPA and GLBA, the frequency of enforcement actions remains limited, typically focusing on large technology firms rather than a broader range of organizations handling personal data.[41] However, the number of such actions is insignificant according to the publicly available information – in other words, while the FTC has the discretion to impose significant fines to the extent it relates to consumer protection, the number of launched investigations is very limited and usually targets tech giants rather than all organisations that in one way another process personal data.

35 Although other federal institutions can impose fines under sector-specific laws, these actions are relatively infrequent. However, when fines are imposed, they tend to be substantial, acting as a deterrent and encouraging compliance within regulated sectors. Despite this, a primary concern in the US remains the actual financial exposure faced by organisations if privacy-related lawsuits are successful. This aligns with the distinct litigation culture in the US, where companies often rely on self-regulation and precautionary measures to avoid substantial liabilities, as highlighted by Shavell.[42] Small and medium-sized enterprises, in particular, perceive less urgency in assessing their capacity to pay fines or face litigation – the data shows that in the US, targets for hefty fines are usually big tech companies, which are also at higher risk of facing a class action.[43]

---

the highest number of complaints in its history' < https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/aepd-recibe-por-tercer-anno-consecutivo-mayor-numero-reclamaciones-historia > accessed 23 August 2024.

38 *See* Valstybinė duomenų apsaugos inspekcija 'The State Data Protection Inspectorate has published its 2023 activity report', < https://vdai.lrv.lt/lt/naujienos/valstybine-duomenu-apsaugos-inspekcija-paskelbe-2023-m-veiklos-ataskaita/ > accessed 23 August 2024.

39 *See* Valstybinė duomenų apsaugos inspekcija 'A company operating an online second-hand clothing trading and exchange platform is fined under the General Data Protection Regulation', < https://vdai.lrv.lt/lt/naujienos/internetine-devetu-drabuziu-prekybos-ir-mainu-platforma-valdanciai-bendrovei-skirta-bauda-pagal-bendraji-duomenu-apsaugos-reglamenta/ > accessed 23 August 2024.

40 For example, the Lithuanian division of the International Council of Monuments and Sites (ICOMOS) was fined 3000 euros for lack of legal basis for data processing under the GDPR. However, the court reduced the fine to 1500 euros, considering the annual budget and the ICOMOS activity in the cultural heritage field. *ICOMOS* case (Judgment of the Vilnius Regional Administrative Court), No. EI2-1249-789/2020 (2020-04-08).

41 Federal Trade Commission, "Privacy and Security Enforcement" <https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement> (accessed 10 October 2024).

42 Shavell (n 5) 363.

43 According to data published by the FTC, over the last five years, actions for different types of privacy violations have been brought before tech giants such as Miniclip, Microsoft Corporation, Facebook, Amazon.com, Google, Epic Games (see: Federal Trade Commission, 'Protecting Consumer Privacy and Security', <https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/kids-privacy-coppa> and <https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement> accessed 26 August 2024). The latter, for example, recently resulted in Epic Games agreeing to pay $520 million - a $275 million fine for violating the Children's Online Privacy Protection Act and $245 million in refunds for using "dark patterns" that misled customers

36 While Shavell's theory suggests that incapacity to pay favours *ex-ante* regulation, this concept proves to be complex in data protection. The development of this field shifted towards fines as a preferred way to incentivise market participants. Therefore, organisations evaluate possible fines in different jurisdictions. Unlike more abstract US approach to fines, the EU's harmonised enforcement across Member States has resulted in a consistent and rigorous application of fines. Furthermore, the ability to assess incapacity to pay in both jurisdictions hinges on differing interpretations of harm within the context of data protection.

3. Escaping the Threat of Suit for Harm Done

37 The possibility of escaping the threat of a suit for harm done is very likely in the data protection field. Shavell indicates that the importance of this aspect is partly determined by why a lawsuit may not be filed.[44] First, the harm that may occur in the data protection field is hardly measured. Therefore, the possibility of escaping the suit is relatively high. Second, usually, in cases of massive data breaches, the harms a company generates are widely dispersed, making it unattractive for any victim individually to initiate legal action, especially against big-tech companies. This may be overcome by the possibility of maintaining class actions. We focus on the possibility of class actions rather than individual claims, as we consider class actions to be more relevant for evaluating organisations' preference for either regulation or liability. Third, difficulties for suing may occur due to a long period of time before actual harm related to a data breach occurs, meaning that the necessary evidence can be ineffective by the time the lawsuit is filed. Fourth, it could be challenging to attribute harm to responsible parties. For example, malicious action that causes harm is performed by a third party that accessed data online and not by an organisation that was in possession of the data.

38 **Europe.** GDPR sets not only a mechanism for imposing fines but the right to claim damages for anyone who has suffered material or non-material harm due to a violation of the GDPR (Article 82(1) of the GDPR). This means that a breach of the GDPR may have consequences under both private and public law. Data subjects can seek compensation before national courts for material or non-material damage that results from the infringement of their rights under the GDPR. The regulation also sets the principle of full compensation for the plaintiffs, which is very protective of data subjects' rights. Some of the potential damages, such as costs incurred due to fraudulent spending, credit card charges, and so on, are straightforward to identify (and for companies to reimburse individuals for). In contrast, "non-material damage" is a more abstract concept under the data protection legislation that is difficult to define.

39 While filing individual actions before corporations for causing harm may not look very promising, the GDPR and EU Regulation on Collective Redress[45] provides for the possibility of class actions.[46] Spreading the cost of litigation across many plaintiffs creates a greater likelihood of challenges being brought in court. However, the situation of bringing collective action is not uniform across the EU. Even though the GDPR states that the data subject "shall have the right to" initiate actions, it does not provide the data subject with an actionable tool. Instead, EU Member States are responsible for this. In other words, because the GDPR does not cover the procedural elements of a data subject's claim, a reference to national procedural legislation should be made. This raises the issue that there could be as many personal data collective action procedures as the EU Member States, contrary to the GDPR's objective of consis-

into making unwanted purchases (see: Federal Trade Commission 'FTC Finalizes Order Requiring Fortnite maker Epic Games to Pay $245 Million for Tricking Users into Making Unwanted Charges' <https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-finalizes-order-requiring-fortnite-maker-epic-games-pay-245-million-tricking-users-making>, accessed 26 August 2024).

44 Shavell (n 5) 363.

45 Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC

46 According to Article 80 of the GDPR, a data subject has the right to appoint a non-profit entity, organisation, or association with statutory objectives in the public interest and activity in the field of data protection to file a complaint on their behalf.

tency across Europe.

40 Significant developments in the right to damages under GDPR infringement were recently provided by the CJEU. A request for a preliminary ruling regarding the case between *UI v. Österreichische Post AG* challenged whether compensating a claimant requires, in addition to a GDPR violation, that the claimant has experienced damage or if the infringement of GDPR provisions is sufficient itself (referral for a preliminary ruling by the Supreme Court of Justice of the Republic of Austria). The CJEU concluded that Art. 82 of the GDPR requires establishing (i) "damage", either material or non-material; (ii) an actual infringement of the GDPR; and (iii) a causal link between the two."[47]

41 **The US.** US tech giants are also not immune from class actions, and the possibility of evading a lawsuit in case of massive data-protection relation issues is relatively high. There are successful examples. For instance, video conferencing platform Zoom faced a class action for allegedly sharing users' data without their consent and providing false information about their software being end-to-end encrypted. Inc. Privacy Litigation sued Zoom, claiming that such alleged conduct violated California state and federal laws. Zoom denies these allegations of any liability whatsoever. The parties agreed to the settlement. The court has decided that everyone who fits the set description is a settlement class member and can submit a claim form and receive payment. Zoom has agreed to pay 85 million dollars to settle the action.[48] The same situation happened with the video-sharing app TikTok, which faced a lawsuit for using and collecting users' data in connection with their use of the app without the proper notice or consent, a violation of state and federal law. TikTok has agreed to pay 92 million dollars to eligible claimants to settle the action.[49]

42 However, recent case law confirmed difficulties faced by privacy class actions brought in the US. The US Supreme Court judgment in *TransUnion LLC v. Ramirez case*[50] confirmed that there is no standing without concrete harm in federal court. The issue stemmed from the Fair Credit Reporting Act, which mandates that credit reporting agencies follow reasonable processes to ensure that customer records are as accurate as possible. According to the Fair Credit Reporting Act,[51] any individual who willfully fails to comply with the rules "is liable to that customer" for damages. Due to database errors, TransUnion has wrongly identified thousands of law-abiding Americans on the government's list of terrorists, drug traffickers, and serious criminals in their credit reports, which made (or could have made) obtaining financial services impossible or very hard to achieve. In this case, the court held that only 30 per cent of the class action members experienced an actual injury from the errors. The remaining 70 per cent lacked standing because the mere presence of inaccuracy in an internal data file, if it was not disclosed to a third party, caused no concrete harm. As a result, the US Supreme Court remanded the case, stating that "in a suit for damages, the mere risk of future harm, standing alone, cannot qualify as a concrete harm."[52]

43 There are certain differences between the litigation cultures in Europe and the US. While there has yet to be a wave of GDPR-related class actions in Europe, the long tail of these kinds of cases makes it impossible to establish if this is because they do not exist or because they are still making their way through the system. However, the risks of facing a class action are relatively low in the data protection field

47 Case C-300/21 *UI v Österreichische Post AG* [2023].

48 In re: Zoom Video Communications, Inc. Privacy Litigation, 'Settlement Agreement' (US District Court for the Northern District of California, Case No. 5:20-cv-02155-LHK, 28 July 2021) <https://www.zoommeetingsclassaction.com/Content/Documents/Settlement%20Agreement.pdf> accessed 14 August 2024.

49 In re: TikTok, Inc., Consumer Privacy Litigation, 'Order and Final Judgment' (US District Court for the Northern District of Illinois, Case No. 1:20-cv-04699, 1 December 2022) <https://angeion-public.s3.amazonaws.com/www.TikTokDataPrivacySettlement.com/docs/264-Order+and+Final+Judgment.pdf> accessed 14 August 2024.

50 *TransUnion LLC v. Ramirez* (Supreme Court of the United States), No. 20–297 (2021-06-25).

51 Fair Credit Reporting Act, Pub L No 91-508, 84 Stat 1114 (1970), 15 U.S.C. § 1681n.

52 *TransUnion LLC v Ramirez* [2021] USSC 16, 594 US 413 (2021), p 436 <https://www.supremecourt.gov/opinions/20pdf/594us2r59_197d.pdf> accessed 14 August 2024.

due to the nature of the activity that could cause harm. Courts both – in the EU and the US – put forward a general tendency that future harm that may occur as a result of a violation of data protection is not enough, and incurred harms shall be tangible. Having this in mind, the data protection field under Shavell's determinants does not necessarily prefer regulation to liability, as risks of facing class actions that could exceed the fine are relatively low because courts tend to critically evaluate harm under data protection regimes.

4. Administrative Costs

44 Administrative costs are one of the first things that organisations take into account while considering privacy-related risks and compliance policies. Therefore, it is crucial to understand administrative costs for estimating efficiency and social preference for the EU or US data protection models. The cost of the liability system must be broadly defined to include the time, effort, and legal expenses borne by private parties in the litigation or settlements and public expenses for trials. The administrative costs of regulation include the expense of maintaining state institutions performing regulatory functions and the private costs for compliance. The main difference is that, unlike under liability, administrative costs are incurred under regulation regardless of whether or not harm is caused.

45 Litigation costs in the EU and US differ significantly according to the International Comparisons of Litigation Costs report by NERA Economic Consulting.[53] Under this report, the US has the highest liability costs as a percentage of the gross domestic product of the countries surveyed, with liability costs at 2.6 times the average level of the Eurozone economies. In addition, US liability costs are four times higher than those of the least costly European countries in the performed study – Belgium, the Netherlands and Portugal. Considering this, it is fair to admit that the EU seems to be a more favourable jurisdiction in terms of litigation costs in the data protection field. However, as litigation costs depend on a number of factors outside of the scope of this article, further analysis focuses on the administrative costs of the data protection regulation models.

46 The background paper by Chander et al.[54] summarises a number of studies regarding the costs of compliance with data protection frameworks in the EU and the US. Chander et al.[55] show that the amount of incurred administrative costs favours *ex-post* liability to *ex-ante* regulation as administrative costs under compliance are always incurred while under liability, incurred only when the harm is done. Furthermore, compared to the EU, the US-chosen sectoral approach creates less overall administrative costs in terms of compliance. However, for actors in specific sectors (e.g., healthcare or finance), these costs are significantly higher than for actors in other fields in the US. Enforcement costs in the EU also supersede the costs in the US due to mandatory funding for Supervisory Authorities and excessive workload due to complaints and investigations under the GDPR.

47 It seems that Shavell's provided model of preference for *ex-ante* regulation and *ex-post* liability is applicable to compare the EU and US-chosen data protection frameworks if the reservations explained above are taken into account. The four determinants may not be applied blindly and have to be adjusted for each legal issue to benefit the evaluation of social preference. In terms of this research, we adjusted the general contents of Shavell's determinants and compared how each of them is reflected in the EU and US data protection regulation models:

53 U.S. Chamber of Commerce Institute for Legal Reform <https://instituteforlegalreform.com/wp-content/uploads/media/ILR_NERA_Study_International_Liability_Costs-update.pdf> accessed 22 December 2023.

54 Chander, Anupam and Abraham, Meaza and Chandy, Sandeep and Fang, Yuan and Park, Dayoung and Yu, Isabel, Achieving Privacy: Costs of Compliance and Enforcement of Data Protection Regulation (April 15, 2021). Policy Research Working Paper 9594. World Bank's World Development Report 2021 Team in collaboration with the Macroeconomics, Trade and Investment Global Practice. 2021. Georgetown Law Faculty Publications and Other Works. 2374., Available at SSRN: < https://ssrn.com/abstract=3827228 > or < http://dx.doi.org/10.2139/ssrn.3827228 >.

55 Ibid.

Determinant	The difference in knowledge about risky activities	The incapability of paying for the full harm done	Escaping the threat of suit for harm done	Administrative costs
Adjustments in the data protection field	-	The data protection field is closely related to imposing fines; therefore, organisations assess not only the sum of possible damages but also possible fines in different jurisdictions.	The risks of facing a class action are relatively low in the data protection field due to the nature of the activity that cxxould cause harm	-
EU	GDPR obliges Supervisory Authorities to possess more information than private parties on technological aspects to enforce the regulation. The regulator is often considered to have created too stringent rules for organisations that usually do not possess significant threats to individuals regarding their data.	Has established a more or less unified practice of imposing fines across the EU Member States	Courts both – in the EU and US – put forward a general tendency that future harm that may occur as a result of a violation of data protection is not enough, and incurred harms shall usually be tangible.	Enforcement costs in the EU supersede the costs in the US due to mandatory funding for Supervisory Authorities and excessive workload due to complaints and investigations under the GDPR.
US	The chosen US fragmentary approach to federal regulation reflects specific fields that require a higher standard of protection and provides examples where the regulator possesses more knowledge than private parties	The US jurisdiction is more abstract in terms of the possibility of fines		The US chosen sectoral approach creates less overall administrative costs in terms of compliance; however, for actors in specific sectors (e.g., healthcare or finance), these costs are significantly higher than for actors in other fields in the US

Table 2. S. Shavell's model applicability to EU and US data protection regulation models

48 The assumption that regulatory authority in the EU is omnipotent within the field of data protection is questionable. There are areas where the costs of accessing information are demonstrably lower for companies, challenging the notion of absolute regulatory control. In contrast, the fragmented regulatory approach of the US, particularly its emphasis on protecting more sensitive areas such as children's privacy, may offer a preferable model. Both jurisdictions face significant challenges in striking a balance between regulatory oversight and liability models, particularly in light of the complexities involved in determining optimal damages. This difficulty is exacerbated by the inherent challenges in quantifying harm within the data protection domain.

49 The nature of data breaches often allows entities in both the EU and the US to evade litigation for the harm caused, largely because proving tangible harm in this field is inherently difficult. Additionally, the high threshold for initiating class action lawsuits, especially in the EU, further complicates the pursuit of redress. The wide disperse of harm done in data breaches may be an argument for a regulatory approach such as in the EU. The overall administrative costs associated with data protection are relatively higher in the EU, particularly when compared to the more fragmented and less stringently monitored regulatory environment in the US. With these considerations in mind, we turn to the central question of this paper: can the application of the Shavell model to data protection regulatory frameworks in the US and the EU provide any valuable policy-oriented insights?

D. Can Economic Analysis of Law Solve the Rising Challenges in the EU and the US Data Protection Regulation Frameworks?

50 Our study shows that neither the data protection frameworks in the EU nor in the US perfectly balances *ex-ante* regulation and *ex-post* liability. On the contrary, recent proposals and policy changes in both jurisdictions suggest that the pursuit of social efficiency, alongside its compatibility with privacy protection, remains an on-going challenge.

I. What are the Challenges that Data Protection Regulation Models are Facing?

51 Both current data protection regulation models in the US and the EU face some severe criticism. As in any other disputable area of regulation, data protection raises concerns for both sides: privacy activists who claim that imposed regulation (or no regulation at all) is not sufficient to protect individuals from abuse of their data and companies operating in the data-related field, claiming that burden imposed on them regarding privacy cause more damage than adds to sufficient protection of persons.

52 Although the GDPR made a big shift in EU society's understanding of data protection, it still faces significant challenges. There is a widely spread opinion that GDPR has shown to be a costly and challenging burden on Europe's digital economy rather than functioning as a "golden" standard data regulation for the rest of the world to follow. Even though it is agreed that the GDPR has drawn significant attention to privacy-related issues, it has "proven to be costly, unmanageable, or prohibitively expensive without providing a commensurate privacy benefit".[56] Considering that the GDPR shortcomings are of core importance to demonstrate whether the chosen economic efficiency model in the EU is the most desired by the society, there are several GDPR issues highlighted by its critics that are relevant to our analys: (i) Most rules in the GDPR are formed as abstract principles and contain vague terminology;[57] (ii) The GDPR's complexities and responsibilities are carried most easily by the market's largest players;[58]

56 Canadian Marketing Association (CMA), 'Privacy Law Pitfalls. Lessons Learned from the European Union' (2022) <https://thecma.ca/docs/default-source/default-document-library/cma-2022-report-privacy-legislation-pitfalls.pdf?sfvrsn=ed54bdf4_6> accessed 22 December 2023.

57 Heiman argues that such vagueness is the opposite of the well-drafted law, in his view – this major data protection law lacks clarity surrounding its terms and, therefore, has fallen short, especially when it parallelly imposes a significant rise in the fine's regime. See Matthew R. A. Heiman, 'The GDPR and the Consequences of Big Regulation' [2020] Pepperdine Law Review, vol. 47, no. 4, 945.

58 Compliance expenses are insignificant for a major

(iii) GDPR creates complexity for consumers.[59]

53 GDPR may even be viewed as a protectionist instrument. "It has been noted that lifting restrictions, such as in data protection, would foster growth, including by increasing imports of digital services".[60] Such growth may lead to greater reliance on large non-EU businesses. In this way, stricter data protection laws could give domestic companies a competitive edge, aiding their global expansion.[61]

54 What are the concerns about the balance of efficiency and privacy standards in the US? For many years now, the US has raised the question of whether federal privacy law is needed in order to balance the interests of business freedom and privacy protection.[62] The support for the lack of unified federal data protection law mainly relies on the freedom of business and the possibility of using personal data almost unrestrictedly. In the current market model, processing personal data means more profit for technology-based organisations. More personal data – more possibilities to provide personalised advertisements, create customer profiles, and use other methods to increase sales or benefit otherwise. Besides, broad data protection regulation creates more limitations for technological developments.[63] For example, despite the intention of the technologically neutral text, GDPR is considered incompatible with many technological solutions, such as based on artificial intelligence or automated decision-making. For example, the GDPR emphasizes transparency, purpose limitation, and data minimization, which can conflict with how AI systems operate. AI often requires large datasets for training and improving accuracy, making it difficult to align with GDPR's restrictions on data collection and processing. As provided in the European Parliament study "a number of AI-related data protections issues are not explicitly answered in the GDPR, which may lead to uncertainties and costs, and may needlessly hamper the development of AI applications".[64] Following this, companies might choose to innovate less or pursue their ideas in less restrictive jurisdictions, such as the US.[65]

55 Despite clear advantages for business activity and advanced technological development, the US data protection framework faces severe criticism: among others are (i) the application, scope, enforcement, and sanctions of distinct sectora legislations and state-level rules vary greatly[66]; (ii) the regulation is often considered as not providing individuals with the necessary level of protection.[67]

corporation, but they are a significant burden for small and medium enterprises in the EU. It is even argued that users are less willing to experiment with new platforms and tools, preferring to remain with the "devil they know" regarding privacy compliance (see Layton R, 'The 10 Problems of the GDPR. The US Can Learn from the EU's Mistakes and Leapfrog Its Policy' (Statement before the Senate Judiciary Committee on the General Data Protection Regulation and California Consumer Privacy Act: Opt-ins, Consumer Control, and the Impact on Competition and Innovation, American Enterprise Institute, 2019).

59 it is argued that with the GDPR, consumer notices have become even more frequent and complicated, making it less possible for users to properly read the content and make informed decisions. See CMA (n 56) 16.

60 Martina F. Ferracane, 'The Costs of Data Protectionism.' In *Big Data and Global Trade Law*, ed. Mira Burri [2021] Cambridge: Cambridge University Press. chapter, 63–82.

61 Pascal D. König, 'Fortress Europe 4.0? An analysis of EU data governance through the lens of the resource regime concept' <https://onlinelibrary.wiley.com/doi/10.1002/epa2.1160> accessed 22 December 2023.

62 Kessler, J. 'Data Protection in the Wake of the GDPR: California's Solution for Protecting "the World's Most Valuable Resource"', (2019) 93/1 Southern California Law Review 99-128.

63 Ibid. p. 105.

64 European Parliament, 'The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence' (Study, 2020) https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2020)641530 accessed 10 October 2024.

65 CMA (n 56).

66 For example, the fact that the FTC *de facto* acts as the federal Supervisory Authority creates uncertainty for companies operating in the US. In many cases, the FTC has charged organisations with violation of Section 5 of the FTC Act, which prohibits unfair and deceptive actions and practices in or affecting commerce.

67 In 2016, Pew Research Centre (PRC) published a report stating that many Americans believe that tracking their online behaviour is in their best interests or that it is a price to pay for free or discounted products (Lee Rainie L and Maeve Duggan, 'Privacy and Information Sharing' (*Pew*

56 In the EU, the GDPR, while pioneering, imposes high compliance costs and extensive regulatory obligations that disproportionately burden smaller entities, creating what Shavell would view as an inefficient allocation of resources. The abstract nature of the GDPR's requirements, combined with its strict data protection mandates, supports Shavell's critique of regulatory error: the high risk of overregulation where harm potential is low, especially for smaller enterprises with limited data processing scopes. By failing to directly address new technological advances the GDPR inadvertently disincentivises technological growth within the EU, reinforcing Shavell's view that *ex-ante* regulations must evolve continually to reflect practical contexts.

57 In the US, the sectoral, fragmented regulatory approach offers flexibility and low compliance costs, arguably fostering innovation. However, this comes at the expense of consistent privacy protections, and the patchwork nature of US data laws results in regulatory gaps that may lead to public mistrust. Shavell's determinants suggest that this model risks underestimating the social cost of privacy harm due to its *ex-post* liability reliance, which may fail to deter data misuse effectively. Furthermore, the absence of a federal standard aligns with Shavell's notion that *ex-post* liability does not guarantee adequate preventative measures. The lack of uniformity across sectors and states means that while companies enjoy greater freedom, this freedom may result in less accountability and variable privacy standards.

II. How Do the EU and the US Jurisdictions Attempt to Consider Economic Efficienty?

58 The developments in recent years in the EU and the US suggest that, with or without intentional economic analysis of law, rule-makers in both jurisdictions understand the flaws of data protection frameworks. Therefore, recent legislative steps presuppose that jurisdictions have already taken steps to rebalance their data protection regulation approaches that encompass efficiency arguments.

59 A good example of the flawed European data protection framework and the possibilities to balance the interests of data subjects and organisations is the approach taken by the United Kingdom's authorities after Brexit. In the post-Brexit era, the regulator started consulting the stakeholders on implementing a more pro-growth and pro-innovation data regulation framework instead of the adopted UK GDPR.[68] According to the UK Information Commissioner, "(...) there are ways in which the legislation can be changed to make it simpler for companies to do the right thing when it comes to our data. Perhaps most notably, it is vital that the inevitable regulatory and administrative obligations of legal compliance are proportionate to the risk an organisation's data processing activities represent."[69] Currently, the UK Parliament is still in negotiations as to the chosen approach to balance the rights of individuals and regulatory certainty for organisations in order to boost the UK economy.[70]

Research Center: Internet, Science & Tech, 14 January 2016) <https://www.pewresearch.org/internet/2016/01/14/privacy-and-information-sharing/> accessed 22 December 2023.). Four years later, another PRC research found that about half of adults in the US (52 per cent) indicated they recently opted not to use a product or service because they were concerned about how much personal data would be gathered (see Andrew Perrin, 'Half of Americans Have Decided Not to Use a Product or Service Because of Privacy Concerns' (*Pew Research Center*, 14 April 2020) <https://www.pewresearch.org/fact-tank/2020/04/14/half-of-americans-have-decided-not-to-use-a-product-or-service-because-of-privacy-concerns/> accessed 22 December 2023).

68 *See* 'UK: ICO Welcomes DCMS Consultation Reviewing UK Data Regime' (*DataGuidance*, 7 October 2021) <https://www.dataguidance.com/news/uk-ico-welcomes-dcms-consultation-reviewing-uk-data> accessed 28 December 2023.

69 *See* ICO 'Ico Response to DCMS Consultation "Data: A New Direction"' <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2021/10/response-to-dcms-consultation-foreword/> accessed 28 December 2023.

70 The UK Parliament is currently in legislative stage of the new Data Protection and Digital Information Bill. *See* Data Protection and Digital Information Bill HL Bill (2023–24) 67 <https://bills.parliament.uk/bills/3430> accessed 31 October 2024.

60 Although data protection is now considered one of the main paradigms in the EU regarding the protection guaranteed to its citizens, the EU still significantly focuses on the economic side of regulation, maintaining its primary idea as an economic union (even though it had already shifted from these roots). Therefore, the approach to economic efficiency cannot be completely abandoned in the EU. The GDPR itself reflects that data protection is necessary for the proper functioning of the internal market[71] and that the activities of Supervisory Authorities in terms of enforcement of the GDPR shall also facilitate the free flow of personal data within the internal market.[72] Irrespective of the fact that GDPR applies directly in all the EU member states, as mentioned above, each national Supervisory Authority still has its own leeway towards the enforcement actions of the GDPR.

61 The recently adopted Digital Markets Act[73] (DMA) exemplifies the EU's effort to balance economic efficiency with data protection. Although the DMA does not function as a data protection law Baschenhof explains that the DMA aims to recalibrate data interactions in the EU by emphasising market objectives more strongly, particularly for reasons connected to fair competition.[74] For data collected by gatekeepers (core platform service providers), the DMA aligns partially with data protection goals by mandating fair practices.

62 While not a dedicated data protection law, the DMA contains several provisions[75] reflecting a "data as a resource", framing data as a market resource to promote competition. This approach may inadvertently lower privacy standards, despite requiring gatekeepers to comply with GDPR. Thus, the DMA reflects the EU's evolving approach, influenced by economic analysis, to balance business growth with data protection.

63 On the other side of the Atlantic, taking into account public opinion and changes in the international arena, the US returns to discussions on whether one federal law to rule all sectoral laws shall be adopted. There are many federal bill initiatives that deal with one or another aspect of federal privacy legislation in the US Congress.[76] The scholarship is divided into two camps – the one is for and the other is against the need to enact federal data protection legislation.

64 Kessler suggests that the US should adopt a federal standard that would grant consumers protection as strong as the GDPR or the California Consumer Privacy Act (CCPA).[77] Large technology businesses are concerned about having to comply with a patchwork system of regulations, which will likely be more expensive and burdensome than complying with a single state's law because other states are expected to follow California's lead and implement rules similar to the CCPA. Most businesses would reject legislation as harsh as the GDPR. Privacy activists claim that these businesses are just trying to pre-empt laws like the CCPA by establishing a diluted standard that is considerably less stringent than California's.[78] Privacy activists reject this strategy and have stated that they would fight attempts to pass a watered-down federal law that pre-empts state laws.[79] The disruption – pandemic-related issues like vaccine certificates, digital contact tracing, and mobile health apps – have helped put privacy and data security at the forefront of public debate, changing the public demand for federal privacy law.

65 There are certain advantages if the federal law is

71 GDPR (n 24) recital §21.

72 GDPR (n 24) recital §123.

73 Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector (Digital Markets Act) [2022] OJ L265/1.

74 Phillip Baschenhof, 'The Digital Markets Act (DMA): A Procompetitive Recalibration of Data Relations?'[2022] Journal of Law, Technology and Policy, Volume 2022, Issue 1, 101.

75 For example, DMA (n 72) Article 6(10).

76 International Association of Privacy Professionals, 'US Federal Privacy Legislation Tracker' (IAPP, 15 August 2023) https://iapp.org/resources/article/us-federal-privacy-legislation-tracker/ accessed 23 August 2024.

77 California Consumer Privacy Act of 2018 (CCPA), California Civil Code Section 1798.100.

78 Kessler (n 62), p. 123.

79 Joanna Kessler (n 62), 99.

enacted, including the ones related to economic efficiency. Rather than requiring consumers to parse through privacy policies and understand the nuances of various state laws, federal privacy legislation would clarify which baseline rights consumers are entitled to when it comes to safeguarding their data and ensure there are appropriate enforcement mechanisms in place. Comprehensive legislation at the federal level would benefit businesses. Rather than monitoring fifty different state laws and sectoral federal legislation and attempting to assess, interpret, and design frameworks that comply with each, federal legislation would provide a simplified framework for company compliance and help the companies to understand better privacy requirements and follow them. The latest developments in state-level enforcement also prove that federal law could provide more clearance for organisations. For example, in August 2022, Sephora Inc. reached a settlement of 1.2 million dollars with the California Attorney General for CCPA violations.[80] With one federal legislation, the enforcement actions would be more coordinated without the possibility for organisations to be fined for the same privacy practices in different states. Enforcement actions before organisations at a state level and rising possibilities to fine organisations by FTC may push the federal government to fasten the federal privacy legislation discussions.

66 The federal privacy legislation in the US could also benefit the economy. In the current global privacy scenery, compliance with privacy standards also makes brands more attractive to customers. Organisations tend to set at least minimal standards if no regulatory framework is in force. Therefore, adopting federal privacy legislation would promote data sharing with organisations subject to privacy standards, such as the GDPR, because data processed by US organisations would be more compatible with these standards. The fact that the EU has already created the data protection framework could benefit the US if it adopts a GDPR-style privacy law. Many American companies do business in the EU. Therefore, they are legally required to follow the GDPR. If the US privacy rules and regulations followed the GDPR's model closely, it would eliminate the necessity for organisations to develop a separate set of data protection measures for US customers.

67 While the US continues to negotiate federal legislation, some companies tend to keep aware and be proactive. Any legislation approved in the US will probably include elements of the GDPR, CCPA, other state laws. Rules on the use of AI-driven technologies, and other privacy and consumer protection areas will be included into regulation accordingly. Compliance with such standards will ensure a smoother transition when a general legislation is adopted in the US. The bottom line of the provided analysis is that irrespective of the chosen current regulatory approach - both jurisdictions aim to search for a long-term balance where economic efficiency plays a significant role.

E. Conclusion

68 Our analysis, grounded on the seminal work of Shavell, utilised efficiency-based arguments to evaluate whether an *ex ante* or *ex post* legal framework is more appropriate in specific regulatory contexts. We discovered that Shavell's classic model is instrumental in analysing current data protection regulations. While comprehensively accounting for all aspects of data protection regulation is challenging, our analysis suggests that the US data protection model more effectively enables data processing organisations to assess risks associated with potential data breaches compared to the EU legal framework.

69 The study shows that while the GDPR overextends regulatory scope, leading to inefficiencies for smaller entities, the US's fragmented model creates inconsistencies in privacy protection. Both the EU and US models face difficulties in ensuring that responsible organisations are held accountable for harm caused, largely due to the challenges in identifying harm in data protection violations. The potential for entities to evade legal consequences for such harm exists in both jurisdictions. This could be attributed to the complex burden of proof in the EU and the lack

80 *See* 'Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of California Consumer Privacy Act' (*State of California - Department of Justice - Office of the Attorney General*, 24 August 2022) <https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement> accessed 22 December 2023.

of clear recognition of harm in data protection violations in the US. The US model appears more favorable, considering administrative costs that constant and comprehensive monitoring in the EU entails. The US model benefits from less regulation and less intrusive oversight, which potentially makes it a more efficient framework for managing data protection concerns.

70 Although our analysis was limited to economic analysis of law, in particular, the model of Shavel, we found out how difficult it is to assess data protection in merely economic analysis of law realm. However, the actual need to minise costs of data protection regulatory frameworks grounds important efforts from both jurisdictions – the EU and the US – to find out better calibrated balance between *ex ante* regulation and *ex post* liability. The most prominent examples include the discussion on whether the differential approaches of national supervisory authorities may ensure better balanced application of GDPR in the EU; the Digital Markets Act as an attempt to balance company interests and privacy of consumers even more in the digital realm and the on-going discussion in the US to adopt federal comprehensive data protection regulation.

71 Our intention was not to deliver a definitive judgment on the superiority of either the US or EU data protection models. We looked whether the purely economic analysis of law based model might contribute to the better understanding of different data protection policies. The research provided insight into how efficiency driven considerations may better support more fragmented legislation such as in the US. The costs grounded rationale of data protection supports *ex post* liability as more preferred option.

72 However, the limitations of the model itself do not allow us to speculate on better policy recommendations. This is strongly related to data protection being primarily the policy developed under different conceptual framework than economic analysis of law, i. e. human rights. The economic analysis of law provides us with more generalised view on regulation costs, disregarding possible market deficiencies such as information asymmetry. The trade-off between economic efficiency and consumer protection is at the heart of data protection. Therefore, the chosen conceptual framework implicitly prioritise one or the other. Although rapidly developing data-driven markets requires us to rethink the way individuals must be protected from intrusion to their privacy, the economic realm should also not be ignored, taking into account better informed consumers who begin to acknowledge the value of their data and the potential to trade of this high-valued asset.

SEP Licensing Level in Value Chains with Emphasis on IoT and Connected Cars

by **Maryam Pourrahim** *

Abstract: The complexities of licensing in multi-tier value chains, notably within industries like connected cars, pose significant challenges. The pivotal question arises: Who should be responsible for obtaining licenses for Standard Essential Patents (SEPs) - Tier 1, Tier 2, Tier 3 suppliers, or end-product manufacturers?

The Daimler vs. Nokia case vividly illustrates the intricate web of connected car value chains, where three primary licensing alternatives were scrutinized. SEP holders typically prefer granting licenses to end-product manufacturers, based on the product's value. However, end-product manufacturers may challenge both the royalty base and the necessity of obtaining the license, advocating for the component supplier to be the licensee.

Conversely, component suppliers seek licensing, aiming to innovate and develop independently. Legally, SEP holders may hesitate to license component makers due to the first sale doctrine, which limits patent exhaustion within the value chain.

This paper meticulously examines the intricate issue of determining the rightful licensee in multi-tier value chains, leveraging insights from the Daimler case. Our analysis explores patent law, including concepts like the have-made right, FRAND commitments under ETSI, and competition law. We scrutinize the potential shifts in policy favoring licensing component suppliers, offering valuable insights into the complex landscape of SEP licensing in connected car industries.

Keywords: SEP, Licensing, FRAND, IoT, Value Chains

Recommended citation: Maryam Pourrahim, SEP Licensing Level in Value Chains with Emphasis on IoT and Connected Cars, 15 (2024) JIPITEC 288 para 1

A. Introduction and Setting the Context

1 The intricacies surrounding licensing levels in multi-tier value chains present a formidable challenge, particularly in industries such as connected cars. Within these intricate chains, the fundamental question arises: Who should bear the responsibility of acquiring a license for Standard Essential Patents (SEPs) - Tier 1, Tier 2, Tier 3 suppliers, or end-product manufacturer?

2 The *Daimler vs. Nokia* case[1] vividly exemplifies the intricate web of connected car value chains, where three primary licensing alternatives were

* PhD in IP and Competition Law. TILEC. Tilburg University. Netherlands. Email: pourrahim85@gmail.com

1 The Mannheim Regional Court's second Civil Chamber on 18 August 2020 (Decision 2 O 34/19, available at: http://eplaw.org/wp-content/uploads/2020/10/DE-2-O-34_19-URT-Allgemeines-Urteil-FINAL_ANONYMISIERT.pdf.) [hereinafter: Mannheim judgment]; the Munich I Regional Court's 7th Civil Chamber on 30 October 2020 (Decision 21 O 3891/19, available at: https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=LG%20M%FCnchen%20I&Datum=3; 0.10.2020&Aktenzeichen=21%20O%203891%2F19.) [hereinafter: Munich judgment]; and the Düsseldorf District Court on 26 November 2020 (Decision 4c O 17/19, available at: https://www.justiz.nrw.de/nrwe/lgs/duesseldorf/lg_duesseldorf/j2020/4c_O_17_19_Beschluss_20201126.html.). The case number before the ECJ is C-182/21. [hereinafter: Düsseldorf judgement]. The District Court of Düsseldorf decided to stay the proceedings and requested further guidance from the ECJ. Nokia

under scrutiny. These alternatives hold different preferences among involved parties. SEP holders ideally prefer granting licenses to end-product manufacturers, based on the end-product's value. However, the end-product manufacturer might challenge not only the royalty base but also the necessity of obtaining the license. They could argue that the appropriate licensee should be the component supplier providing the SEP-integrated component, advocating that the component price itself should be the royalty base.

3 Conversely, component suppliers, often spanning multiple tiers, may stake their claim for a license. Their aim extends beyond legally furnishing the 4G component for end-product manufacturing; they seek the freedom to innovate and develop independently, potentially selling to other clients. However, they are unlikely to agree to pay royalties based on the end-product's value, challenging this as an appropriate base.

4 But legally why is it that SEP holders are not willing to license at component makers' level? The answer should be sought in the *first sale* doctrine (also known as *patent exhaustion*), which acts as a defence against a claim of patent infringement in value chains.[2] Under this doctrine, once a patentee grants licence to some tier in a value chain, he cannot succeed on a claim that a subsequent user or purchaser of the article infringes the patent. It is because a patentee can license only *once* in the production chain *per* patent, either to the component or to the end-product manufacturer.[3] The first licensed sale of patented products exhausts patent rights. Therefore, if a SEP holder gives licences to a component maker, he will be prevented from future attempts to extract royalties from downstream purchasers of the component including the end-product manufacturer who is economically a more interesting client for the SEP holder.[4]

5 In this paper, our goal is to meticulously examine and address the intricate issue of determining the rightful licensee in multi-tier value chains, leveraging the insights and complexities detailed through the lens of the Daimler case.

I. Structure of Value Chain in Connected Cars

6 Nokia initiated a legal action against Daimler, alleging patent infringement concerning a vital data transmission method for Long Term Evolution (LTE), the fourth-generation mobile communications standard regulated by the 3rd Generation Partnership Project (3GPP), under

Technologies Oy vs. Daimler AG (Case C-182/21), Request for a preliminary ruling from the Landgericht Düsseldorf (Germany), lodged on 23 March 2021. Available at: https://curia.europa.eu/juris/document/document.jsf;jsessionid=380BD291C5D9D971330D7A64BE50965A?text=&docid=243511&pageIndex=0&doclang=en&mode=doc&dir=&occ=first&cid=620502. [hereinafter: Nokia vs. Daimler, Request for a preliminary ruling]. For an English translation of the referral decision. See: https://curia.europa.eu/juris/showPdf.jsf?text=&docid=240963&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=3837153.
It is also worth noting that the request for a preliminary ruling was removed from the register as Nokia and Daimler concluded a licensing agreement for the use of Nokia's mobile patents by the German car manufacturer. The terms of this agreement remain confidential as agreed between the parties. See: ECLI:EU:C:2021:575, available at: https://curia.europa.eu/juris/liste.jsf?lgrec=fr&td=%253BALL&language=en&num=C-182/21&jur=C).

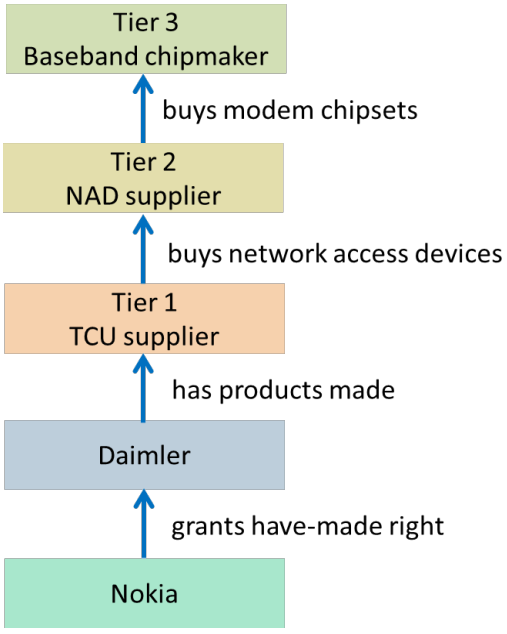
2 *Quanta Computer, Inc. vs. LG Electronics,* Inc., 553 U.S. 617 (2008). The court stated that *"[t]he longstanding doctrine of patent exhaustion provides that the initial authorized sale of a patented item terminates all patent rights to that item*".

3 Anne Layne-Farrar and Richard J. Stark, 'License to All or Access to All? A Law and Economics Assessment of Standard Development Organizations' Licensing Rules', George Washington Law Review, 88.6 (2020), 101–42 <https://doi.org/10.2139/ssrn.3612954>. P. 114.

4 One may wonder could one prevent patent exhaustion if the SEP holder grant royalty free licence to the component maker and a licence to end-product manufacturer with the argument that by this the patentee's right will not be exhausted. (See Justus Baron and others, 'Group of Experts on Licensing and Valuation of Standard Essential Patents "SEPs Expert Group" (E03600) Contribution to the Debate on SEPs' <https://ec.europa.eu/docsroom/documents/45217>. P. 92). The answer is negative as this argument was once repelled by the US Supreme Court in LifeScan Scotland, Ltd. vs. Shasta Technologies as the Court held that patent exhaustion principles apply to all authorised transfer whether it be by sale or as a gift, and that in the case of an authorised and unconditional transfer of title, absence of consideration is no barrier to the application of patent exhaustion principles. (See *LifeScan Scotland, Ltd. v. Shasta Technologies*, LLC, 734 F.3d 1361 (Fed. Cir. 2013). At 1375 and 1376).

European Telecommunications Standards Institute's (ETSI) umbrella. Nokia notified ETSI in 2014 about its patent application's importance to the LTE standard and issued a FRAND commitment, pledging to offer licenses under fair and reasonable terms to third parties.

7 Daimler, a renowned German automaker, provides diverse mobility and financial services, including vehicles equipped with Telematics Control Units (TCU). These TCUs enable internet connectivity via the LTE network, allowing users access to services like satellite navigation, music streaming, and over-the-air updates without dealership visits. Crucially, TCUs facilitate the required emergency call system (eCall), enhancing vehicle safety and user experience. The TCUs are not manufactured by Daimler itself, but as shown below, in a multi-tier production chain. Daimler obtains the TCUs from its direct suppliers (Tier 1 suppliers). The Tier 1 suppliers, for their part, obtain the NADs (Network Access Devices) required to produce the TCUs from other suppliers (Tier 2 suppliers). The Tier 2 suppliers in turn receive the chips they need for the NADs from Tier 3 suppliers. After the Tier 1 supplier provides the TCU to the Original Equipment Manufacturer (OEM), it is integrated into the vehicle. The broadband chipset enables cellular communications, while downstream equipment handles other functions beyond cellular standards.



Chain structure in connected car

8 The litigation between Nokia and Daimler began in 2019 following a failure in the initial negotiations between the car manufacturer and the mobile company. Daimler and some of its suppliers including Continental, Huawei, Burry, and TomTom, complained to the European Commission that Nokia was exploiting its market power with its SEPs.[5] Nokia initiated a counter-offensive, suing Daimler for infringement of several patents at the regional courts of Mannheim, Munich and Düsseldorf. Then invalidity suits against Nokia patents were brought at the European Patent Office and the German Federal Patent Court. Daimler and its suppliers had emphasised that not the car manufacturer, but rather its Tier 1 and Tier 2 suppliers should take the Nokia patents licence, while Nokia had long refused this.[6]

9 While Germany's competition authority, the Bundeskartellamt, had recommended in June 2020 for the Mannheim Court to pause the proceedings and seek guidance from the ECJ regarding the appropriate level of licensing for SEPs, it did not

5 See: Foo Yun Chee, 'Daimler Asks EU Antitrust Regulators to Probe Nokia Patents' (*REUTERS*) <https://www.reuters.com/article/us-eu-daimler-nokia-patents/daimler-asks-eu-antitrust-regulators-to-probe-nokia-patents-idUSKCN1RA2KF>.

6 In the course of negotiations Nokia was relatively flexible with regard to licensing level, as it once offered a limited license to the tier 1 suppliers. However, it could not resolve the problem as Nokia were insisting on an end-product royalty base that was rejected by Daimler and its suppliers (Daimler argued for a licence to its suppliers and based on the average purchase price of TCUs. See: Mannheim judgment. (n 1). In July 2019, Nokia presented the Connected Vehicle Value Chain Licensing Model (CVVL) as a supplement to the tier 1 Model. Under this model, suppliers would be granted a limited license for research and development and for the production of a connected car. They would also provide a license to their customers, who would be entitled to produce a TCU via a have-made right provided at upstream. Following a hearing at the Düsseldorf court in 2020, Nokia made another licensing offer known as the Automotive Licence Agreement (ALA) to several tier 1 suppliers, including Continental, Bosch, Bury, TomTom, Peiker, Renault, Harman, Fico Mirrors, and Huawei. The offer provided unrestricted licenses to manufacture and distribute TCUs, as well as licenses for the car manufacturer's customers and any other customers of the suppliers. However, the tier 2 supplier Sierra Wireless, which had applied for a license, was not offered by Nokia.

occur[7] until March 2021 when the Düsseldorf Court referred the case to the ECJ. The referral sought clarification on ten detailed questions, the main one being: *"[i]s there an obligation to license suppliers on a priority basis?"*[8] This was a great chance to see the ECJ's judgment on this delicate issue, however, it failed as the parties were able to conclude a licensing agreement.

II. Research Objective and Approach

10 The main objective in this paper is to see whether any related branch of law can provide some legal basis to define a certain level of licensing in value chain or to definitely exclude a certain level. Obviously, the problem of licensing does not stem from the mere legal concerns, but it is certainly the financial aspects of the problem that are much more important. In fact, the licencing level is a matter of debate because it is directly or indirectly related to the royalty rate.

11 In practice, three primary licensing options are possible. The first option is a licence to the end-product manufacturer at an end-product rate, which is mostly the SEP holders' preference. The second is a licence to component suppliers at a component-based rate, which is mostly the end-product manufacturer's preference. The third is a licence to the component manufacturer at an end-product rate which is also demanded by SEP holders.

12 These options were exactly the principal offers and counteroffers exchanged in the *Nokia vs. Daimler* case[9] (*Daimler*). By focusing on this case and through investigating different branches of law, we aim to examine the problem of licencing level and royalty base in multi-tier value chains. This objective is met through exploring those parts in any branch of law that can somehow help resolve the level definition problem either in a positive (affirmative) or negative manner. That is to say that whether and which legal source may suggest or exclude one level (either component or end-product).

13 It should be noted that the provided study is driven such that any borderless and lengthy discussion is avoided, and for this, we fix our scope within the boundary of the three main offers exchanged between the parties and the three judgements provided in the *Daimler case*.

14 This study falls within the purview of European jurisdiction, with the primary focus directed towards European law, encompassing both EU law and national law. In instances where there is no relevant EU law, such as when interpreting the ETSI contract, reference is made to the provisions of national law, exemplified by the French Civil Code.

15 However, in certain specific contexts, particularly when exploring aspects related to have-made rights, the study incorporates insights from US jurisprudence. This inclusion is motivated by the advanced and diverse nature of US legal precedents, as well as their prominent status in the literature. Omitting reference to US case law would render the discussions incomplete, given its substantial relevance and contribution to the overall understanding of the subject matter. We, however, believe that the findings drawn from US case law are also applicable to the EU context.

B. Level of Licencing Problem

16 In this paper the question of level of licencing is treated through examining it from the perspective of patent law, FRAND commitment, and competition law.

17 In each topic, we collect those parts that are related to this question. Such a relation can be either in an affirmative manner, where any above-mentioned legal sources designate a certain level as the right licensee, or in a negative manner where they exclude a level from the right or possibility of having licence. In some topics such as patent claims and exhaustion, the findings may only suggest an efficient level rather than imposing a legal duty. Regardless,

7 See: Mathieu Klos, 'Federal Cartel Office Issues Opinion in Connected Cars Case' (*JUVE*, 2020) <https://www.juve-patent.com/cases/federal-cartel-office-issues-opinion-in-connected-cars-case/>.

8 *Nokia vs. Daimler*, Request for a preliminary ruling. (n 1). P. 2.

9 (n 1).

we will focus on the offers made by the parties in *Daimler* and the courts' judgments in this very case, as justified earlier.

I. Patent Law

18 Patent law is not directly concerned with licensing since a patent confers a negative right to exclude others from practicing the invention, rather than an affirmative right to practice it. However, we examine patent law to determine if the key principles derived from it could help address the issue of level of licensing. For this purpose, we start with investigating the capacity of have-made right in determining the licencing level. Then, we discuss if patent claim and patent exhaustion can suggest an appropriate tier of value chain as a true licensee.

1. Have-Made Right

19 Nokia's offer to only license Daimler and not its suppliers was based on the legal justification that licencing to the end-product manufacturer along with have-made rights can be sufficient to protect Daimler's suppliers from any patent infringement claim. Due to its importance in *Daimler*, and its capacity in responding to our question about licensing level, have-made rights will be discussed in detail in this section to understand its conditions and limitations, and to see whether it can be an effective means for protecting component suppliers against possible infringement.[10]

a.) Definition of Have-Made Right

20 The concept of have-made rights shares similarities with the German legal concept known as the *extended workbench*. Under the extended workbench concept, a licensed manufacturer can have components of the licensed product produced by a third party under its directions. In this study, we primarily rely on US cases due to their greater number, diversity, and development. However, it is important to note that a similar approach would likely apply in the EU as well. Analysing have-made rights provides a foundational understanding of how the concept of the extended workbench can be interpreted in the European context.

21 According to the US case law,[11] a licensed party who has the right to "have products made", can exercise his right by requesting an unlicensed third party to manufacture the product but return it *solely* to the licensee who can either use it for his purpose or sell it out in the market.[12] The unlicensed party is protected under this arrangement, but the licensee is only permitted to have the product made for himself though he can sell it later.[13] The US courts articulate

10 When it comes to evaluating the essence of a license agreement, the assessment ultimately depends on the applicable law in each jurisdiction. However, regardless of the jurisdiction, what matters most is how licensing is carried out in practice, especially in the context of a complex value chain.

11 Under the US case law there are two factual circumstances where unlicensed parties can attain rights that shield their actions from infringement. The first scenario is have made right. The second which is called foundry suggests that an unlicensed third party can give his design (in the form of technical drawings, plans, etc.) to a licensee and ask him to use his rights to manufacture the product, then either sell it out directly in the market under his licence or sell it back to the third party for that he resells it to his customers. Once the product was made and sold by the licensee to the third party, the doctrine of patent exhaustion precluded the SEP holder from suing the unlicenced third party. The *Intel Corp. vs. ULSI Sys. Tech., Inc.*, 995 F.2d 1566 (Fed. Cir. 1993) is an example of this scenario where HP was given a license by Intel to be a foundry for certain computer chips, to manufacture and sell them to third parties. Another company, ULSI, designed its own, similar chip, and asked HP to manufacture it. HP did so, at this point Intel sued ULSI for infringing Intel's patents, as ULSI had obtained no license from Intel. The Court held that because HP had manufactured the chips, and because at the time it did so it held a license to the patents, therefore it was a legitimate source of the chips, no infringement had occurred and every sale of ULSI chips were lawful and thus exhausted those patents.

12 *Cyrix Corp. vs. SGS-Thomson Microelectronics*, 77 F.3d 1381 (Fed. Cir. 1996). At 1387-88.

13 The *Cyrix* case is the example of this scenario where the third-party (ST-Italy) manufactured microprocessors under ST's have-made rights, and ST then properly sold the products to a different entity, Cyrix. The two agreements, one permitting ST-Italy to manufacture microprocessors for ST and the other providing for ST's sale of microprocessors to Cyrix, were separate business transactions. The court found that ST was using both its own facility and ST-Italy's to satisfy its obligation to provide microprocessors to Cyrix. The products manufactured by ST-Italy were made for ST. Therefore, the arrangements among ST, ST-Italy, and Cyrix

that a have-made right is derived from the term "to make" set forth in 35 U.S.C § 271 (a), that provides that a licensee with have made rights possesses the right to request an unlicensed third-party to manufacture a licensed good for the licensee.[14]

22 The relatively recent decision of *TCL vs. Ericsson* precisely explains the necessary conditions when a have-made right can be granted: (a) the licenced party owns and supplies the *designs*, *specifications and working drawings* supplied to the third party; (b) such designs, specifications and working drawings are complete and sufficient so that no substantial additional design, specification and working drawings are needed by the third party; and (c) the third party is not allowed to sell such product to other third parties.[15] It then concludes that as long as the *design* is carried out fully by the licensee, the manufacture can be fulfilled by any third-party including tier 1, tier 2 and so on.

23 In this context, the distinction between *design* and *manufacture* is of essential importance. What have-made rights mean is, in fact, to have the third party manufacture the product not to have him both design and manufacture. In some cases, like those related to metal production, design (method) and manufacture are not separable[16] but, in most cases including telecommunication technology they are two separate processes. This is also the case in connected car.

b.) Evaluation of Have-Made Rights

24 After having provided a definition for have-made right and its fulfilment conditions, we need to know if it can work well and effectively in practice. To get this purpose, we examine it critically through the existing literature and case law.

(aa) Scope

25 Geradin criticises the effectiveness of the have-made right approach arguing that it does not allow component makers to have some components manufactured by suppliers higher in the supply chain (tier-2 or tier-3).[17] However, US case law holds a different perspective. In *Carey*, the court ruled that the have-made rights permit the licensee to engage *others* to do all the work connected with the production of the licensed article for him.[18] A license to produce, use, and sell is not limited to personal production, use, or sales by the licensee. It allows the licensee to employ others to assist in the production, use, and sale of the invention. Nor need he take any personal part in the production.[19] The court explained that the legal effect of have-made rights flow from the licensor to the licensees and down to the third-party manufacturer before the third party engages in any of those otherwise infringing acts. In this context, it is more reasonable to believe that the manufacturer is not limited only to the upstream operator immediately above the end-product manufacturer, but any third-party suppliers (tier 1 to 3) are included provided that the principal condition emphasised in *TCL vs. Ericsson* case is met.

(bb) Explicit or Implicit

26 In the US, case law indicates that have-made rights are among the exclusionary rights outlined in the patent statute. However, unless otherwise stated in the grant clause, the right to make, use and sell a licensed product inherently includes the implied

were a valid exercise of ST's have-made rights under its agreement with Intel.

14 For e.g., see *Cyrix Corp. vs. Intel Corp.*, 77 F.3d 1381 (1996) and *Intel Corp. vs. Broadcom Corp.*, 173 F. Supp. 2d 201 (D. Del. 2001).

15 *TCL Commc'n Tech. Holdings, Ltd. vs. Telefonaktiebolaget LM Ericsson*, CASE NO: SACV 14-341 JVS(DFMx) (C.D. Cal. Mar. 9, 2018).

16 In the *Carey* case, the patented process of manufacturing titanium was licensed, and the licensee had titanium "manufactured" by a third party. *Carey vs. United States*, 326 F.2d 975 (Fed. Cir. 1964).

17 He argues that component makers are excluded from extended workbench since they are not considered part of the extended bench of the licensed OEM/end -product manufacturer. Damien Geradin, 'SEP Licensing After Two Decades of Legal Wrangling: Some Issues Solved, Many Still to Address' (2020) DP 2020-04 TILEC Discussion Paper.

18 *Carey vs. United States*, 326 F.2d 975 (Fed. Cir. 1964). At 979.

19 *Idem.*

right to have those licensed products made by a third party. In the *Star* case, for example, Star used third-party contractors to manufacture licensed products for its own use. CoreBrace (the patentee) argued that such use of third parties was a violation of the licence agreement, as Star (licensee) did not have the right to have a third party make products for them.[20] The court, however, ruled that Star did not breach the licence agreement by using third-party contractors to make the licensed products.[21] The court reasoned that even when a licence agreement prohibits sublicensing, have-made rights are still granted unless they are expressly prohibited.[22] The court explained that a licence to produce, use, and sell a product inherently includes the right to have it made by a third party, and have-made rights are implicit in the right to make, use, and sell, unless there is a clear and explicit contrary intent.[23]

27 It is worth mentioning that the have-made right is explicitly included in the ETSI IPR policy. Therefore, there is no doubt regarding its applicability in the context of *Daimler*.

(cc) Legal Certainty

28 Have-made rights may not provide component makers with adequate legal certainty as they indirectly protect them, i.e., their legal position is dependent of that of the licensed end-product manufacturers, meaning that if the latter lose their licence, the component makers could be susceptible of infringement claims. However, we recognize that such uncertainty is almost inevitable in a multi-tier supply chain, as there is only one licence per patent for the entire chain.[24] Thus, both end-product manufacturers and component makers may feel such an uncertainty.

(dd) Innovation and R&D Concerns

29 By limiting the activity of component makers to only manufacturing at the direction of end-product manufacturers, the scope for their independent research and development may be restricted. This could result in a reduced ability for the component makers to invest in new technologies, innovate and offer new improved products to the market. However, many countries have research exceptions in their patent rules.[25] These exceptions also exist at the international level.[26]

30 It must be noted that although the availability of research exceptions can provide some relief to component makers in short term, in the long run their usefulness may be limited. For example, if a tier 1 supplier finds an alternative use for a patented technology, they may eventually need a licence to exploit it. Moreover, the availability of research exceptions may not be sufficient to encourage

20 *Corebrace LLC vs. Star Seismic LLC*, 566 F.3d 1069 (Fed. Cir. 2009).

21 *Ibid.* At 1071.

22 *Idem.*

23 *Ibid.* At. 1073.

24 See discussions provided later for patent exhaustion.

25 Most the EU Member States have adopted statutory exceptions. Article 27(b) of the Community Patent Convention (CPC) states that: "*[T]he rights conferred by a Community patent shall not extend to... [the] acts done for experimental purposes relating to the subject-matter of the patented invention*". German case law shows that the research exemption is not limited to pure scientific research and can also cover the development of new consumer products. Siebrasse and Culver refer to the Clinical Trials I and II (Klinische Versuche [1997] RPC 623 (Bundesgerichtshof and [1998] RPC 423) where the court ruled that "*Since the provision makes no limit, either qualitative or quantitive on the experimental acts, it cannot matter ... whether they are employed for wider purposes, such as commercial interests. And, of course, on the facts, the use found to be experimental was aimed ultimately at the commercial purpose of developing and marketing a new indication for the drug in question*". Similarly, in Clinical Trials II, the court stated (at 433) that "*the purpose that the experiment is intended to serve does not at all have to be of a purely scientific nature. According to this, the commercial orientation does not from the outset turn the experimental activity into an impermissible patent infringement*." Norman Siebrasse and Keith Culver, 'The Experimental Use Defence to Patent Infringement : A Comparative Assessment' (2006) 56 The University of Toronto Law Journal 333 <https://www.jstor.org/stable/4491699>.

26 For example, article 30 of the TRIPS Agreement allows for research exceptions stating that "*Members may provide limited exceptions to the exclusive rights conferred by a patent, provided that such exceptions do not unreasonably conflict with a normal exploitation of the patent and do not unreasonably prejudice the legitimate interests of the patent owner, taking account of the legitimate interests of third parties.*"

component makers to invest in long-term research. Patent holders may still have significant leverage over them, and the threat of patent infringement litigation may deter component makers from investing in new technologies and innovations.

(ee) Competition Concern and Commercial Freedom on Open Market

31 If have-made right becomes the norm, it may lead to concerns about competition, since suppliers are only able to manufacture components for the end-product manufacturer but are not legally allowed to develop, manufacture, and distribute the components independently.

32 In the *Daimler* case, the Munich and Düsseldorf courts did not share the same view on competition concerns stemming from the have-made right solution. The Munich court observed that the suppliers without their own licence are not completely without rights, they do have a right to legally secure access to the standardised technology. It ruled that Daimler is easily able to have LTE standard-compliant supplier parts manufactured by its suppliers in the future by means of extended workbench and thus grant them legally secure access to the technology licensed by Daimler.[27] On the contrary, the Düsseldorf court placed significant emphasis on the challenge faced by component makers operating under the extended workbench without a comprehensive licence. The court contended that such a limitation could hinder their economic activity, curtail their ability to explore new markets, and potentially lead to higher prices that eventually will reduce consumers' choice. The issuance of a licence must extend beyond mere access to the standardised market. Instead, a licence should encompass the provision of opportunities for the licensee to engage fully in standardised technology. This must enable them to compete unrestrictedly across all product markets, both current and future[28].

33 It is noteworthy to reference the EU Commission Notice on the assessment of subcontracting agreements.[29] This Notice affirms the legality of the extended workbench concept under EU competition law. Specifically, it states that any extended workbench agreement and its restrictive clauses between the contractor (in our case, Daimler) and the subcontractor (Daimler's suppliers) do not fall under the scope of Article 101(1) TFEU. In essence, this notice supports the argument that if the conditions for have-made rights are met, a licensor is not obligated to license component makers, as it is considered legally permissible under competition law.

2. Patent Claim

34 The other patent law element that has potential of significance in terms of the licencing level is the subject of patent claim.

35 By definition, the protection of patents shall be determined by the terms of the claims.[30] Here a helpful indication is that if *all* the elements of a patent claim are shown to exist in a component with not even one single element missing,[31] the claim is said to be infringed.[32] This condition is a sufficient condition in the sense that if in addition to having all the patent elements, the component has also some extra elements which are not related to the patent, the patent is still considered infringed.[33]

36 But how can this help determine the licensing level? To answer this, it will make sense if we believe that

27 See Munich judgement, (n 1).

28 See Düsseldorf judgement, (n 1).

29 European Commission, Commission notice of 18 December 1978 concerning its assessment of certain subcontracting agreements in relation to Article 85 (1) of the EEC Treaty. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31979Y0103(01)>.

30 European Patent Convention (EPC 1973), Article. 69.

31 *TIP Systems, LLC vs. Phillips & Brooks/Gladwin, Inc.,* 529 F.3d 1364 (Fed. Cir. 2008). At. 1377.

32 *Markman vs. Westview Instruments, Inc.,* 517 U.S. 370, 373 (1996). At 373-374.

33 *A.B. Dick Co. vs. Burroughs Corp.*, 617 F. Supp. 1382 (N.D. Ill. 1985). At. 1398. In a simple example, for claim of the widget X composed of the elements 1, 2, and 3, a widget with elements 1, 2, and 3 would infringe, as would a widget with elements 1, 2, 3, and 4. On the other hand, a widget with elements 1 and 3, but lacking 2, would not infringe.

one way for a component maker to insist on getting a licence (or for the end-product manufacturer to insist on refusing the licence offer) is to show that the component in question involves all the elements of the SEP's claim. In such a case, the component maker can show himself as the right licensee. On the other hand, if the SEP's claim is so broad that it applies to a combination of multiple components of the end-product, then the SEP holder has a legitimate reason to want to grant license to the end-product manufacturer.[34]

37 It should be noted that SEPs are often licensed as a portfolio, consisting of hundreds or even thousands of patent families. Additionally, a single SEP may cover multiple technologies, which can lead to overlap between the patents used by different suppliers. As a result, the SEP holder would need to ensure that all suppliers are licensed to use only the relevant patents for their specific component and that no unlicensed patents are being used. Therefore, the licensing process can be complex and require lengthy negotiations between the patent holder and the potential licensees to determine which patents are essential to the standard and the appropriate licensing terms and conditions.

38 This finding is important for our study on the licensing level as it suggests that in complex standards such as cellular, there may be many SEPs involved that may not be reduced to a single component.[35] Therefore, these SEPs would not be infringed until when all the components sharing them are incorporated at the end-product level. In other words, a component can indirectly infringe the SEPs once it is inserted in the end-product and puts the SEPs into effect. In this case, making use of a patent claim to identify the licensing level yields to the SEP holder's favourite choice, i.e., suggesting the end-product manufacturer as the right licensee. It is worth saying these complex situations apply specifically to cellular standards and the smartphone industry. The situation may vary in other standards and industries. Therefore, a thorough case-by-case analysis of each standard and SEP is required to determine whether infringement occurs at the component or at the end-product level, and to be able to suggest one level as licensee.

39 It must be noted that this finding is not a legal basis for requiring granting licence at one level or another, however, it makes clear which level may be more efficient and reduce transaction costs.

3. Patent Exhaustion

40 Typically, and as seen in the *Daimler* case, the end-product manufacturers try to place the licence at the component supplier level to make it possible for everyone down in the chain including the end-product manufacturer (Daimler) to use the components (TCU) free from any patent rights. Conversely, the patentee (Nokia) who prefers to licence at the end-product level, is very attentive not to licence at any level above the end-product. Patent

34 Now if an infringement occurs at the component level, the SEP holder has still the option to license the patents or consent to infringement without seeking to enforce his rights. If he decides to offer licence, he is free to set the terms and conditions as he sees fit. (see: *McCoy vs. Mitsuboshi Cutlery, Inc.*, 67 F.3d 917, 920 (Fed. Cir. 1995). At. 922. However, the FRAND commitment restricts options available to him since he has agreed to make his patents accessible to standard users and offer licenses on FRAND terms. As a result, he cannot exclusively reserve implementation rights for himself.

35 In a study by Putnam and Williams, they analysed Ericsson's SEPs portfolio for 2G/3G and 4G standards and found that the claims of Ericsson's SEPs portfolio read on many components alone, components in combination, complete handsets alone, and/or complete handsets in networks. Their analysis showed that around 71% of Ericsson's patents claimed some aspect of user equipment, either alone or in combination with claims to the network, while none of them claimed only the baseband chip. See: Jonathan D Putnam and Tim A Williams, 'The Smallest Salable Patent-Practicing Unit (SSPPU): Theory and Evidence' [20166] SSRN Electronic Journal.U.S. courts have begun to require that litigating parties base patent infringement damages on sales of the "smallest salable patent-practicing unit," or SSPPU, in an effort to constrain the patentee's damages claim to the true "economic footprint" of the invention. We ask whether this legal requirement can be grounded in economic theory, industry licensing practices, or the scope of actual patent claims. We find significant theoretical reasons to reject the mandatory imposition of the SSPPU rule, because the economic impact of an invention is not, in general, limited to the sales price of an input that allegedly embodies it. In the telecommunications industry, where the SSPPU rule has assumed additional policy significance in the context of FRAND commitments by owners of standard-essential patents (SEPs Pp. 41-43.

exhaustion[36] further reinforces this preference, as it is a one-way road downward in the supply chain, and not upward meaning that if the patent holder licenses the end manufacturer, the component maker would still need a separate licence to make and sell the patented component to other manufacturers or end users.

41 Against this background, one may conclude that patent exhaustion can suggest the component maker level as the right licensing level, since such a choice makes licensing more efficient as by adopting it there would be no need for further licensing downstream.[37] Although, this could be an option in simple-structured value chains, in complex chains including those related to the cellular, the outcome goes in the opposite direction as licensing the end-product manufacturer can be more efficient. Because in a SEP portfolio with multiple patents, if a component supplier receives a licence, it will only exhaust the relevant part of the SEP portfolio. The end-product manufacturers may still require a licence for the remaining patents that read on the downstream products.[38] This split licensing would be difficult and therefore it appears that having only one licence at the end-product level is much more efficient as in that level most of the patents in the portfolio are infringed and exhausted by the sale of the licensed product.[39]

42 However, licensing only at the end-product level raises the question of what would happen to the component makers without a licence, as they would still be infringers. Borghetti et al., argue that if the patent owner chooses not to pursue component makers in this case, it implies that the owner is not willing to exercise its exclusionary right against them, and have made rights safeguard them against patent infringement.[40]

4. Takeaway

43 Determining the appropriate licensee within a multi-tier value chain is beyond the scope of patent law. Patent law primarily defines the rights held by a patent holder and outlines actions that require authorisation. It does not, however, dictate which parties must engage in licensing agreements or under what circumstances. Nonetheless, it may offer guidance or recommendation for efficient licensing levels. In fact, patent law's role is primarily suggestive, rather than prescriptive when it comes to defining licensing levels.

44 To summarise this section, we can draw the following conclusions:

- If its conditions are fulfilled, most importantly that the end-product manufacturer is the body who completely performs the design of the IoT component, the have-made right serves as a tool that can suggest end-product level as the right licensing level.
- In industries related to cellular, since a single component often exhausts a SEP portfolio partially, attempt for making use of patent claim as a tool to define licensing level may lead to the recognition of end-product manufacturer as licensee.
- Since a licence relevant to a part of a SEP portfolio only exhausts that part, licensing at component maker level may lead to licensing

36 As discussed previously, the first sale doctrine also known as patent exhaustion acts as a defence against claim of patent infringement in value chains. Once a patentee gives license to some tier in a value chain, he cannot succeed on a claim that a subsequent user or purchaser of the article infringes the patent.

37 Damien Geradin and Dimitrios Katsifis, 'End-Product- vs. Component-Level Licensing of Standard Essential Patents in the Internet of Things Context', SSRN Electronic Journal, 2021, 1–34 <https://doi.org/10.2139/ssrn.3848532>. at p. 11 share the same view arguing that if the majority (or possibly all) of SEPs are implemented for the first time at an earlier stage (such as the chipset level), licensing at this level would not lead to additional transaction cost and would not involve multiple levels of licensing. This is due to the principle of patent exhaustion, which would provide immunity to operators further down the chain.

38 Jean-Sébastien Borghetti, Igor Nikolic, and Nicolas Petit, 'FRAND Licensing Levels under EU Law', European Competition Journal, 2020, 1–48 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3532469>. P. 17

39 *Ibid.* P. 18.

40 *Idem.*

split. Therefore, licensing at this level is not efficient.

II. FRAND Commitment

45 As a contractual obligation, FRAND commitment should be examined by reference to the wording of each tandards Development Organisation'a (SDO) IPR policies under which the commitment has been made. However, the current policies are not in harmony with each other, and there is an absolute lack of consensus regarding their interpretation. The Institute of Electrical and Electronics Engineers (IEEE) mandates SEP holders to license their SEPs to all parties including component suppliers.[41] The situation with the ETSI is less clear, as some interpret the ETSI IPR policy as requiring SEP holders to license their patents to component suppliers, while others disagree.[42] The lack of specific case law on this issue has further complicated the debate, with proponents of each approach interpreting the SDOs' policies to suit their arguments.

46 This section evaluates the legality and the feasibility of Daimler's counteroffer to Nokia which suggested a direct licencing to the tier 1 suppliers. We want to examine if SEP holders are obliged, based on their FRAND commitment to carry out such a licencing agreement rather than giving licence to the end-product manufacturer. To answer this, we examine the ETSI's IPR policy including its FRAND commitment to check if there exists any technical reason[43] for SEP holders to prefer one tier of the value chain over the others. It is worth saying that in our research, we focus solely on the analysis of the ETSI IPR policy as it serves as the basis for the FRAND commitment in the majority of SEP litigations including our *Daimler* case.[44]

1. ETSI IPR policy, Annexe 6, Article 3

47 Adopted in 1994, ETSI policy in Article 3 provides,

> "[...] STANDARDS and TECHNICAL SPECIFICATIONS [should] be available to potential users in accordance with the general principles of standardisation".[45]

48 If one recognises licensing as the *only way* to make SEP available to a potential user (i.e., a component maker), then of course this article is requiring the SEP holder not to refuse the supplier's request for licence. However, the dispute lies in the interpretation of the word *availability* with some arguing that it can only

41 IEEE-SA Standards Board Bylaws 2022.

42 In favour of the "licence to all" approach, see e.g., Karl Heinz Rosenbrock, 'Why the ETSI IPR Policy Requires Licensing to All', 2017.; Damien Geradin and Dimitrios Katsifis, 'End-Product- vs. Component-Level Licensing of Standard Essential Patents in the Internet of Things Context', SSRN Electronic Journal, 2021, 1–34 <https://doi.org/10.2139/ssrn.3848532>; Roberto Grasso, 'Standard Essential Patents: Royalty Determination in the Supply Chain', Journal of European Competition Law and Practice, 8.5 (2017), 283–94 https://doi.org/10.1093/jeclap/lpw089>; Tim W. Dornis, 'Standard-Essential Patents and FRAND Licensing-at the Crossroads of Economic Theory and Legal Practice', Journal of European Competition Law and Practice, 11.10 (2020), 575–91 <https://doi.org/10.1093/jeclap/lpaa047>; In favour of the "access to all" approach see e.g., Bertram Huber, 'Why the ETSI IPR Policy Does Not and Has Never Required Compulsory License to Alll: A Rebuttal to Karl Heinz Rosenbrock', SSRN Electronic Journal, 2017, 1–12 <https://doi.org/10.2139/ssrn.3038447>; Jean Sébastien Borghetti, Igor Nikolic, and Nicolas Petit, 'FRAND Licensing Levels under EU Law', European Competition Journal, 17.2 (2021), 205–68 <https://doi.org/10.1080/17441056.2020.1862542>; Anne Layne-Farrar and Richard J. Stark, 'License to All or Access to All? A Law and Economics Assessment of Standard Development Organizations' Licensing Rules', George Washington Law Review, 88.6 (2020), 101–42 <https://doi.org/10.2139/ssrn.3612954>; Marvin Blecker, Tom Sanchez, and Eric Stasik, 'An Experience-Based Look At The Licensing Practices That Drive The Cellular Communicatinos Industry: Whole Portfolio/Whole Device Licensing', Les Nouvelles - Journal of the Licensing Executives Society, LI.4 (2016) <ssrn: https://ssrn.com/abstract=2855078>.

43 By technical reason, we refer to all technical aspects of the patent and its implementation, and the way those aspects may affect the licensing process for different tiers of the value chain.

44 The number of SEPs reported to ETSI surpasses all those declared to any other SDOs, see: Chryssoula Pentheroudakis and Justus A Baron, 'Licensing Terms of Standard Essential Patents. A Comprehensive Analysis of Cases' (2017) <https://ec.europa.eu/jrc>. P.31.

45 Article 3 of ETSI states that: "the ETSI IPR POLICY seeks to reduce the risk to ETSI, MEMBERS, and others applying ETSI STANDARDS and TECHNICAL SPECIFICATIONS, that investment in the preparation, adoption and application of STANDARDS could be wasted as a result of an ESSENTIAL IPR for a STANDARD or TECHNICAL SPECIFICATION being unavailable."

be achieved through licensing, while others contend that it refers to accessibility in general that is not limited to mere licensing.[46]

49 To unlock the situation, the French law as the governing law of the ETSI IPR Policy[47] must be used to interpret any of its vague contractual terms.[48] The French Civil Code's Article 1190[49] states that "*in case of doubt, an agreement shall be interpreted against the one who has stipulated, and in favour of the one who has contracted the obligation*". In this context, SEP holder is the one who has committed to the obligation, and he may believe that accessibility favours him rather than licensing.[50] Hence, attempts to oblige the SEP holder to license the component maker based on this article fails.

2. ETSI IPR Policy, Annex 6, Article 6

50 According to Article 6 of Annex 6, in case of essential IPR related to a particular standard or technical specification, the IPR owner should provide the following.

> [A]n irrevocable undertaking in writing that it is prepared to grant irrevocable licences on fair, reasonable and non-discriminatory ("FRAND") terms and conditions under such IPR to at least the following extent:
>
> MANUFACTURE, including the right to make or have made customized components and sub-systems to the licensee's own design for use in manufacture; sell, lease, or otherwise dispose of EQUIPMENT so manufactured, repair, use, or operate EQUIPMENT, and use METHODS.[51]

51 The policy then defines the meaning of the term *manufacture* as the production of *equipment* and the latter as "any system, or device fully conforming to a standard". However, *device* and *system* have not been defined. The uncertainty is about whether the term *equipment* implies the mere end-product device, or whether it includes components as well. As discussed above, based on our interpretation of the French Civil Code, Article 3 will let the SEP holder interpret the vague terms including *equipment* here in his favour. And he will opt for a choice which favours him the most, i.e., licensing the end-product manufacturer based on the end-product price. In addition, the use of the words *at least* and *including* is not convincing to believe that the ETSI text includes component suppliers.

52 However, if one wants to go farther, he may utilise Article 1188 of the French Civil Code that suggests contracts are to be interpreted according to the common intent of the parties, rather than the literal meaning of the terms. If such an intent cannot be ascertained, the contract should be interpreted in accordance with the meaning that a *reasonable person* in the same situation would give to it. Identifying

46 See the list of literature at (n 42).

47 Article 12, ANNEX 6:ETSI Intellectual Property Rights Policy 2022.

48 ETSI as an *association* (a non-profit organisation) under French law is a type of contract governed by French contract law and according to the reform of 2016 is governed by the old code civil as it has concluded before 1st October 2016. See, *ordonnance n°2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations.* Available at: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000032004939.

49 Available at: https://www.trans-lex.org/601101/_/french-civil-code-2016/.

50 Where an IPR holder gives a commitment under Clause 6.1 of the ETSI IPR Policy, the IPR holder is the "promisor"; and ETSI is the "stipulator/ promisee". A person wishing to implement the standard is the "beneficiary". The primary effect of the declaration is to create a contract between the promisor (the IPR holder) and the stipulator (ETSI), the terms of which require the promisor to grant a right (a licence on FRAND terms) to the beneficiaries (the implementers of the standard). According to Judge Briss, ETSI's blank form constitutes an offer, and a properly filled form acts as acceptance, specifying the chosen pre-defined options in line with ETSI's offer. The form explicitly references Clause 6.1 of the ETSI IPR Policy for future contracts, ensuring that such contracts will adhere to FRAND terms. Courts can objectively determine whether terms are FRAND in a given context, making the commitment legally enforceable. Judge Briss also highlighted that the FRAND commitment, sought by ETSI when patentees declare their patents as essential to an ETSI standard, benefits third parties. As a result, the "stipulation pour autrui" doctrine makes the FRAND commitment enforceable by third parties. See: [2017] EWHC 711 (Pat). Paras. 134-140. Available at: https://www.judiciary.uk/wp-content/uploads/2017/04/unwired-planet-v-huawei-20170405.pdf.

51 ANNEX 6: Intellectual Property Rights, ETSI Intellectual Property Rights Policy.

the common intent of the ETSI members at the time of adopting the policy back in 1994 appears to be challenging.[52] For example, in 2017, Rosenbrock, the former Director-General of ETSI, stated that the common intention was a general commitment to license any SEP user whether component maker or end-product manufacturer. He argued that this view is aligned with ETSI's objective of making ETSI standards available to members and other stakeholders.[53] But another former member of the ETIS IPR committee, Huber, countered Rosenbrock's argument by suggesting that the common intention of ETSI policy drafters was based on the prevailing industry practice of granting licences to end-product manufacturers.[54] This shows well how attempts to reveal the then-common intent of the ETSI members fails.

53 The last attempt in this direction would be to determine the interpretation of a *reasonable person*. Such person should have adequate knowledge of the telecommunications industry in the 1990s allowing him to interpret the term *equipment* in the context of the ETSI IPR policy. This approach leads to an impasse too as there is no consensus over the common industry practices in the ETSI.[55] Therefore, wording of ETSI does not limit the beneficiaries of the licence, nor limits the SEP holders' freedom in choosing their licensees in a supply chain.

3. Discussion on SDOs' Role

54 With the rise of IoT and the increasing use of ETSI connectivity standards in various sectors, an official policy clarification from ETSI can help determine if the SEP holder under the ETSI FRAND commitment is obliged to licence component makers.

55 For example, the IEEE's revised patent policy in 2015 resolves this ambiguity for their standard users. Under the IEEE revised policy, the FRAND commitment explicitly states that the licensor must provide an unrestricted licence to an unlimited number of applicants including component makers for essential patent claims. This licence allows the licensees to make, use, sell, offer to sell, or import any compliant implementation conforming to the IEEE standard. A *Compliant Implementation* refers to any product or service that adheres to any mandatory or optional part of an IEEE standard, including *components.*[56] Thus, the SEP holder who made the FRAND commitment at IEEE cannot decline to license its patents to component manufacturers when they request.[57]

56 ETSI, in contrast, does not provide an official policy clarification regarding this issue. As a result, the ambiguity surrounding ETSI's licensing policies allows for more clashes in the literature. Borghetti et al. refer to an ETSI Director General's speech[58] expressing that "*specific licensing terms and negotiations*

52 The absence of a shared understanding among the drafters at the time has reflected in the policy's voting base as it was determined by a majority vote rather than by a consensus.

53 Rosenbrock (n 42) 3-4.

54 Huber (n 42). He explains the history and reasoning for his view that the obligation to license under the ETSI IPR Policy, once a commitment is given to license at fair, reasonable, and non-discriminatory (FRAND pp. 4-5 and 8). Huber also argues that an IPR Policy mandating that SEP owners grant licenses to component markets would be legally and practically unworkable, in that (a) it would be impossible to grant the same license to the same technology to companies operating at different levels by reason of patent exhaustion; (b) such a system would be inefficient and unfair, and would make it hard to account for the full economic value that the patented technology confers on the end-product; and (c) such a system would hinder the ability of IPR holders to fully obtain the benefits of the "reciprocity" condition in the ETSI IPR Policy.

55 While Huber argues that at the time the ETSI IPR Policy was adopted, the prevailing industry practice was to license at the device level, and Becker et al. at p. 230 and Borghetti et al. at p. 30 share the same view arguing that whole-device licensing is an efficient and universally accepted norm in the cellular communications industry; Rosenbrock refer to the examples of Qualcomm and Ericsson granting licenses at the chipset level, arguing that the description of end-product licensing as the prevailing industry practice is not correct nor consistent with the author's own experience of discussions in ETSI.

56 See: § 6 IEEE-SA Standards Board Bylaws.

57 According to the Clause 6 of the IEEE Standards Board Bylaws, an Accepted Letter of Assurance is intended to be binding upon any and all assignees and transferees of any Essential Patent Claim covered by such LOA.

58 Borghetti, Nikolic and Petit (n 38) 24.

are commercial matters between the companies and shall not be addressed within ETSI".[59] Meanwhile, Huber,[60] referring to ETSI's General Assembly meeting, reports that ETSI's Director of Legal Affairs states that ETSI's IPR policy does not require essential patent owners to grant licences at the "smallest saleable unit", leading some to argue that ETSI is clearly refusing the requirement to license to component suppliers.[61] On the other hand, Geradin and Katsifis argue that ETSI aims to balance the interests of IPR owners and standardisation requirements through FRAND licences. This aim is attained only through a direct licence to component makers, the ETSI policy does not consider *access* as distinct from licensing, and its alternatives (including have- made right) may not provide legal certainty or support the objective of ETSI Policy.[62]

57 In summary, the ETSI IPR policy being vague, it opens the door for contradictory interpretations. In our view, a clear policy such as that of the IEEE, even if it may be criticised,[63] is better than a vague one.

III. Competition Law

58 In this section, we explore whether SEP holders are obliged under the EU competition law to grant a licence to component suppliers rather than to end-product manufacturers. Our goal is to determine if Nokia's refusal to grant licences to Daimler's suppliers can be deemed an abuse under Article 102 TFEU.

59 There is currently no formal view or decision from the ECJ nor the EU Commission regarding FRAND licencing in multi-tier value chains, and in fact, it was just in the *Daimler* case that the Düsseldorf court asked the ECJ for a preliminary ruling on the level of licensing and any obligation to prioritise licenses for suppliers.[64] However, the case got settled following the parties' agreement before the ECJ's ruling.[65] We then analyse this question under the most recent ruling of the ECJ on the SEPs: the *Huawei* case,[66] where *indispensability condition* and *legitimate expectation* were addressed. In this context, the question we will try to examine is whether the *Huawei* doctrine could apply to the *Daimler* context. This subject has been already tried by some scholars.[67] Nevertheless, our contribution addresses the problem from novel perspectives that can enhance the literature particularly in the sections of legitimate expectation and licence denial as an exclusionary abuse. Additionally, we examine this question under the non-discrimination principle, and explore any potential guidance that can be provided by the Commission Horizontal Guidelines.

1. Huawei Doctrine

60 Freedom to deal or not to deal is a foundation of freedom of trade. Companies are free to choose with whom they want to do business and to dispose of their property including IPR.[68] These freedoms as fundamental rights are guaranteed by the EU Charter of Fundamental Rights.[69] As a matter of fact, the exercise of a statutory right cannot constitute

59 Sophia Antipolis, 'ETSI's Director General Issues Public Statement on IPR Policy' (2018) <https://www.etsi.org/newsroom/news/1458-etsi-s-director-general-issues-public-statement-on-ipr-policy>.

60 Huber (n 42) p. 6.

61 ETSI/GA(15)65_030r2, ETSI, 'Draft Minutes from the ETSI General Assembly' <https://portal.etsi.org/ngppapp/ContributionSearchForm.aspx?tbid=&SubTB=&Param=&MeetingId=15538>.

62 Geradin and Katsifis (n 37) pp. 25-26.

63 See some critics regarding the revised IEEE Policy: 'Will IEEE Finally Admit the Errors of Its 2015 Patent Policy Changes?' (*IP Europe*, 2021) <https://ipeurope.org/blog/will-ieee-finally-admit-the-errors-of-its-2015-patent-policy-changes/>; Keith Mallinson, 'Development of Innovative New Standards Jeopardised by IEEE Patent Policy' [2017] 4iP Council <https://www.4ipcouncil.com/application/files/6015/0479/2147/Mallinson_IEEE_LOA_report.pdf>.

64 *Nokia vs. Daimler*, Preliminary Ruling. (n 1).

65 ECLI:EU:C:2021:575. See (n 1).

66 Case C-170/13 *Huawei Technologies Co. Ltd vs. ZTE Corp.*, EU:C:2015:477. (hereinafter: *Huawei*)

67 See for e.g., Borghetti, Nikolic and Petit (n 38) pp. 6-11 and pp. 35-40

68 Opinion of AG Jacobs in Case C-7/97 *Oscar Bronner GmbH & Co. KG vs. Mediaprint*, EU:C:1998:264. Para. 56.

69 Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012. p. 391-407. Article 16 and 17.

an abuse of a dominant position.[70] In this context, the SEP holder is free to choose his business partner to grant a FRAND licence. However, according to settled case law,[71] the exercise of a statutory right may, in *exceptional circumstances*, involve abusive conduct for the purposes of Article 102 TFEU. In *Volvo*, *Magill*, *IMS Health*, and *Microsoft* the court had established conditions for identifying exceptional circumstances where a *refusal* to deal would be deemed abusive.[72] This subject was then discussed by the ECJ in 2015 specifically in the context of SEP. The ECJ in fact, established a shortcut analysis for identifying exceptional circumstances in the SEP context where refusal to license could be considered abusive. Thanks to the *Huawei* ruling, it is no longer necessary to scrutinise all the conditions outlined in *Volvo*, *Magill*, *IMS Health*, and *Microsoft.* Instead, the Court in *Huawei* ruled that a SEP is *indispensable* to the manufacturer of a standard-compliant product, and, in addition, the FRAND commitment creates *legitimate expectations* for every SEP implementer.[73]

61 Therefore, in our analysis of *Daimler* under the *Huawei* doctrine, we will demonstrate how the conditions of indispensability and legitimate expectations can be applied concerning the refusal to grant licenses to component manufacturers. However, as we will discuss later, the *Huawei* conditions are necessary but not sufficient, and therefor, an additional step is required to assess if the denial of licence could be an abusive practice in the case of *Daimler*. Ultimately, we will propose a policy change that imposes an obligation to grant licence to component manufacturers.

a.) Indispensability Condition

62 There is no distinction between the indispensability of SEPs at the component level and at the end-product level. SEPs are equally essential to component manufacturers for producing and selling components as they are to end-product manufacturers for integrating the component into their final product and selling it.[74] The ECJ in the *Huawei* case emphasised that the user of an IPR, "*if he is not the proprietor, is required to obtain a licence prior to any use*".[75] Without a licence, the SEP users will be under the constant threat of an infringement claim, an injunction, or the recall of products from the market. As component makers cannot operate *lawfully* without a licence, this makes the use of SEP indispensable to every SEP implementer including component maker. Thus, the indispensability condition is undoubtedly fulfilled in *Daimler*.

b.) Principle of Legitimate Expectations

63 The ECJ in *Huawei* ruled that commitment to grant licence on FRAND terms creates legitimate expectations on the part of third parties that the SEP holder will in fact grant licences on such terms.[76] Given that the principle of legitimate expectations has been always referred to in cases where one party is a public authority,[77] we need to examine if based on the *Huawei* judgement such an expectation could be

70 *Huawei* judgement. (n 66) para. 38.

71 Judgment of the Court of 5 October 1988, *AB Volvo vs. Erik Veng* (UK) Ltd, Case 238/87, ECLI:EU:C:1988:477 (hereinafter: *Volvo*);Judgment of the Court of 6 April 1995, *Radio Telefis Eireann (RTE) and Independent Television Publications Ltd (ITP) vs. Commission of the European Communities,* joined cases C-241/91 P and C-242/91 P, ECLI:EU:C:1995:98 (hereinafter: *Magill*); and Judgment of the Court (Fifth Chamber) of 29 April 2004, IMS *Health GmbH & Co. OHG vs. NDC Health GmbH & Co. KG*, C-418/01, ECLI:EU:C:2004:257 (hereinafter: *IMS Health*); Judgment of the Court of First Instance (Grand Chamber) of 17 September 2007.*Microsoft Corp. vs. Commission of the European Communities,* T-201/04, ECLI:EU:T:2007:289 (hereinafter: *Microsoft*).

72 While these conditions are challenging to categorise, generally, it was determined that a dominant company's refusal to supply could be considered abusive if: 1-The product or service in question is indispensable to operate in the relevant market; 2-There is no viable alternative to the product or service; 3-The refusal is likely to eliminate all competition in the relevant market; 4-The refusal would eliminate all competition in the market for the new product; 5-The refusal to license IPRs prevents the appearance of a new product for which there is a potential consumer demand; 6-The refusal to license is not objectively justified .

73 *Huawei* judgement (n 66) para. 49 and 53.

74 Renato Nazzini, 'Level Discrimination and FRAND Commitments under EU Competition Law' (2017) 40 World Competition 213. Pp. 229-230.

75 *Huawei* judgement (n 66) para. 58.

76 *Huawei* judgement (n 66) para. 53.

77 Borghetti, Nikolic and Petit (n 40) pp. 6-7.

still proved legitimate when the parties involved are private entities. What can help us in this direction is that the ECJ in *Huawei* expressed legitimate expectations without any reference to the previous cases. If we can believe that it was intentional, it can certainly represent a new application for this principle between the private entities.

64 Borghetti *et al.* do not believe in such an intention.[78] They argue that according to the EU settled case law (i.e., those actually were not referred to by the ECJ in the *Huawei* case), the principle of legitimate expectation as a general principle of EU law[79] is limited to the sectors where the EU exerts a significant degree of regulatory control to protect economic agents against the State,[80] and even in those cases, the principle has been rarely invoked successfully.[81]

65 In addition, they argue that this principle could have been established if the basis for the expectation had been adequately *specific* and *precise.*[82] For them, any expectation of third party should be assessed based on the SDOs' IPR policy and the specific FRAND commitment thereof. For example, if a SDO in its policy states that FRAND means royalty-free or pricing based on the Smallest Saleable Patent Practicing Unit (SSPPU), then any licensing offer deviating from these terms could disappoint a potential licensee that expects a licensing based on those terms.[83] But if the SDO's policy does not require any specific licensing condition, as it is the case in ETSI's policy, a FRAND commitment cannot be regarded as a *reliable source*[84] to create legitimate expectation.[85]

66 Against Borghetti et al., we consider SDOs, their IPR policies, and FRAND commitment thereof as reliable sources that serve as a basis for members to determine how to develop standards.[86] We also distinguish a mere expectation to obtain a licence from the expectation to obtain it on specific FRAND terms. We believe that what the ECJ ruling safeguards in *Huawei* is the former, and for that end the Court set a detailed framework to guarantee access to licence for any willing licensee. In other words, obtaining a FRAND licence is a legitimate expectation of SEP implementer, but the specific terms of such a licence can be established later through parties' negotiations or by third parties.[87]

78 They argue that reference to the protection of legitimate expectations in a private setting in Huawei is decorative, but not dispositive. Ibid pp. 6-8.

79 They refer to the *Schenker & Co and Others*, C-681/11, ECLI:EU:C:2013:404, which concerned the legal advice of a lawyer arguing that previous cases refuse the idea that the private entities can create legitimate expectations *vis-a-vis* other private entities. Ibid. Pp. 10 and 38.

80 Eleanor Sharpston, 'European Community Law And The Doctrine Of Legitimate Expectations : How Legitimate , And For Whom?' (1990) 11 Northwestern Journal of International Law & Business 87 <https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1312&context=njilb>. P. 90.

81 Borghetti, Nikolic and Petit (n 38) p. 7.

82 *Ibid*. P. 9. They refer to the case *Citymo vs. Commission* (T-271/04, EU:T:2007:128, §138), where the General Court stated that only "*precise, unconditional and consistent information*" can lead third parties to entertain legitimate expectations.

83 *Ibid*. P. 10.

84 In the *Branco vs. Commission* case, the Court ruled that three conditions must be satisfied in order to claim entitlement to the protection of legitimate expectations: "*precise, unconditional and consistent assurances originating from authorized and reliable sources*" must have been given to the person claiming to have a legitimate expectation, which "*give rise to a legitimate expectation on the part of the person to whom they are addressed*". Case T-347/03 *Branco vs. Commission*, ECLI:EU:T:2005:265. Para. 102.

85 Borghetti, Nikolic and Petit (n 38) p. 10. For the opposite view, see Geradin and Katsifis (n 37) p. 33.

86 Borghetti et al., argue that previous cases within the realm of competition law appeared to reject the notion that private entities could establish legitimate expectations in relation to other private organisations. They refer to the Court ruling in *Schenker* (*supra fn.* 101) where it stated that "*legal advice given by a lawyer cannot, in any event, form the basis of a legitimate expectation on the part of an undertaking that its conduct does not infringe Article 101 TFEU or will not give rise to the imposition of a fine*". Nonetheless, we disagree with this comparison and share the idea of Geradin and Katsifis emphasising the fact that any comparison between a legal advice provided by a lawyer to a client and the FRAND commitment made by members of a SDO is not accurate. The FRAND commitment serves as a basis for members to determine how to develop the standard and cannot be equated with individual legal advice given by a lawyer to a client. See: Geradin and Katsifis (n 37) pp. 33-34.

87 We believe that this is what the ECJ ruled and not an expectation about a detailed FRAND licence. That is why,

67 We believe that in *Huawei* the ECJ dispositively applied the principle of legitimate expectation to a case involving two private entities,[88] as the Court did explicitly refer to it twice which cannot be interpreted *decorative* at all:[89]

> "53 In those circumstances, and having regard to the fact that an undertaking to grant licences on FRAND terms creates legitimate expectations on the part of third parties that the proprietor of the SEP will in fact grant licences on such terms, a refusal by the proprietor of the SEP to grant a licence on those terms may, in principle, constitute an abuse within the meaning of Article 102 TFEU.
>
> 54 It follows that, having regard to the legitimate expectations created, the abusive nature of such a refusal may, in principle, be raised in defence to actions for a prohibitory injunction or for the recall of products. However, under Article 102 TFEU, the proprietor of the patent is obliged only to grant a licence on FRAND terms. In the case in the main proceedings, the parties are not in agreement as to what is required by FRAND terms in the circumstances of that case."

68 In addition, this application seems not bizarre nor unprecedented. The Commission also referred to this principle in the *Rambus*[90] and the *Motorola* cases,[91] where the EC stated that given the standardisation process resulted in the GPRS standard, and Motorola's voluntary commitment to license the Cudak SEP on FRAND terms, those implementing the GPRS standard have a legitimate expectation that Motorola offers them a licence for that SEP, as long as they are willing to agree to FRAND terms and conditions.

69 Furthermore, to ensure effective access to the standard, the Commission in the revised Horizontal Guidelines refers to the legitimate expectations of the standard implementers laid out in *Huawei* and *Motorola.*[92]

70 Based on the *Huawei* ruling, we believe that FRAND commitment creates two legitimate expectations.[93] First, the SEP holder's FRAND commitment creates *substantive* legitimate expectations for potential licensees, who anticipate obtaining a licence on FRAND terms. If the SEP holder, then refuses to

---

the Court ruled that if parties cannot reach an agreement on FRAND terms, third parties may intervene. The ruling mandates SEP holders to provide a written offer for a FRAND licence, and potential licensees to respond to that offer in good faith. If the parties cannot come to an agreement, they may seek the intervention of a court or an arbitration panel to determine the specific FRAND terms.

88 Just because there has not been any prior case law on legitimate expectation in the private sector does not mean that there could or should not be. Case law is established as a result of factual circumstances and not vice versa.

89 Borghetti, Nikolic and Petit (n 38) at p. 8 argue that the protection of legitimate expectations in a private setting in *Huawei* is decorative, but not dispositive.

90 *Rambus* [2010] OJ L30/14. [hereinafter: *Rambus*]. Para. 38.

91 The Commission in para. 417 of the Motorola states that "In view of the standardisation process that led to the adoption of the GPRS standard and Motorola's voluntary commitment to license the Cudak SEP on FRAND terms and conditions, implementers of the GPRS standard have a legitimate expectation that Motorola will grant them a licence over that SEP, provided they are not unwilling to enter into a licence on FRAND terms and conditions"; in para 521 also states that: "Apple and other manufacturers of GPRS-compliant products that are not unwilling to enter into a licence on FRAND terms and conditions should therefore be able to rely on the legitimate expectation that Motorola will honour its commitment to license the Cudak GPRS SEP on FRAND terms and conditions. The seeking and enforcement of an injunction by Motorola against Apple in Germany on the basis of the Cudak GPRS SEP runs counter to that commitment". Case AT.39985 – Motorola, 29 April 2014, C(2014) 2892 final.[hereinafter: Motorola]

92 Communication from the Commission, Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements, C/2022/1159, OJ C 164, 19.4.2022, p. 1–121. [hereinafter: revised Horizontal Guidelines 2022]. Para. 482.

93 In the literature there is no agreement whether FRAND has procedural or substantive meaning. Borghetti, Nikolic and Petit (n 38) at p.9, argue that the ECJ does convey a procedural understanding of FRAND and the procedural legitimate expectations. They argue that the FRAND framework is a comity device that creates mutual obligations of fair play between both the patent owner and potential licensees. Lundqvist describes these obligations as "*good governance procedural rules*", which suggests that they promote ethical and transparent practices in patent licensing. Björn Lundqvist, 'The Interface between EU Competition Law and Standard Essential Patents–from Orange-Book-Standard to the Huawei Case' (2015) 11 European Competition Journal 367. P. 389.

license, it can be viewed as a violation of those legitimate expectations, especially when the potential licensee has relied on that expectation when making his business decisions. Secondly, there are *procedural* legitimate expectations for him, as he expects fair negotiations, access to information, and the right to present his case before a neutral third party if a dispute arises. The ECJ has provided a framework for FRAND negotiations to ensure fairness and balance.[94] Failure to meet these expectations may be seen as a violation.

71 In line with us, Geradin and Katsifis claim that as the reference of the ECJ to legitimate expectations on the part of third parties is phrased indiscriminately to the benefit of *any* third party, it could be read as a basis for the proponent of imposing licensing at component maker level.[95]

72 We therefore conclude that component makers have a legitimate expectation to obtain a licence from SEP holders, if they comply with the procedural framework outlined by the Court. With this in mind, we still need to move one step forward and examine whether the refusal to grant licences to component makers could be considered an abuse under Article 102 TFEU. The reason for this further examination lays in the difference between the facts of *Huawei* and *Daimler*. In the case of a vertically integrated SEP holder, as in *Huawei,* the risk of harm per Article 102 TFEU may be evident (exclusion of competing implementers). But how about the *Daimler* context, where the SEP holder is a non-vertically integrated entity, i.e., if it is only active in the licensing of technology and not in the manufacture of end-products at the market at issue? This question, studied below, makes more sense as one may argue that the fulfilment of the conditions mentioned in *Huawei* may be *necessary* but not *sufficient* to justify a competition law duty to license (rather than a contract law duty). If this is the case, contract law would be the right vehicle to address the refusal of the SEP holder in breach of its FRAND commitment.[96]

94 *Huawei* judgment (n 66) para. 55.

95 Geradin and Katsifis (n 37) pp. 32-33.

96 *Idem*.

c.) Licence Denial as an Exclusionary Abuse

73 In *Huawei*, whenever the Court referred to the liability of the SEP holder, it considered him as vertically integrated in the market who could , by refusal to licence, keep the production of the product for himself. In paragraph 52 of *Huawei*, the Court highlighted that by preventing products manufactured by *competitors* from appearing or remaining on the market, the SEP holder can *reserve to himself* the manufacture of the products in question. The Court then concluded that "*in those circumstances*", the conduct may in principle constitute an abuse.[97] Therefore, the refusal to grant a FRAND licence was viewed as an *exclusionary* abuse, thereby a violation of Article 102 TFEU.

74 But in the *Daimler* case, the SEP holder is not vertically integrated in the market. This is worth mentioning because in *Huawei* (*Motorola*[98] and *Samsung,*[99] as well), the possibility of the foreclosure of the market was evident as the dispute occurred between downstream market rivals. In addition, in *Daimler* the conflict stems from the preference of the SEP holder in licensing the end-product manufacturer instead of the suppliers. But in *Huawei*, the Court did not address the issue of level of licensing explicitly, instead, it determined under what circumstances seeking an injunction by an SEP holder under FRAND commitment could be considered abusive within the meaning of Article 102 TFEU.

75 In this section, we examine if the *Huawei* ruling, despite these differences, can still be applied to the level of licensing disputes as in *Daimler*. In other words, we want to know if the fulfilment of the conditions defined in *Huawei* with respect

97 *Huawei* judgment (n 66) para. 53.

98 *Motorola* (n 91). The Commission noted that Motorola is a competitor in the downstream market for mobile telephones that implement relevant telecommunication standards, including GRPS, and competes against other implementers.

99 Case No. AT.39939 Samsung – Enforcement of UMTS Standard Essential Patents, C(2014) 2891 final. (hereinafter: *Samsung*). The Commission took a preliminary view that the conduct under review could potentially exclude Apple, a rival manufacturer of UMTS-compliant mobile devices, from the market.

to indispensability and legitimate expectation is *sufficient* to say that the refusal of a non-vertically integrated SEP holder (like Nokia) to license a component maker will lead to antitrust harm within the meaning of Article 102 TFEU?

76 If Nokia was vertically integrated in the automotive market, its refusal to license the component suppliers would be deemed an abuse, and no future discussion would be required. But it is not.

77 The following discussion shows that it is possible that conduct is an abuse even if the conduct does not reserve the downstream market to the dominant firm, and such an abuse would happen in the form of exclusionary.[100]

78 First, the refusal by a non-vertically integrated SEP holder to license component makers can potentially lead to adverse consequences, including limiting production, markets, and technical development, which ultimately harm consumers. This type of behaviour may be in violation of Article 102(b) TFEU, as it restricts the commercial operations of unlicensed component makers, exposing them to legal and commercial uncertainties, even if they may have certain limited have-made rights.[101]

79 Second, in addition to the abuse of dominant position against competitors, a dominant firm can be found to abuse its position when it restricts the freedom of non-competitors. This concept is well explained by Deringer, who highlights that the objective of competition rules is to safeguard the freedom of choice for market participants and to ensure the unhindered interaction of supply and demand in a competitive environment.[102] The conduct constitutes an abuse when a dominant firm utilises its position to limit or eliminate the freedom of decision-making in competition, whether it be the freedom of competitors or the freedom of choice for consumers.[103] Such actions undermine the fundamental principles of fair competition and hinder market dynamics that lead ultimately to harming the overall welfare of the market.

80 Finally, abuse of dominance can occur when a firm holds a dominant position in one market (Market A) and refuses to license its SEPs to suppliers in another market (Market B). In such cases, the SEP holder, with market power in Market A, may seek higher licensing fees, potentially causing harm in Market B. It is important to note that abusive behaviour need not occur within the market where the SEP holder holds dominance and there is no need to have cause and connection between dominance and effects. Consider the example provided by Monti,[104] where Market A represents a raw material market, and the dominant firm is the sole producer of that raw material. In this scenario, the dominant firm can exert influence on Market B by withholding the raw material supply from downstream firms. This refusal to license may be deemed exclusionary if it hinders supplier access to the market, impedes innovation, or creates entry barriers for potential competitors.

81 Crucially, it is not a requirement for the dominant firm to be active in Market B where the refusal to license takes place. The key consideration is whether the firm's refusal to license its intellectual property or essential inputs in Market A, where it is dominant,

100 In contrast, Nazzini argues that since no competitors of the dominant SEP holder are foreclosed in Daimler context, the abuse is not exclusionary but exploitative. Renato Nazzini, *The Foundations of European Union Competition Law The Objective and Principles of Article 102* (Oxford OUP 2011). Pp. 231-234.

101 The Court in *Höfner and Elser* stated that Article 102(b) was breached because the dominant undertaking was unable to satisfy the existing demand. (See: Case No. C-41/90 *Klaus Höfner and Fritz Elser vs. Macrotron GmbH* [1991] ECR I-1979). In the case of level discrimination, the SEP holder may be considered unwilling to satisfy existing demand. Article 102 TFEU does not require proof of actual effects of anti-competitive behaviour, only proof of potential effects in the relevant legal and economic context. Therefore, it is not necessary for the conduct under review to have caused a restriction of output, but only to have the likely effect of causing such a restriction. This reasoning can be extended to the Daimler context, where component manufacturers could not legally manufacture and sell standard-compliant components without a license. Although overall output may not be affected by the practice in each case, the restriction on output is likely to occur.

102 Arved Deringer, *The Competition Law of the European Economic Community* (New York (osv) : Commerce Clearing House 1968). Pp. 166-167.

103 *Idem*.

104 Giorgio Monti, *EC Competition Law* (2007). Pp. 186-192.

has an anti-competitive impact in Market B.[105]

82 In the context of *Daimler*, the SEP holder is not extending dominance into another market but is rather seeking maximum royalties by licensing to Daimler at end-product royalty rates. Moreover, by refusing to license to component makers, the SEP holder prevents them from successfully entering another market and developing potentially beneficial products. This behaviour harms competition, and the market suffers as component makers are unable to harness their innovation potential. Such conduct is considered exclusionary abuse.

83 In line with the argument discussed above, the Düsseldorf court in *Daimler* noted that when component makers have their own licences, they may develop and produce a component on their own and sell to their preferred downstream customers. Moreover, if component makers rely on derived rights, such as have-made rights obtained from the licensed end-product manufacturer, they are limited to selling only to that specific OEM and cannot trade their components in the open market. This constraint prevents them from independently innovating and developing their products, which can have a negative impact on consumers.[106] In such cases, a refusal by the SEP holder to grant an independent licence to component makers may impede competition, potentially triggering a duty to deal under Article 102 TFEU. This is particularly relevant considering that component makers have the potential to further advance the patented technology for new applications and explore untapped markets beyond a specific sector.

84 In conclusion, building upon the landmark judgment of the *Huawei* case by the ECJ, we contend that the refusal of a SEP holder to grant licences to component makers could be considered an abuse of dominant position. This applies not only when the refusal has the potential to exclude competitors downstream, but also when it obstructs technological advancement and innovation, ultimately harming consumers. An example of this is the limitations faced by unlicensed component makers in their commercial activities.

d.) Policy Change Suggestion

85 Based on the provided discussion, we can suggest a policy change in the EU on imposing SEP holders under FRAND commitment to license component makers. Such a change could be relevant for four reasons. First, there is no hard-and-fast rule that requires the dominant undertaking to be vertically integrated and in competition with potential licensees in downstream market for abuse withing the meaning of Article 102 TFEU. Second, while it is true that most cases of refusal to license under Article 102 TFEU have involved vertically integrated firms, the EU courts have not definitively stated that a non-vertically integrated firm can never be subject to exclusionary abuse. Third, the circumstances that led to the imposition of a duty to license in *Huawei* also apply to non-vertically integrated undertakings as indispensability condition is met because the SEP is equally necessary for all who want to manufacture and sell standard-compliant products regardless of whether or not the SEP holder is vertically integrated. In addition, the condition of legitimate expectation is also satisfied because FRAND commitment creates a legitimate expectation that the SEP holder will license the SEP on FRAND terms to all entities that require it to manufacture and sell standard-compliant products. And lastly, imposing a duty to license to component makers would not have a detrimental effect on the SEP holder's incentives to innovate because they have already decided to exploit their patent by granting FRAND licences.[107]

86 Such duty to license to component makers would be more crucial in two following scenarios:

87 The first case is when the suppliers need the SEPs to develop patented technology for a new usage that goes beyond a particular sector, opening a new market. In this scenario, a licence request from the component makers should not be refused. That said, one may wonder what the role of these suppliers in the supply chain at issue would be. Are they indeed suppliers for the standards-compliant product in

105 *Idem*.

106 Düsseldorf judgment (n 1).

107 Nazzini (n 74) pp. 234-235.

question, or independent persons as they want to develop a new product/component?

88 There should be a distinction between component makers who are part of the chain, and those who are independent makers of a product. In the latter case, the independent makers should prove that they do not intend to duplicate goods already offered on the market. Instead, they want to produce new goods or services for which there is a potential consumer demand, therefore, they are entitled to a licence because they are no longer component suppliers, but in fact producers.

89 The second scenario involves a situation where the SEP holder insists on licensing to end-product manufacturer while arguing that have-made right would safeguard component suppliers, but the conditions of have-made right could not be fulfilled, i.e., the end-product manufacturer could not design the component himself. Therefore, if end-product manufacturer claims that the standard-compliant component was designed by his suppliers and not by himself, then the SEP holder cannot benefit from the arguments for have-made rights in convincing the end-product manufacturer to take a licence. In such a situation, the SEP holder must license component suppliers instead of end-product manufacturer.[108]

2. Non-Discrimination Principle

90 The general principle of non-discrimination under EU Law could be relevant to our study as it argues that by refusing to license, the SEP holder makes a discriminatory choice based on his position in the supply chain. This could be an alternative approach to determine if a refusal to license a component manufacturer is an abuse of dominance. In terms of value chain, the key question is whether refusing licenses to component makers, while granting them to end-product manufacturer, constitutes different treatment of equivalent transactions with other trading parties under Article 102(c) TFEU, ultimately putting them at a competitive disadvantage. It is worth mentioning that the non-discrimination (ND) prong of FRAND commitment and non-discrimination principle are usually discussed together in the literature, however, as the ND prong does not address licensing level but royalty base, it will be discussed in the next section.

a.) Equivalent Transaction

91 To determine whether a dominant company has engaged in discriminatory behaviour under Article 102(c) TFEU, it must be shown that the company has placed some of its trading partners at a competitive disadvantage on a relevant market where they compete.[109] The following elements must also be present: equivalent transactions, dissimilar conditions, and competitive disadvantage.[110] If these elements are established, it is up to the dominant undertaking to provide evidence that their conduct

108 When considering the application of Article 102 TFEU, it is important to keep in mind two key factors. Firstly, this article only applies to undertakings that have a dominant position in the relevant market(s). Therefore, any analysis under Article 102 TFEU must begin with determining whether the company in question holds such a position. Secondly, even if a refusal to license is found to constitute an abuse that restricts competition, the dominant undertaking can attempt to show that its conduct is objectively justified. The dominant undertaking must bear the burden of substantiating an objective justification for their conduct. In the case of a refusal to license to component makers, such conduct may be justified if it is either objectively necessary or produces efficiencies that outweigh the restrictive effects on consumers. The Guidance Paper outlines four requirements that a company must meet to justify abusive conduct that forecloses its rivals. Firstly, the conduct must lead to efficiencies, which are not limited to economic considerations such as price or cost but can also include technical improvements in the quality of the goods. Secondly, the conduct must be essential for realising these efficiencies. Thirdly, the efficiencies must outweigh the negative effects on competition. Fourthly, the conduct must not eliminate effective competition by removing all or most existing sources of actual or potential competition. See Communication from the Commission — Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings, OJ C 45, 24.2.2009, p. 7–20. Para 30.

109 Judgment of 19 April 2018, *MEO vs. Autoridade da Concorrência*, C-525/16, EU:C:2018:270. [hereinafter: *MEO*]. Para. 23.

110 The ECJ in the *United Brands* case clarified that the scope of Article 102(c) is limited to situations where a dominant undertaking engages in transactions equivalent to those with its customers. Case 27/76, United *Brands Company and United Brands Continentaal BV vs. Commission* (1978) ECLI:EU:C:1978:22. [hereinafter: *United Brands*]

is objectively justified.[111] This type of discrimination is the only one prohibited under Article 102(c) TFEU and is known as market-distorting discrimination, as its anti-competitive effect immediately distorts downstream or upstream competition.[112]

92 In our context, the first two elements are not present: The practice of licensing only end-product manufacturers would not consist in the application of dissimilar conditions to equivalent transactions as transactions with component makers are not equivalent to transactions with end-product manufacturers and additionally, component makers are not in a competitive relationship with end-product manufacturers. Therefore, the practice could not cause competitive distortions between suppliers or customers of the SEP holder.

93 With regard to the competitive disadvantages, the following analysis is crucial for applying subparagraph (c) of the Article 102 TFEU: it must be shown not only that the behaviour of an undertaking in a dominant market position is *discriminatory*, but also that it tends to *distort* that competitive relationship that hinders the competitive position of some of the business partners of that undertaking in relation to the others. The ECJ has elaborated the subparagraph (c) of the Article 102 TFEU in *MEO* case. Though it is related to price discrimination, it could be inspiring for our analysis. In *MEO*, The Court ruled that the concept of competitive disadvantage must be interpreted to the effect that where a dominant undertaking applies discriminatory prices to trade partners on the downstream market, it covers a situation in which that behaviour is capable of distorting competition between those trade partners.[113] Competitive disadvantage presupposes a distortion of competition between two undertakings which are competitors, *at least potentially*. The anti-competitive effect under Article 102(c) must flow from discrimination, but the discrimination must be proved to cause competitive distortions upstream or downstream. The competitive harm is the negative effect of discrimination on the productive and dynamic efficiency of the suppliers or customers of the dominant undertaking.[114]

94 This ultimately means that Article 102(c) cannot establish a duty of the SEP holder to license component manufacturers if the SEP holder is licensing only end-product manufacturer. This is because transactions with component makers are not equivalent to transactions with end-product manufacturers, and component makers are not in a competitive relationship with end-product manufacturers. However, under Article 102(c), the SEP holder may be obligated to grant licenses to all competing component makers once he has licensed one of them.[115]

95 By the same token, Mannheim court in *Daimler* ruled that there was no indication that Nokia was distorting competition between trading partners by imposing discriminatory conditions in the selection of the contracting partner or requiring the royalty be based on the last stage of the value chain.[116] Specifically, the court found that there was no risk of Daimler being placed at a competitive disadvantage compared to other car manufacturers, nor was there any risk of Daimler being unable to switch to other licensed suppliers for LTE connectivity in vehicles, possibly on more favourable terms. Thus, the existing supplier chain would not be affected by the SEP holder licensing practice.[117]

96 Overall, the provided discussions bring out that the rules on discrimination under Article 102 (c) TFEU do not solve the puzzle of licensing level in value chain.

3. Horizontal Guidelines

97 The bottom line from the two previous analyses revealed that unlike non-discrimination under Article 102 (c) TFEU, the *Huawei* doctrine could be applied in determining licensing level in the

111 *Ibid*. Paras. 24-27 and 37.

112 *Idem*.

113 *MEO* (n 109) para. 37.

114 Nazzini (n 74) p. 250-255.

115 However, this obligation is subject to considering relevant factors that differentiate the position of one licensee from another.

116 Mannheim judgment (n 1) 64.

117 *Idem*.

sense that it could impose a duty to license to component makers. To complete our competition law investigation, in the following section we study the EU Commission Guidelines on the applicability of Article 101 of the TFEU to horizontal cooperation agreements[118] to see whether in these guidelines and their new version of 2022, there is an indication to show that the Commission may also expect the SEP holder to grant a licence to component makers.

98 From the standpoint of the scope of the Horizontal Guidelines (HGs) there is doubt whether they can cover vertical licensing agreements between SEP holders and (non-competing) implementers. In addition, the Horizontal Guidelines are to provide a safe harbour for the SDOs, and in the standardisation agreements section seek to promote SSOs' IPR policies compliant with Article 101 TFEU. The Horizontal Guidelines do not propose an antitrust obligation. Their function is to provide a safe harbour that specifies which competitors' agreements can be deemed presumptively lawful.[119] Hence, outside of this safe harbour, there is no antitrust presumption of liability. However, in the literature, mostly the proponent of licencing to all including component makers refer to paragraph 285[120] which states that: "*[i]n order to ensure effective access to the standard, the IPR policy would need to require participants wishing to have their IPR included in the standard to provide an irrevocable commitment in writing to offer to license their essential IPR to all third parties on fair, reasonable and non-discriminatory terms...",* arguing that licence to all third parties is clear enough to envisage an obligation for SEP holders to licence to component makers. On the other hand, the proponents of access to all argue that the term "all third parties" is not further defined and full implementation of standard could be only happened at end-product level. They also argue that what is important for the Commission is accessibility of a standard to the users of that standard and accessibility does not exclusively mean a licence.[121]

99 With regard to the "access" or "licence",[122] while some believe that what legally matters is access, some other deplete access from any legal meaning and make arguments for licence.[123] The former argue that in the Guidelines the prevention of *effective access* to the standard is crucial; standardisation agreements should provide *access* to standardised technology; and that FRAND commitment is made to guarantee *effective access* to standards.[124] The latter, however, highlight that this distinction between access and licence is meaningless and effective accessibility does not occur but through licence.[125]

118 European Commission, Guidelines on the applicability of Art. 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements [2011] OJ C11/1. [hereinafter: Horizontal Guidelines].

119 The para. 279 (476 in the revised HGs) states that "*the non-fulfilment of any or all of the principles set out in this section will not lead to any presumption of a restriction of competition within Article 101 TFEU.*".

120 In the revised Horizontal Guidelines 2022 (n 92) para. 482.

121 See the list of both groups (n 42).

122 Legally speaking, a license, has an affirmative defence to a claim of patent infringement. A contract under which the patent holder promises not to assert claims of infringement of its patents against an identified body. A license is a suspension or exemption from the exclusionary right, which the patent holder, in its sole discretion, may grant. It is a common misconception to think of a patent licence as providing the ability to make and sell some product. Agreements of that sort are known as technology transfers and can entail the conveyance of technical information, know-how, documentation, or even physical materials, facilities, and personnel, to enable the transferee to manufacture a particular product or carry out process, for example. A patent licence will often accompany a technology transfer, perhaps in the same contractual document. But it is quite common for parties to enter into patent licences without engaging in any technology transfer, with each promising not to sue the other over patent infringement while each using its own know-how. Because a patent license is not about gaining access to the know-how or the technical capability needed to participate in a commercial endeavour, a licence is not necessarily required for an implementer to carry on its business. Implementers can, and often do, manufacture and sell products that may be patented by others and then they get a licence to legalise their business from patent law perspective. See Layne-Farrar and Stark (n 3).reasonable, and non-discriminatory ("FRAND" Pp. 110-112.

123 Geradin and Katsifis (n 37) p. 4.

124 See for e.g., Borghetti, Nikolic, and Petit (n 39) p. 39; Juan Martinez, 'FRAND as Access to All versus License to All', *Journal of Intellectual Property Law & Practice*, 14.8 (2019), 642–51 <https://doi.org/10.1093/jiplp/jpz075>. P. 646.

125 Geradin and Katsifis (n 37) p. 4.

100 Our examination shows that in the Horizontal Guidelines context, access is applied in two occasions. First, in standardisation agreements under which effective access to the technology should be guaranteed through IPR Policies of SDOs for the relevant *industry*. The Guidelines explain how the IPR policy through good faith disclosure could provide this access.[126] In this context, the access is a goal provided through the SDOs' IPR Policies and in particular different types of disclosure models.[127] Some models may require participants to engage in IPR discourse, while others may only encourage it.

101 The proponent to licence to all including component makers also refer to paragraph 294[128] arguing that where the result of a standard is not at all accessible for all members or third parties, this may foreclose or segment markets and is thereby likely to restrict competition.[129] Likewise, competition is likely to be restricted where the result of a standard is only accessible on discriminatory or excessive terms for members or third parties. However, in the case of several competing standards or in the case of effective competition between the standardised solution and non-standardised solution, a limitation of access may not produce restrictive effects on competition. One however must highlight that this paragraph is also about the Commission assessment of the standardisation agreements at the SDO level, and it is not imposing any obligation for the SEP holders. The Guidelines then state that a clear and balanced IPR policy, adapted to the industry and the needs of the SDO in question, increases the likelihood that the implementers of the standard will be granted effective access to the standards elaborated by that standard development organisation. This is a bridge to the second usage of access where the goal is to provide the standardised technology for its implementers which is fulfilled through FRAND commitment set by the SDOs.

102 Second, the Guidelines state that to ensure effective access to the standard, the IPR policy would need to require participants wishing to have their IPR included in the standard, to provide an irrevocable commitment in writing to offer to license their essential IPR to all third parties on FRAND terms.[130] Accordingly, the first access is at the disclosure level and the addressee is the relevant industry, however, the second access is the ultimate goal of standardisation which is typically attained through licence. One however should not conclude that the effective access is attained only through a licence. As stated earlier, Horizontal Guidelines do not create legal obligations and FRAND obligation is created by the patentees' signature of the SDOs' IPR policies. It is in line with the Guidelines stating that FRAND commitment is designed to ensure that the essential IPR protected technology incorporated in a standard is "accessible to the users" of that standard on FRAND terms and conditions.[131]

103 As concluding remarks, we share the idea that access is a goal while a licence is a legal means to achieve it.[132] What the SEP holder typically committed to the

126 Paragraph 483 provides that: "the IPR policy would need to require good faith disclosure by participants of their IPR that might be essential for the implementation of the standard under development. This is relevant for (i) enabling the industry to make an informed choice of technology to be included in a standard 279 and (ii) assisting in achieving the goal of effective access to the standard. Such a disclosure obligation could be based on reasonable endeavours to identify IPR reading on the potential standard and to update the disclosure as the standard develops. With respect to patents, the IPR disclosure should include at least the patent number or patent application number. If this information is not yet publicly available, then it is also sufficient if the participant declares that it is likely to have IPR claims over a particular technology without identifying specific IPR claims or applications for IPR (so-called blanket disclosure)281. Except for this case, blanket disclosure would be less likely to enable the industry to make an informed choice of technology and to ensure effective access to the standard. Participants should also be encouraged to update their disclosures at the time of adoption of a standard, in particular if there are any changes which may have an impact on the essentiality or validity of their IPRs. Since the risks with regard to effective access are not the same in the case of a standard development organisation with a royalty-free standards policy, IPR disclosure would not be relevant in that context."

127 Revised Horizontal Guidelines 2022 (n 92) para. 492.

128 *Ibid*. Para. 491.

129 Rosenbrock (n 42) pp. 5-6.

130 Revised Horizontal Guidelines 2022 (n 92) para. 482.

131 *Ibid*. Para. 484.

132 Bowman Heiden, Jorge Padilla and Ruud Peters, 'The Value

SDOs is to provide all third parties with an access through a licence. The HGs do not define any specific rule for how licence should be granted to ensure that access, nor impose any duty to license to component manufacturers.[133]

C. Conclusion

104 Connected cars present a distinctive challenge within the realm of SEP licensing due to the integration of TCUs, fostering intricate complexities within their value chains. This multi-tiered structure raises pivotal questions regarding the rightful licensees and the optimal rates for licensing. Traditionally, SEP holders favour directing licenses to end-product manufacturers, often driven by the prospect of attaining greater royalties based on a percentage of the final product's value. Conversely, the end-product manufacturers and their suppliers advocate for licensing to suppliers, advocating for royalties confined to the TCU's price. This precise scenario played out prominently in the legal tussle involving Nokia (the SEP holder), Daimler (the automobile manufacturer), and its supplier before the German courts.

105 When negotiations between the involved parties reach an impasse, recourse to court intervention becomes commonplace to adjudicate the debate over the licensing foundation. These parties often seek authoritative intervention to ascertain the FRAND-compliant offering, whether through competition authorities or courts. The FRAND commitment forms a robust legal groundwork empowering these entities to establish FRAND terms for licenses. It functions as a primary legal impetus for authority or court involvement in these disputes, irrespective of its legal construct.

106 In our study, we initially scrutinized the potential of patent law, FRAND commitments, and competition law to enforce SEP holders to license suppliers in alignment with Daimler's stance. A deep dive into patent law revealed guidance but not an inherent requirement for licensing, as it hinges on specific standards and doctrines. We explored the have-made right concept, contemplating scenarios where the end-product manufacturer serves as the IoT component designer (in this case, the TCU), potentially instructing suppliers to fabricate the TCU component. Yet, this condition often remains unfulfilled in the IoT domain due to the lack of technical prowess, infrastructure, and interest from end-product manufacturers. Despite this, if met, the SEP holder might opt to license the end-product manufacturer, while suppliers could be shielded through the have-made right against patent infringement actions, aligning with Nokia's argument.

107 Furthermore, our examination delved into ETSI's IPR policy and FRAND commitment, uncovering ambiguous wording necessitating interpretation under the French Civil Code, ETSI's governing law. However, conclusive establishment of the ETSI FRAND commitment mandating licensing to component makers remained elusive. Analysing competition law, particularly within the Huawei doctrine section, steered us toward suggesting a policy shift favouring licensing component suppliers.

of Standard Essential Patents and the Level of Licensing' [2020] SSRN Electronic Journal 1. P. 6.

133 It is however worth noting that the new version highlights the possibility of hold-out situation under which the user of the standard, refuses to pay a FRAND royalty fee or uses dilatory strategies We believe that this new consideration is a clear message from the Commission to highlight the two-side objectives of FRAND commitment: a) to prevent SEP holders from making the implementation of a standard difficult by refusing to license or by requesting unfair or unreasonable fees, (hold-up) and b) to allow them to monetise their technologies via FRAND royalties. Therefore, the issue of implementation is better to be determined on a case-by-case and industry-by-industry basis. See: Revised Horizontal Guidelines 2022 (n 92) para. 482.

Generative AI and Creative Commons Licences

The Application of Share Alike Obligations to Trained Models, Curated Datasets and AI Output ***

by **Kacper Szkalej * and Martin Senftleben ****

Abstract: This article maps the impact of Share Alike (SA) obligations and copyleft licensing on machine learning, AI training, and AI-generated content. It focuses on the SA component found in some of the Creative Commons (CC) licences, distilling its essential features and layering them onto machine learning and content generation workflows. Based on our analysis, there are three fundamental challenges related to the life cycle of these licences: tracing and establishing copyright-relevant uses during the development phase (training), the interplay of licensing conditions with copyright exceptions and the identification of copyright-protected traces in AI output. Significant problems can arise from several concepts in CC licensing agreements ('adapted material' and 'technical modification') that could serve as a basis for applying SA conditions to trained models, curated datasets and AI output that can be traced back to CC material used for training purposes. Seeking to transpose Share Alike and copyleft approaches to the world of generative AI, the CC community can only choose between two policy approaches. On the one hand, it can uphold the supremacy of copyright exceptions. In countries and regions that exempt machine-learning processes from the control of copyright holders, this approach leads to far-reaching freedom to use CC resources for AI training purposes. At the same time, it marginalises SA obligations. On the other hand, the CC community can use copyright strategically to extend SA obligations to AI training results and AI output. To achieve this goal, it is necessary to use rights reservation mechanisms, such as the opt-out system available in EU copyright law, and subject the use of CC material in AI training to SA conditions. Following this approach, a tailor-made licence solution can grant AI developers broad freedom to use CC works for training purposes. In exchange for the training permission, however, AI developers would have to accept the obligation to pass on – via a whole chain of contractual obligations – SA conditions to recipients of trained models and end users generating AI output.

Keywords: Copyright, AI, Machine Learning, Licensing, Creative Commons, Share Alike

Recommended citation: Kacper Szkalej and Martin Senftleben, Generative AI and Creative Commons Licences The Application of Share Alike Obligations to Trained Models, Curated Datasets and AI Output, 15 (2024) JIPITEC 313 para 1

* Dr, Researcher in Intellectual Property Law, Institute for Information Law (IViR), University of Amsterdam, The Netherlands.

** Professor of Intellectual Property Law and Director, Institute for Information Law (IViR), University of Amsterdam; Of Counsel, Bird & Bird, The Hague, The Netherlands.

*** This article is based on the study *Mapping the Impact of Share Alike/Copyleft Licensing on Machine Learning and Generative AI* for which the authors secured funding from the Open Future Foundation, available at: https://openfuture.eu/publication/the-impact-of-share-alike-copyleft-licensing-on-generative-ai/. Both the study and this article have been established in complete academic independence.

A. Introduction

1 The increasing impact of AI on the copyright system has led to a multi-faceted discussion ranging from the creation of breathing space for text and data mining (TDM)[1] to the potential displacement of human creative labour.[2] A further facet of this debate is the impact of contractual obligations relating to copyright-protected training material on machine learning (ML) and, more broadly, the development and exploitation of generative AI systems. Copyleft licensing strategies and ShareAlike clauses found in some CC licences (we will call them collectively CLSA) impose obligations on the recipient to use the same licensing model that underlies the original license for downstream use.[3] In this way, a network effect is ensured that preserves and extends the commons. However, when copyright-protected knowledge resources are released under CLSA clauses and subsequently used for AI training, the question arises whether such licences provide the same safeguards for commons-based projects that they provide in case of more traditional uses. In the following analysis, we examine this question step-by-step. First, we explain the anatomy of CLSA licences and shed light on main features relevant to downstream use (section B). Second, we identify acts of use with copyright relevance in AI training processes (section C) before turning to the sensitive question of whether TDM exceptions are capable of prevailing over SA obligations and rendering corresponding licensing terms inapplicable (section D). On this basis, we explore more closely the application of the CLSA concept of 'adapted materials' to generative AI development and exploitation (section E). Finally, we discuss different strategies to ensure that SA obligations remain intact and can be passed on to AI developers, recipients of trained AI models and end users generating AI output (section F).

2 Throughout the analysis we will refer to the *development phase* by which we mean the entire ML-process culminating in the creation of a generative AI system, and the *exploitation phase* by which we mean the subsequent use of the generative AI system by a user who gives instructions (prompts) that result in the generation of material on the basis

1 Cf. S.M. Fiil-Flynn and others, 'Legal Reform to Enhance Global Text and Data Mining Research – Outdated Copyright Laws Around the World Hinder Research', *Science* 378 (2022) 951, 951 ; T. Ueno, 'The Flexible Copyright Exception for 'Non-Enjoyment' Purposes Recent Amendment in Japan and Its Implication', *Gewerblicher Rechtsschutz und Urheberrecht International* 70 (2021), 145 (150-151); M.W. Carroll, 'Copyright and the Progress of Science: Why Text and Data Mining Is Lawful', *U.C. Davis Law Review* 53 (2019) 893, 954; C. Geiger, G. Frosio, O. Bulayenko (2019), 'Text and Data Mining: Articles 3 and 4 of the Directive 2019/790/EU', *Centre for International Intellectual Property Studies Research Paper* 2019/08, (Strasbourg: CEIPI 201), 5 and 31; T. Margoni and M. Kretschmer, 'A Deeper Look Into the EU Text and Data Mining Exceptions: Harmonisation, Data Ownership, and the Future of Technology', *CREATe Working Paper* 2021/7 (Glasgow: CREATe Centre 2021), 10; M.A. Lemley and B. Casey, 'Fair Learning', *Texas Law Review* 99 (2021) 743, 770-771; R.M. Hilty and H. Richter, 'Position Statement of the Max Planck Institute for Innovation and Competition on the Proposed Modernisation of European Copyright Rules – Part B: Exceptions and Limitations – Art. 3 Text and Data Mining', *Max Planck Institute for Innovation and Competition Research Paper Series* 2017-02, 1.

2 Cf. G. Westkamp, 'Borrowed Plumes: Taking Artists' Interests Seriously in Artificial Intelligence Regulation', 1 (19-26), forthcoming; K. de la Durantaye, 'Nutzung urheberrechtlich geschützter Inhalte zum Training generativer künstlicher Intelligenz – ein Lagebericht', *Archiv* für *Presserecht* 55 (2024), 9 (21-22); M.R.F. Senftleben, 'AI Act and Author Remuneration – A Model for Other Regions?' (2024), 6-23 <https://ssrn.com/abstract=4740268>; C. Geiger, 'Elaborating a Human Rights Friendly Copyright Framework for Generative AI', *International Review for Intellectual Property and Competition Law* 2024, forthcoming, 29-33 <https://ssrn.com/abstract=4634992>; D. Friedmann, 'Creation and Generation Copyright Standards', *NYU Journal of Intellectual Property and Entertainment Law* 14 (2024), forthcoming, 7-8; C. Geiger, 'When the Robots (Try to) Take Over: Of Artificial Intelligence, Authors, Creativity and Copyright Protection', in F. Thouvenin and others (eds), *Innovation – Creation – Markets, Festschrift für Reto M. Hilty* (Berlin: Springer 2024), 67-87; M.R.F. Senftleben, 'Generative AI and Author Remuneration', *International Review of Intellectual Property and Competition Law* 54 (2023) 1535, 1542-1556; G. Frosio, 'Should We Ban Generative AI, Incentivise It or Make It a Medium for Inclusive Creativity?', in E. Bonadio and C. Sganga (eds), *A Research Agenda for EU Copyright Law* (Cheltenham: Edward Elgar 2024), 19-21 <https://ssrn.com/abstract=4527461>; C. Geiger and V. Iaia, 'The Forgotten Creator: Towards a Statutory Remuneration Right for Machine Learning of Generative AI', *Computer Law and Security Review* 52 (2024), forthcoming, 10-16 <https://ssrn.com/abstract=4594873>.

3 Copyleft licensing was originally developed within the free and open source software movement as an alternative to so-called permissive licensing. See generally P. McCoy Smith, 'Copyright, Contract, and Licensing in Open Source', in: A. Brock (ed.), *Open Source Law, Policy and Practice* (2nd ed., Oxford: Oxford University Press 2022) 83-97.

of those instructions. The terms *development* and *exploitation*, as used in the following discussion, are roughly equivalent to *training* and *inference* as used in technical literature.

B. Copyleft Licences And Their Applicability To Machine Learning

3 When a literary or artistic work is created by a human author, copyright law confers a set of exclusive rights to the creator.[4] The inevitable consequence of this is that use falling within the scope of exclusive rights is only permitted where authorisation for each relevant use exists. Such authorisation may either come from a licence given by the copyright holder or be based on a statutory permission such as a copyright exception or fair use provision.[5] In any other case the use is prohibited because of the exclusive nature of the conferred rights.

4 Within this matrix, CLSA licencing is based on the idea of *relying* on copyright as a mode to promote access to content by making the work available under specified conditions. For this reason, it is essential to determine the manner in which the exclusive rights are exercised in the case of this specific licensing model. Typically CLSA licences distinguish between two types of material: on the one hand, the original material protected by copyright, often denoted as 'licensed material'; on the other hand, derivative material, denoted in CC licences as 'adapted material', created by the licensee and derived from, or based on, the original, licenced material.[6] The two concepts are not mutually exclusive but merely denote, from the perspective of the rightholder (licensor) whether the licensed material has undergone further modifications.

5 CLSA licences rely on copyright, essentially, to achieve two central goals. First, the licence describes uses that are permitted, often in broad terms. By way of example, the CC BY-SA 4.0 licence enables the recipient to reproduce and share the licensed material, in whole or in part, and to produce, reproduce, and share adapted material.[7] Moreover, the recipient is authorised to exercise the permissions in all media and formats (known and unknown) and make necessary technical modifications.[8] These use permissions depend on compliance with further conditions that are imposed on the licensee to ensure that a subsequent recipient downstream can enjoy similarly broad permissions. In this vein, the recipient of licensed material may be prevented from offering or imposing additional or different licensing terms, and applying technological protection measures.[9] The CC BY-SA 4.0 licence also clarifies that a subsequent downstream recipient of the material receives an automatic offer setting forth the same licence conditions (including in the licensee's later licence, denoted as 'adapter's licence' – at least to the extent to which the licence relates to material over which the original licensor has rights).[10] Depending on the needs of the licensor, a licence may also restrict commercial use.[11]

6 Second, CLSA licences introduce a set of requirements on which the operability of the granted use permissions depends. That is, failure to comply renders the granted permissions inapplicable. For example, where recipients share the licenced material, as is expressly permitted, they may be required to retain copyright information supplied with the licensed material (attribution) or indicate that they have modified the material or retain an already existing indication of previous modifications, or indicate that the licensed material is licensed under a specific CLSA licence and include the text of, or a reference to, the licence.[12] Moreover, and most

4 For instance, see ISD, Articles 2 to 4.

5 CDSMD, Articles 3 and 4. As to the US fair use system, see P. Samuelson, 'Fair Use Defenses in Disruptive Technology Cases', UCLA Law Review 72 (2024), forthcoming <https://ssrn.com/abstract=4631726>; M. Sag, 'The New Legal Landscape for Text Mining and Machine Learning', *Journal of the Copyright Society of the USA* 66 (2019), 291.

6 As another example of a CL licence that has wide application, the Free Art Licence 1.3 refers to 'subsequent works'.

7 CC BY-SA 4.0 Section 2(a)(1).

8 CC BY-SA 4.0 Section 2(a)(4)

9 CC BY-SA 4.0 Section 2(a)(5)(c).

10 CC BY-SA 4.0 Section 2(a)(5)(a)-(b).

11 For example CC BY-NC-SA 4.0 Section 2(a)(1).

12 Such as in the case of CC BY-SA 4.0 and CC BY-NC-SA 4.0,

importantly, for adapted material produced by the licensee, the licence may require that the adapted version be made available on the same terms (SA condition). For example, the CC BY-SA 4.0 licence requires the licensee to apply the same licence, with the same conditions, or a licence that is equivalent with the granted licence.[13]

7 With such a setting in mind, CLSA licensing essentially sets in motion a cascade of contractual arrangements that ensure, and maintain, open access to the protected material. Recipients are free to use the original, licensed material as long as they observe the specific requirements set forth in the licence. If they create adapted material, they must make it available under the same terms. The model, simply stated, passes on the CLSA obligation to every user of the material. This contractual mechanism works because copyright protection of the original, licensed material, as well as those portions of adapted material that are derived from the licensed material, will prevent uses outside of the licence. In other words, copyright protection of the licensed material serves as a basis for granting the permissions and enforcing the conditions that establish the SA scheme. A licensee who does not observe CLSA obligations steps outside of the use permission following from the licence and, thus, acts without rightholder authorisation. As a result, downstream use of adapted material that neglects CLSA obligations amounts to infringement of copyright in the original material offered under CLSA terms.[14] The use of CLSA material for generative AI development, thus ultimately boils down to the question whether, and if so where exactly, a ML workflow using CLSA training resources involves copyright-relevant acts that may trigger an obligation to observe the CLSA conditions accompanying the materials offered under CLSA terms.

C. Machine Learning And Copyright-Relevant Acts Of Use

8 In the development phase, the ML workflow – namely the training of foundation models – typically requires accumulating vast amounts of multi-modal data.[15] In the case of foundation models relating to literary or artistic expression, copyright-protected source material will serve as 'data' input for training purposes.[16] As this data collection and use may involve copying of individual expression enjoying protection, the question arises whether the training process falls within the scope of the reproduction right granted in copyright law (following sections C.I and C.II).[17] The supply of curated datasets also raises the question whether the right of communication and making available to the public may play a role (section C.III).

I. Right of Reproduction

9 Article 9(1) of the Berne Convention for the Protection of Literary and Artistic Works (BC) confirms that authors enjoy the exclusive right to authorise the reproduction of their works in any manner or form.[18] The right has also been

which make this clear in Section 3(a).

13 CC BY-SA Section 3(b).

14 Although there seems to be a view that non-conformity with a licence should "merely" be treated as breach of contract (for which the default statutory remedies are normally weaker than in case of infringement, or as agreed in the contract), the CJEU has made it clear in Case C666/18 *IT Development SAS v Free Mobile SAS*, that remedies and sanctions available to rightholders through the Enforcement Directive must be available also in case of breach of a copyright licence agreement. Inevitably that presumes that infringement of copyright has taken place..

15 R. Bommasani et al., *On the Opportunities and Risks of Foundation Models*, Centre for Research on Foundation Models (CRFM) (Stanford Institute for Human-Centred Artificial Intelligence (HAI), Stanford: Stanford University 2021), 146 <https://crfm.stanford.edu/assets/report.pdf> .

16 As to the distinction between use of literary and artistic works as 'works' and use of works as 'data', see R. Ducato/A. Strowel, 'Ensuring Text and Data Mining: Remaining Issues with the EU Copyright Exceptions and Possible Ways Out', *European Intellectual Property Review* 43 (2021), 322 (334). Cf. also M. Borghi/S. Karapapa (2011), 'Non-display Uses of Copyright Works: Google Books and Beyond', *Queen Mary Journal of Intellectual Property* 1 (2011), 21 (44-45).

17 For a more detailed discussion of this conceptual issue, see M.R.F. Senftleben, 'Compliance of National TDM Rules with International Copyright Law – An Overrated Nonissue?', *International Review of Intellectual Property and Competition Law* 53 (2022), 1477 (1493-1502).

18 T. Dreier, 'Berne Convention' in Dreier T and Hugenholtz

incorporated in the so-called WIPO 'Internet' Treaties of 1996 (the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT)) which aimed to adapt copyright law to the digital environment.[19] As the scope of the reproduction right in the digital environment was a highly contentious issue during negotiations, particularly in respect of temporary copying, such as in the operating memory of computers, the WCT does not contain a self-standing right of reproduction but instead incorporates it from the Berne Convention[20] and includes an Agreed Statement indicating that the right fully applies in the digital environment and that storage of a work in digital form in an electronic medium constitutes a reproduction.[21] However, an Agreed Statement does not have the status of an adopted treaty article.[22] The interpretative value of the Agreed Statement addressing the right of reproduction in the WCT is further reduced by the fact that the sentence referring to storage was not adopted unanimously and fails to provide an agreed definition of storage,[23] thus leaving the scope of the reproduction right in the digital environment open and prone to 'highly variable interpretation' as far as temporary copying goes.[24] Consequently, international copyright law has been said to leave open the question of temporary reproduction.[25] With regard to AI development, it is important to note that the right of reproduction granted at the international level need not be understood to cover TDM for ML training purposes.[26] The applicability of the reproduction right depends on the individual national or regional transposition of the applicable international rules into domestic law.

10 In the EU, the question was settled through the adoption of the 2001 Directive on Copyright in the Information Society (ISD),[27] which introduced in its Article 2 a comprehensive reproduction right that covers everything from permanent to temporary reproduction, in whole or in part, in any form and by any means, covering both the reproduction of works as well as subject-matter protected by neighbouring rights.[28] Accordingly, at least in the EU copyright

B (eds), *Concise European Copyright Law* (Kluwer Law International 2016), 45; S. Depreeuw, *The Variable Scope of the Exclusive Economic Rights in Copyright* (Kluwer Law International 2014), 65. In case of neighbouring rights this is Article 3(e) Rome Convention, which laconically explains that a reproduction involves the making of a copy or copies of a fixation. The fact that it must be a copy of a fixation follows naturally from the category of subject matter – recordings of sound (phonograms), of performances, or of broadcasts. In case of the Berne Convention (works), commentators note that the language of the Convention is absent a fixation requirement; Z. Efroni, *Access-Right: The Future of Digital Copyright Law* (Oxford University Press 2010), 220. S. Ricketson and J. Ginsburg, *International Copyright and Neighbouring Rights: The Berne Convention and Beyond* (vol I, 2nd ed, Oxford University Press 2006) 645 observe that it is 'open to debate whether the Berne Convention also requires member states to interpret 'any manner or form' to extend to transient digital fixations'. At least in terms of subsistence of protection, the Berne Convention introduces a discretionary possibility to require fixation of the work in Article 2(2).

19 WCT and WPPT, Preamble.

20 WCT, Art. 1(4).

21 WCT, Agreed Statement concerning Article 1(4). An identical statement is present in WPPT. See Agreed Statement concerning Articles 7, 11 and 16. Cf. M.R.F. Senftleben, (n 17).

22 J. Reinbothe and S. von Lewinski, *The WIPO Treaties on Copyright: A Commentary on the WCT, the WPPT, and the BTAP* (2nd ed., Oxford: Oxford University Press 2015) 66.

23 As to the specific circumstances surrounding the adoption of the Agreed Statement, see furthermore M.R.F. Senftleben, 'Compliance of National TDM Rules with International Copyright Law – An Overrated Nonissue?', *International Review of Intellectual Property and Competition Law* 53 (2022), 1477 (1489 and 1500-1501).

24 Ricketson and Ginsburg (n 18), 687; also JAL Sterling and P. Johnson , 'WIPO Copyright Treaty (1996)' in T. Cook (ed), *Sterling on World Copyright Law* (4th edn, Sweet & Maxwell 2015), 929 noting the question is open.

25 M.R.F. Senftleben, 'WIPO Copyright Treaty', in: T. Dreier and P.B. Hugenholtz (n 18) 99. The same is understood to hold true in respect of the WPPT. See F. Brison, 'WIPO Performances and Phonograms Treaty', id., 201-205.

26 M.R.F. Senftleben (n 17).

27 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, *Official Journal of the European Communities* 2001 L 167, 10. As to an earlier recognition in case of specifically software, see Article 2 of the Software Directive.

28 In case of neighbouring rights, however, this only concerns fixations of performances, first fixations of films, phonograms (sounds recordings), and fixations of

acquis, it is settled that the exclusive rights of copyright and neighbouring right holders cover virtually any form of copying protected content. Whilst certain types of copying *may* be subject to a copyright exception, the fact remains that, as a starting point, the broad right of reproduction granted in the EU covers acts of copying in the digital environment.

11 Considering this scope and reach of the reproduction right in the EU, we consider that the AI development phase is likely to involve, as a default, reproductions within the meaning of EU copyright law, thus rendering CLSA licences relevant.[29] In this vein, Recital 105 of the AI Act[30] confirms that the use of literary and artistic works for AI training purposes has copyright relevance[31] and involves TDM activities that require the authorisation of rightholders in the absence of a copyright exception: '[a]ny use of copyright protected content requires the authorisation of the rightholder concerned unless relevant copyright exceptions and limitations apply.'

II. Impact on Machine Learning

12 The analysis of ML processes based on the EU position requires a closer look at the individual training and development steps as not every ML stage involves the making of copies. For the sake of simplicity we think of the development phase as involving five stages, consisting of (1) data corpus compilation (2) data corpus preprocessing, (3) data corpus annotation, (4) training of the model, and (5) permanent creation of an artefact (trained model).[32] The initial stages concerning the creation of a training dataset (stages 1 and 2) which involve data collection, for example through web scraping, and conversion of the data into desirable formats, involve reproductions, be it downloading and storage, or reproductions in the operating memory of the system. For a reproduction to take place in computer systems, human cognition (perception of the work) is not necessary. That is why storage of protected material on non-volatile storage media, such as a flash drive, or more fluidly in volatile memory, such as the operating memory of a computer, amounts to a reproduction in the sense of copyright law. Because of the breadth of the reproduction right granted in the EU, the individual acts carried out during the ML process are likely to amount to independent, separate, acts of reproduction determined by the particular needs of the entire process.[33] In other words, the act of transferring data to the operating memory of the system for the purpose of conversion does not, as such, remove the copyright relevance of the reproduction carried out previously to store a copy. If that already stored copy is later deleted from the storage resource, it raises the question whether the conversion process can be regarded as a permissible form of transient copying in the sense of the copyright exception laid down in Article 5(1) ISD.[34] Needless to say, any back-up copies created as a result of security diligence also amount to separate reproductions. The third stage, essentially, involves data labelling and is essential for supervised learning, while the fourth constitutes the actual training phase involving computational analysis, correction and validation.[35] In these instances the

broadcasts. Protection of non-original photographs remains a matter for national legislation in the Member States.

29 However, see also the analysis by R. Ducato and A. Strowel (n 16) 334, who propose to distinguish between use of copyrighted material 'as a work' and use of copyrighted material as mere data – with the result that use as mere data may fall outside the scope of the right of reproduction.

30 This numbering refers to the text of the AI Act, as adopted by the European Parliament on 6 March 2024.

31 As to the discussion about the applicability of Articles 3 and 4 CDSMD to the training of generative AI models, see M.R.F. Senftleben (n 2), 7-14; F. Hoffmann, 'Zehn Thesen zu Künstlicher Intelligenz (KI) und Urheberrecht', *Wettbewerb in Recht und Praxis* 2024, 11 (16-18).

32 See generally T. Margoni, 'Artificial Intelligence, Machine Learning and EU Copyright Law: Who Owns AI?', *CREATe Working Paper* 2018/12 <https://www.create.ac.uk/artificial-intelligence-machine-learning-and-eu-copyright-law-who-owns-ai/>.

33 Cf. Recital 105 AIA and M.R.F. Senftleben (n 2) 7-14.

34 Even if it has, the subsequent creation of a converted copy will amount to a new reproduction.

35 See generally on the training stage J.-M. Deltorn, 'The elusive intellectual property protection of trained machine learning models: A European perspective', in: R. Abbott (ed.), *Research Handbook on Intellectual Property and Artificial Intelligence* (Cheltenham: Edward Elgar 2022) 87.

same principle applies: *if* labelling and training involve copying of copyright-protected data, at least in the operating memory, these acts are likely to constitute reproductions within the meaning of the broad right granted in the EU,[36] even though they are merely a means to an end.

13 The broad EU approach to the reproduction right also raises the question whether the right may become relevant beyond the act of, strictly speaking, duplication of copyright-protected data collected during the corpus compilation phase, in particular in relation to stages 2 and 3 (data corpus preprocessing and annotation). Notably, the Court of Justice of the European Union (CJEU) has considered the process of canvas transfer (the removal of ink form a paper poster and its transfer to a canvass) as an act of reproduction because of the change of medium.[37] Although not concerning digital copies, this broad approach raises the question of whether electronic changes to a computer file containing a work that result in adaptation or conversion of the file to a desirable format could similarly involve an act of reproduction, which would be different and separate from the mere act of copying data. While CJEU jurisprudence points in this direction, the Canadian Supreme Court has reached a different conclusion for such acts.[38] Hence, the issue has not yet been settled. If the issue is brought before the CJEU, the Court may refrain from extending the Canvas approach to file conversions for TDM purposes.

14 Whether copyright-relevant acts of reproduction take place during stage five is not as straightforward. Although the applicable copyright principles are easy to explain, the model exists as a separate artefact: normally operating independently from its training pipeline.[39] It does not seem to retrieve the contents of the training dataset when generating outputs during the exploitation phase. Hence, it can be argued that the artefact exists and operates independently from the copyright-protected data, including 'licensed material' triggering CLSA obligations, that have been used as training resources in the preceding steps one to four. Following this line of argument, the artefact can be described as a giant collection of data points and vectors that have been derived from the training material. [40] It can also be assumed that the artefact is unlikely to contain copyright-protected traces of works that were used for training.[41] The adoption of this perspective leads to the conclusion that the creation of the trained model at stage five breaks the link with CLSA licensing obligations that may rest on training resources. If the artefact as such does not contain copyright-protected traces of CLSA works used for training purposes, copyright law does not offer tools for enforcing CLSA conditions: relevant acts of reproduction are sought in vain.

15 As so often in the legal debate, however, nuance is important. In the CJEU's jurisprudence, in particular the case law established in *Infopaq* and *Pelham*,[42] confirms that for assuming a relevant act of reproduction it would be sufficient that a fragment of a work is included in the artefact. In the case of copyright, this fragment would have to satisfy the originality test of free, creative choices (a text

36 ISD, Article 2.

37 Case C-419/13 *Art & Allposters v Stichting Pictoright*, para 43.

38 Compare *Théberge v. Galerie d'Art du Petit Champlain Inc* [2002] 2 S.C.R.

39 J.-M. Deltorn, (n 35) p. 88.

40 *See* for similar reasoning by American scholars P. Samuelson, C.J. Sprigman, M. Sag, *Comments in Response to the Copyright Office's notice of Inquiry on Artificial Intelligence and Copyright* (30 October 2023), 7-8 <https://www.regulations.gov/comment/COLC-2023-0006-8854>.

41 As discussed in more detail below, it cannot be ruled out that AI models memorise certain aspects of training data. Cf. I. Emanuilov and T. Margoni, 'Forget Me Not: Memorisation in Generative Sequence Models Trained on Open Source Licensed Code' <https://ssrn.com/abstract=4720990>>, 10-15; S. Biderman and others , 'Emergent and Predictable Memorization in Large Language Models' (*arXiv*, 31 May 2023) <https://arxiv.org/abs/2304.11158>; X. Gu and others, 'On Memorization in Diffusion Models' (*arXiv*, 4 October 2023) <https://arxiv.org/abs/2310.02664>. However, the central question from a copyright perspective is whether these memorised aspects contain protected traces of copyright-protected works or other protected subject matter, such as sound recordings. As discussed below, it seems to us that, at least in the majority of cases, it cannot generally be assumed that protected elements of CLSA material will be memorised and become part of trained models.

42 Case C-5/08, *Infopaq v DDF*, paras 38-39; Case C-476/17 *Pelham v Hütter and Schneider-Esleben*.

extract of 11 words may be sufficient).[43] This is why we referred to 'copyright-protected traces' above. In the case of neighbouring rights, the test for assuming protection may be even more relaxed. With regard to sound recordings, for instance, the CJEU has confirmed that the reproduction right of phonogram producers covers sound extracts 'even if very short' (a sound sample of 2 seconds may be sufficient).[44] These nuances might prove to be relevant in cases where memorisation, or overfitting or parroting, of data from the training dataset might actually take place.[45] If, therefore, protected fragments of a work or subject matter enjoying neighbouring rights protection are contained in the stage five artefact, a relevant act of reproduction takes place and the equation is different. Here the CJEU's judgment in *Allposters* mentioned above may prove to offer an additional relevant argument, if it is to be read as implying that the potentially different technological representation of such a fragment in the stage five artefact, compared to its representation in the training dataset, is indeed to be captured by the European concept of reproduction. However, whilst the decisions in *Infopaq* and *Pelham* confirm that an infringing exploitation can already be assumed in the case of text excerpts that are as short as 11 words, or extracts from sound recordings that are as short as 2 seconds, the copyright assessment is not quantitative but qualitative and therefore case-specific. In the case of works, the used fragment must be original and contain free, creative choices of the original work.[46] In the case of neighbouring rights, the CJEU has also developed additional criteria. Fragments taken from a protected sound recording, for instance, no longer amount to infringement if they are used in a derivative phonogram 'in a modified form unrecognisable to the ear.'[47]

16 Factoring this important nuance into the equation, it nevertheless seems to us that, at least in the majority of cases, we can uphold the above conclusion: with the creation of the stage five artefact, the link with CLSA obligations is broken and copyright is no longer available as a tool to enforce CLSA conditions. In practice, it will also be difficult to prove that protected traces of works or other subject matter made their way into the trained model, especially absent access to the training data for comparison. How can we provide evidence that free, creative choices of a human author have been woven into the fabric of the final artefact? How can we prove that sound snippets in the trained model are recognisable to a human ear?

17 These practical considerations need not always thwart copyright claims. Ultimately, copyright is a property right and the duty of care to ensure compliance lies not with the rightholder but the developer or adopter of the model. In an infringement case, the judge may reverse the burden of proof and impose the obligation on the artefact developer or adopter to show that the trained model does not contain copyright-protected traces of CLSA works. In the case of iconic works that a web crawler looking for training material is likely to collect very often, such as a famous quote[48] or drawings of famous fictional characters, the AI developer may even find it particularly difficult to provide this proof.[49]

43 Case C-5/08 *Infopaq v DDF*, paras 38-39.

44 Case C-476/17 *Pelham v Hütter and Schneider-Esleben*, para 29.

45 See generally D.J. Gervais and others, 'The Heart of the Matter: Copyright, AI Training, and LLMs' (2024), 11 https://ssrn.com/abstract=4963711>; I. Emanuilov and T. Margoni (n 41) pp. 10-15; N. Carlini and others, 'Extracting Training Data from Large Language Models', in: *30th USENIX Security Symposium (USENIX Security 21)* (USENIX Association 2021), 2633-2650 <https://www.usenix.org/system/files/sec21-carlini-extracting.pdf>; N. Carlini and others, 'Quantifying Memorization Across Neural Language Models' (*arXiv*, 6 March 2023) <https://arxiv.org/abs/2202.07646v3>; S.A. Taghanaki and J. Lambourne, 'Detecting Generative Parroting through Overfitting Masked Autoencoders' (*arXiv*, 19 June 2024) <https://arxiv.org/html/2403.19050v3>.

46 Case C-5/08, *Infopaq v DDF*, para 51. See also Joined Cases C-403/08 and C-429/08 *FAPL*, para 159; Case C-406/10 *SAS Institute v World Programming*, para 70.

47 Case C-476/17 *Pelham v Hütter and Schneider-Esleben*, paras 29-31 and 39.

48 For an example concerning the beginning of a chapter of J.K. Rowling's *Harry Potter and the Philosopher's Stone*, see I. Emanuilov and T. Margoni (n 41) p. 15.

49 I. Emanuilov and T. Margoni (n 41) p. 26. Cf U. Hacohen and N. Elkin-Koren, 'Copyright Regenerated: Harnessing GenAI to Measure Originality and Copyright Scope', Harvard Journal of Law and Technology (2024) 37 <https://ssrn.com/abstract=4530717>; U. Hacohen and others, 'Not All Similarities Are Created Equal: Leveraging Data-Driven

If the system has somehow stored all the information necessary to identify and reproduce a cat or dog, why should the system have refrained from doing the same with regard to Mickey Mouse, Spiderman, Lucky Luke and Nijntje?

18 However, even if we could assume that there is a statistical probability of copyrighted traces of iconic CLSA works finding their way into the trained model, we believe that this statistical probability of CLSA facets in the artefact is not a sufficiently solid basis for *routinely* enforcing SA conditions in AI development contexts, as the legal discussion is currently in its infancy and there is no series of court decisions providing established case law. Given the legal uncertainty surrounding copyright claims based on training material memorisation, it is important to explore alternative, potentially more robust solutions. To bring these alternative solutions to light, we focus on the above-described assumption that the trained model only contains unprotected data points and vectors which, in turn, leads to the conclusion that, in the majority of cases, the link with CLSA licensing obligations is broken.

19 Ascertaining the copyright status of the stage five artefact may also raise a challenge that goes to the core of the reproduction right and beyond the legal-technical questions of training material memorisation and the burden of proof. If we conceive of the model as having a capacity to evoke the image of an existing work (or parts thereof) following training, rather than a capacity to retrieve it from a repository of stacked copies (or fragments thereof) that are algorithmically selected and modified following a prompt, the manner in which the model operates may be more similar to how a human being is capable of imagining an object. If this is the feature of the stage five artifact, it may be difficult – if not impossible – to qualify the creation of the stage five artefact as involving the reproduction right from the outset.

Biases to Inform GenAI Copyright Disputes' (*arXiv*, 7 May 2024) <https://arxiv.org/abs/2403.17691>; M. Sag, 'Copyright Safety for Generative AI' Houston Law Review 61 (2023) 295, 321-337; A. Guadamuz, 'A Scanner Darkly: Copyright Liability and Exceptions in Artificial Intelligence Inputs and Outputs', Gewerblicher Rechtsschutz und Urheberrecht International 73 (2024) 111, 121-122.

III. Right of Communication and Making Available To The Public

20 While the right of reproduction is certainly the centre of gravity in the debate on generative AI systems and CLSA conditions, we must not overlook interactions that may take place on the market for ML technology. Adding this broader context, other exclusive rights than the right of reproduction may also become relevant at the development phase, namely the 'right of communication' to the public, and particularly the 'making available' prong of the right.[50] In particular, offers to the public to obtain curated training datasets that include copies of protected content, whether annotated or not, may amount to an act of making available to the public in the sense of EU copyright law. This is ultimately a jurisdictional issue as copyright protection is limited by the principle of territoriality, but at least in the case of the EU the matter seems to be settled. Considering CJEU jurisprudence on the right of communication to the public granted in Article 3 ISD,[51] it cannot be ruled out that such an offer would involve copyright law and amount to an act of communication to the public/making available to the public that requires the authorisation of the rightholder. Accordingly, it would activate the obligations following from SA conditions in cases where CLSA knowledge resources are used to build a curated dataset. The offer and distribution of such a dataset would require compliance with CLSA terms. In the case of CC BY-SA 4.0, the use will also be governed by the prohibition to offer or impose additional or different terms than provided under that CLSA licence in respect of 'licenced material' (to which the licensor has exclusive rights).[52] It is also noteworthy that whilst the use permissions granted by copyleft licences are broad, they may also be limited to non-commercial use (CC BY-NC-SA 4.0).

50 ISD, Article 3.

51 Case C-263/18 *NU and GAU v Tom Kabinet*, establishing that the offer to buy an e-book (that could be purchased by one person only) amounts to a communication to the public. In the EU the same applies in case of offers of products that are not delivered online, see Case C-516/13 *Dimensione Direct Sales and Labianca v Knoll Internationall*, para 28-32; Case C-5/11 *Donner*, para 30.

52 CC BY-SA 4.0, Section 2(a)(5)(c).

Such a licence might prevent the sharing of material if it is done for a commercial purpose.

D. Copyright Exceptions Covering Machine Learning In The EU

21 An important aspect of CLSA licences is the manner in which they address the relationship to copyright exceptions. Certain copyleft licensing schemes explicitly give precedence. For example, the CC BY-SA 4.0 license states the following in Section 2(a)(2):

> *For the avoidance of doubt, where Exceptions and Limitations apply to Your use, this Public License does not apply, and You do not need to comply with its terms and conditions.*

22 This clause, essentially, makes it necessary to identify uses permitted under relevant 'exceptions and limitations' (collectively referred to as 'copyright exceptions' or 'exceptions' in the following analysis) in a given copyright regime. To the extent to which ML workflows and related uses fall within the scope of exceptions in the EU, these statutory use permissions prevail and render the CLSA conditions inapplicable. Concomitantly, uses that are not covered by a copyright exception continue to instead be governed by the terms of the licence. For this reason, it is essential to determine the scope of copyright exceptions that can apply to ML workflows. Where legislators have introduced provisions that have the potential of covering the entire ML process, such as the TDM provisions in the EU, it is crucial to determine the impact of those provisions as the precedence given to copyright exceptions in copyleft licences is likely to affect the continued viability of CLSA terms.

23 The catalogue of exceptions in Article 5 ISD is quite diverse. In respect of ML processes, it is noteworthy that it includes the possibility to carry out temporary reproductions under certain further conditions (Article 5(1) ISD). With the adoption of the 2019 Directive on Copyright in the Digital Single Market (CDSMD),[53] the EU legislator has introduced two additional provisions that have given the debate an entirely new edge. Conditioned on lawful access to the material used for ML purposes, Articles 3 and 4 CDSMD provide for exceptions to the right of reproduction that enable TDM, which Article 2(2) CDSMD defines broadly as an 'automated analytical technique aimed at analysing text and data in digital form in order to generate information which includes but is not limited to patterns, trends and correlations'. With this broad definition, imposing no restriction on the type of information that should be generated, the provisions are apt candidates for covering various ML uses, and are indeed considered as such.[54] The European legislature has recently affirmed the relevance of the TDM provisions for the development and training of generative models in Recital 105 of the AI Act. Most important for our purposes is the exception in Article 4 CDSMD because it is not subject to a general purpose limitation but applies to any actor or purpose for which TDM is carried out, including commercial TDM projects. Article 3 CDSMD, by contrast, imposes both a purpose limitation and a beneficiary limitation: it applies only to research organisations[55] and cultural heritage institutions[56] and covers only TDM for the purpose of scientific research.[57] To complete the overview of copyright exceptions that play a role in

53 Directive 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, *Official Journal of the European Communities* 2019 L 130, 92.

54 T. Chiou, 'Copyright lessons on Machine Learning: what impact on algorithmic art?', *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 9 (2019), 398 (409).

55 Defined in CDSMD, Article 2(1), as 'a university, including its libraries, a research institute or any other entity, the primary goal of which is to conduct scientific research or to carry out educational activities involving also the conduct of scientific research: (a) on a not-for-profit basis or by reinvesting all the profits in its scientific research; or (b) pursuant to a public interest mission recognised by a Member State'.

56 Defined in CDSMD, Article 2(3), as 'a publicly accessible library or museum, an archive or a film or audio heritage institution'.

57 See further K. Szkalej, 'The paradox of lawful text and data mining? Some experiences from the research sector and where we (should) go from here' (2024), forthcoming <https://ssrn.com/abstract=5000116>.

ML contexts, we also address, at the end of this part, the aforementioned temporary copying exception provided under Article 5(1) ISD.

I. TDM Provisions

24 As explained, copyleft licences let statutory copyright exceptions prevail over the licencing terms. Against this background, the introduction of TDM exceptions in the CDSM Directive raises the question of whether it still makes sense to deploy CLSA licences as a mode to regulate downstream use. To the extent to which the TDM exceptions cover ML processes, they prevail over the SA condition and render it inapplicable under the current configuration of the relationship between CC licenses and copyright exceptions. Nonetheless, we believe that SA conditions can still play an important role. To explain this point, we must take a closer look at the TDM exceptions in EU copyright law.

1. Output Not Covered

25 First, the TDM exceptions laid down in Articles 3 and 4 CDSMD only concern the TDM *process* of collecting and analysing copyright-protected data to generate information relevant for creating a ML tool or foundational model.[58] Articles 3 and 4 CDSMD do not cover the reproduction of copyright-protected features in literary and artistic content which the fully trained AI model generates in the end. It is an entirely different question of who might be liable under copyright law in the event that such output could be deemed to infringe copyright in a pre-existing work. We return to this issue in part 5, highlighting here only the aspect that the applicability of a copyright exception covering TDM does not, as such, automatically render CLSA licence clauses inapplicable with regard to AI output even though a copyleft licence scheme such as CC BY-SA 4.0 states explicitly that copyright exceptions prevail. Instead, the precedence given to copyright exceptions only concerns the exempted form of use falling within the scope of the exception, namely the ML process leading to the establishment of the generative AI model in the case of the TDM provisions in Articles 3 and 4 CDSMD. Any other use, such as the subsequent content generation based on a user prompt, could in principle be regulated by the CLSA licence terms, to the extent that it involves copyright-relevant acts requiring the authorisation of the CLSA licensor.

2. Opt-out Mechanism

26 Second, whereas Article 3 CDSMD is mandatory by law and cannot be contracted out,[59] in case of Article 4 CDSMD, TDM can be carried out only if the rightholder has not reserved the use of the protected material in an appropriate manner. With this opt-out mechanism, Article 4(3) CDSMD, rather than staying silent on contractual overridability, affords rightholders the opportunity to determine whether they wish to make their works available for TDM. In other words, Article 4 CDSMD is merely a conditional exception. Once the rightholder has opted out in accordance with Article 4(3) CDSMD, the use privilege no longer applies:

> *The exception or limitation provided for in paragraph 1 shall apply on condition that the use of works and other subject matter referred to in that paragraph has not been expressly reserved by their rightholders in an appropriate manner, such as machine-readable means in the case of content made publicly available online.*[60]

27 With regard to CLSA licence terms, this means that rightholders can use the opt-out mechanism in Article 4(3) CDSMD when they wish to minimise the impact of the copyright exception in Article 4 CDSMD and maximise the scope of copyright as a basis for enforcing CLSA conditions. As a result of the opt-out, the use of the original material for TDM purposes requires authorisation unless it falls within the scope of the mandatory exemption of scientific TDM in Article 3 CDSMD. Hence, the rightholder has the opportunity to impose CLSA licensing terms and make the use dependent on compliance with these terms. This exercise of the opt-out possibility, admittedly, may give rise to a dilemma in the light of

58 See also the definition in CDSMD, Article 2(2).

59 See however K. Szkalej (n 57), 11.

60 CDSMD, Article 4(3).

the current configuration of CLSA licensing regimes: the opt out shuts down the exception. Current CLSA licensing schemes, however, take as a starting point that copyright exceptions ought to remain intact in order not to curtail user rights following from statutory use permissions.

28 Against this background, the crucial question is whether, from the perspective of the CLSA licensing approach, it can be deemed legitimate to use the opt-out mechanism in Article 4(3) CDSMD and curtail the TDM freedom following from Article 4(1) CDSMD for the purpose of imposing CLSA conditions. From the perspective of EU copyright law, a rightholder availing itself of the opt-out possibility is exercising a prerogative and limitation of the TDM freedom that is inherent in the copyright exception itself. From this perspective, it does not seem inconsistent to restrict TDM falling under Article 4 CDSMD in order to create the possibility of granting and enforcing a tailor-made CLSA licence (that may be broad and allow TDM as long as the SA condition is observed). The opt-out mechanism thus appears as an efficient tool to expand CLSA culture to the realm of AI-generated literary and artistic output.[61]

II. Temporary Copying

29 As already explained above, the EU has opted for the introduction of a broad, comprehensive right of reproduction in Article 2 ISD – a right of reproduction that applies regardless of whether the act of copyright is 'temporary or permanent'. As a counterbalance to this comprehensive exclusive right, the EU copyright system prescribes a mandatory exception that enables temporary copying in Article 5(1) ISD. The provision permits temporary reproductions, which are transient or incidental, and form an integral and essential part of a technological process, and the sole purpose of which is to enable lawful use of the content,[62] on condition that it does not have independent economic significance.

30 Although this temporary copying rule only applies on several further conditions – ranging from the transient nature of the reproduction to the absence of independent economic significance – it nevertheless can cover ML activities taking place during the development phase leading to a generative AI model. Importantly, the adoption of specific TDM exceptions has not made Article 5(1) ISD obsolete. Instead, Articles 3 and 4 CDSMD coexist with the temporary copying rule in Article 5(1) ISD.[63] All these copyright exceptions thus offer statutory use permissions for ML reproductions falling within their specific fields of application.

31 As to the specific scope of Article 5(1) ISD, it must be pointed out that the temporary copying rule is quite a complex provision with five central requirements that must be satisfied cumulatively in order to benefit from the use privilege.[64] As regards the first condition, the existence of a 'temporary' reproduction can be assumed, for example, when the copies are immediately deleted or replaced automatically.[65] A reproduction can be deemed 'transient' when the conservation period of copies is limited to the time necessary for the technical process of making the reproduction and the copies are automatically erased after completion of the process.[66] A reproduction is 'incidental' where it is not self-contained with respect to the technical process of which it forms part. Thus, copies resulting from temporary reproductions should have no purpose that is separate from the one for which they have been made in the framework of ML.[67]

32 These conceptual contours indicate clearly that Article 5(1) ISD only offers limited possibilities in ML

61 See also A. Lazarova and others, *Creative Commons Statement on the Opt-Out Exception Regime / Rights Reservation Regime for Text and Data Mining under Article 4 of the EU Directive on Copyright in the Digital Single Market* (Creative Commons 2021) <https://creativecommons.org/wp-content/uploads/2021/12/CC-Statement-on-the-TDM-Exception-Art-4-DSM-Final-updated.pdf>.

62 ...or a transmission in a network between third parties by an intermediary.

63 CDSMD, recital 9.

64 Case C-5/08 *Infopaq v DDF*, para 55.

65 Case C-360/13 *PRCA v NLA and Others (Meltwater)*, para 26.

66 Id., para 40.

67 Id., para 43.

contexts.[68] As copies based on Article 5(1) ISD cannot be retained for a longer period, the provision does not permit the creation of source data repositories. The transient nature of the copies excludes reuse from the outset.

33 Nonetheless, Article 5(1) ISD may play a role when ML concerns online sources that can be analysed directly and processed in the format in which they are available on webpages.[69] For a computational analyses based on web scraping, the requirements of a temporary and transient nature need not constitute insurmountable hurdles. The invocation of the use privilege in connection with ML also seems in line with the general objectives underlying the provision.[70] The CJEU has recognised that, in order to protect the effectiveness of the temporary copying rule and safeguard its purpose, Article 5(1) ISD must be understood to allow the development and operation of new technologies and ensure a fair balance between the rights and interests of rightholders and those of users.[71]

34 Against this backdrop, it seems consistent to assume that, as long as the individual requirements of the provision are fulfilled, AI trainers can belong to the circle of users who can benefit from Article 5(1) ISD in the context of ML. As CLSA licensing terms allow copyright exceptions to prevail over contractual SA conditions, this means that, to the extent to which the temporary copying rule covers reproductions carried out for ML purposes, SA obligations are rendered inapplicable.

E. Generative AI and The Concept Of 'Adapted Materials'

35 The concept of 'adapted materials' is an essential component of CLSA clauses with particular importance to downstream use. As it may be relevant to both the development phase and the exploitation phase, we treat the two phases separately in our analysis. However, it is useful to first define the term as it gives us an idea of the type of material we are dealing with. For the purpose of our analysis, we rely on the definition of 'adapted materials' in the CC BY-SA 4.0 licence, which defines the term as:

> *material subject to Copyright and Similar Rights that is derived from or based upon the Licensed Material and in which the Licensed Material is translated, altered, arranged, transformed, or otherwise modified in a manner requiring permission under the Copyright and Similar Rights held by the Licensor. For purposes of this Public License, where the Licensed Material is a musical work, performance, or sound recording, Adapted Material is always produced where the Licensed Material is synched in timed relation with a moving image.*[72]

36 In light of this definition, it seems safe to assume that the term covers in any case material that (1) is protected by copyright; and (2) is derived from or based on licenced material (which too is protected by copyright). Importantly, the material has been modified *in a manner requiring permission* from the licensor. Seen from the perspective of the rightholder (the CLSA licensor), licence clauses that concern adapted material continue to operate in the sphere of copyright law, i.e., as explained above, the exclusive rights granted in copyright law serve as a basis for imposing CLSA obligations and enforcing these obligations. One initial question is nonetheless whether the definition of 'adapted material' is intended to fully align with copyright nomenclature.

68 Cf. C. Geiger, G. Frosio, and O. Bulayenko, 'Text and Data Mining in the Proposed Copyright Reform: Making the EU Ready for an Age of Big Data? Legal Analysis and Policy Recommendations', International Review of Intellectual Property and Competition Law (2018), 814 (821-822); R.M. Hilty and H. Richter, 'Position Statement of the Max Planck Institute for Innovation and Competition on the Proposed Modernisation of European Copyright Rules – Part B: Exceptions and Limitations – Art. 3 Text and Data Mining', *Max Planck Institute for Innovation and Competition Research Paper Series* 2017-02, 2.

69 M.R.F. Senftleben, *Study on EU Copyright and Related Rights and Access to and Reuse of Data*, European Commission, Directorate-General for Research and Innovation (DG RTD) (Brussels: Publications Office of the European Union 2022) , 27-28 <https://data.europa.eu/doi/10.2777/ 78973>.

70 Cf. T. Margoni and M. Kretschmer, 'A Deeper Look Into the EU Text and Data Mining Exceptions: Harmonisation, Data Ownership, and the Future of Technology', *CREATe Working Paper* 2021/7 (Glasgow: CREATe Centre 2021),18-19.

71 Joined Cases C-403/08 and C-429/08 *FAPL*, paras 163-164; Case C-360/13 *PRCA v NLA and Others (Meltwater)*, para 24.

72 CC BY-SA 4.0, Section 1(a).

We assume it need not strictly follow the concept of 'adaptation' in copyright law. As explained in part 1, the term merely seems to denote that the CLSA licensee has no objection against the licensed material undergoing further modifications.

37 In this context, the reference to 'material subject to Copyright and Similar Right' at the beginning of the definition indicates, in our view, that the CLSA licence is intended to cover material in which the original material (licensed material) is shimmering through to such an extent that the licensor can invoke copyright as a means to enforce the CLSA conditions because the adapted material still displays copyright-protected creative choices of the licensor.[73] In this scenario, the CLSA clause imposes obligations on what the CC BY-SA 4.0 licence denotes as 'Adapter's Licence', which is the licence that the licensee provides downstream. On the one hand, this additional aspect of the licensing scheme seems to presume that the licensee/adapter creates material that attracts copyright protection itself – copyright that can be used as a basis for passing on CLSA obligations downstream. On the other hand, considering the entire design of the CC BY-SA 4.0 licence, it is noteworthy that the licensee/adapter *does not* issue a sublicence to the original material. As indicated earlier, under clause 2(a)(5) of CC BY-SA 4.0, it is the original licensor who licenses the rights in the relevant portions of the adapted material:

> Every recipient of Adapted Material from You automatically receives an offer from the Licensor to exercise the Licensed Rights in the Adapted Material under the conditions of the Adapter's License You apply.

38 Arguably, this chain of licences granted by the original licensor offers room for arguing that SA obligations can survive modifications even if these modifications do not attract copyright protection themselves. The current wording of clause 2(a)(5) obscures this argument by referring to 'Every recipient of Adapted Material'. If 'Adapted Material' must be understood to require material which adds sufficient new creative choices to attract copyright protection, it becomes doubtful whether the offer – a licence by the original licensor – also covers cases where modifications of the original material are not eligible for copyright protection.

39 However, this potential doubt can be dispelled. First, the formulation 'material subject to Copyright' at the beginning of the definition of 'adapted materials' need not be understood to introduce a strict requirement of modifications attracting copyright protection themselves. It may simply reflect the fact that, because of takings from the copyrighted material offered under CLSA conditions, the adapted material is subject to the copyright in the original CLSA source. Interestingly, this more flexible interpretation is in line with CJEU jurisprudence. In *Deckmyn*, the CJEU clarified that it could not be inferred from the usual meaning of the term 'parody' in everyday language, that the concept was:

> *subject to the conditions set out by the referring court in its second question, namely: that the parody should display an original character of its own, other than that of displaying noticeable differences with respect to the original parodied work...*[74]

40 With regard to work adaptations in the guise of parody, the Court, thus, explicitly rejected an approach requiring the parodist to add free, creative choices[75] that attract copyright protection coming on top of the protection which the original source material enjoys. Following in the footsteps of *Deckmyn*, the requirement of 'material subject to Copyright' in the definition of 'adapted material' can be deemed satisfied whenever protected features of the original material are still present – regardless of whether the adaptation itself is also eligible for copyright protection. This flexible reading allows us to establish a CLSA licence chain which, under clause 2(a)(5), has its origin in the SA offer made by the licensor of the original, licensed material. As

73 For a discussion of the relatively low threshold for assuming this copyright relevance in EU law, see M.R.F. Senftleben, 'Flexibility Grave – Partial Reproduction Focus and Closed System Fetishism in CJEU, *Pelham*', International Review of Intellectual Property and Competition Law 51 (2020), 751 (751-769).

74 Case C-201/13, *Deckmyn Vrijheidsfonds VZW v Vandersteen and Others*, para 21.

75 Case C-5/08 *Infopaq v DDF*, para 45; Case C-145/10 *Painer v Standard Verlags and Others*, para 89.

long as sufficient copyright-protected features of the original work remain discernible in downstream productions – qualified as 'adapted material' regardless of whether they have fresh, original features of their own – the SA obligation (that can be traced back to the original work and the initial licence granted by the original licensor) remains intact and enforceable.

41 For the purposes of our present inquiry, the essential point is that the definition of 'adapted material' and the outlined licence design determine the extent to which CLSA licensing schemes impact ML processes (development phase, section E.I) and AI-generated output (exploitation phase, section E.II). We now turn to a more detailed analysis of these two dimensions.

I. Input/Development Phase

42 Considering the different stages of ML described above, it is clear that collected material undergoes certain modifications for the purpose of making the ML process possible and more efficient. From the perspective of the licence mechanism, which refers to 'adapted material' in the context of regulating downstream use, the crucial question is whether work results that are obtained during the training process constitute modifications of the original, licensed CLSA material that can be classed 'adapted material' in the sense of the CC definition. As explained, the test is whether protected traces of the original, licensed CLSA material are still present in modifications arising during the training process: protected traces that allow the licensor to rely on copyright as a vehicle to enforce CLSA obligations. As already discussed in section C.II, the final artefact – the trained model – is unlikely to constitute adapted material. Arguably, it is independent from copyright-protected CLSA resources that have been used for training purposes. If the trained model is primarily seen as a giant collection of data points and vectors,[76] it can be assumed that it does not contain copyright-protected traces of works used for training. Following this approach, the model as a whole and its components cannot be regarded as 'adapted material' in the sense of the CC definition and the copyright link with CLSA licensing obligations is broken. Hence, copyright law does not offer tools for enforcing CLSA conditions with regard to the final trained model: in the absence of copyright-protected traces, the model does not have copyright relevance. Neither the creation of the model nor its further distribution amount to copyright infringement if protected features of original CLSA material do not shimmer through.

43 As explained in section C.III, the equation is different in the case of CLSA works that become building blocks of curated datasets. It is conceivable that obligations regarding 'adapted material' in the sense of the CC definition cover curated training datasets that contain sources to which the SA obligation is attached. Subject to our caveat further below relating to technical modifications, the making available of such datasets to the public, which may fall under a separate 'Adapter's Licence',[77] may trigger obligations to comply with SA conditions. This also means that the provider of the curated dataset containing CLSA components would be under an obligation to pass on the SA obligation to recipients (model developers).

44 However, where content originally released under a CLSA licence, such as CC BY-SA, is used to curate a training dataset and this dataset is later offered to external model developers, the provider of the curated dataset would have to ensure compliance with the SA condition of the relevant licence that governed the development of the curated dataset. The inevitable consequence of providing the curated dataset in a manner that contradicts the SA conditions imposed by the licence might, additionally, be that neither the TDM provisions in Articles 3 and 4 CDSMD nor the temporary copying exception in Article 5(1) ISD can be invoked any longer. While the discussion on lawful access requirements in EU copyright law is ongoing,[78] the view might be held that the

76 as to the question of memorisation of copyright-protected traces, see section C.II above.

77 'Adapter's Licence' in the terminology of CC-BY-SA 4.0, as mentioned above.

78 See the broader discussion on lawful access requirements and the problem of circularity: lawful access requirements subjecting copyright exceptions to contractual terms that may erode the freedom of use which the legislator sought to create when introducing the copyright exception in the first place. Cf. T. Margoni, 'Saving Research: Lawful Access

requirements of 'lawful use',[79] 'lawful access'[80] or 'lawfully accessible'[81] set forth in these provisions are not satisfied if CLSA components in the training dataset are used by model developers who do not assume the SA obligation themselves. The making available of the curated dataset in a way that does not pass on the SA obligation to model developers would culminate in use of CLSA resources without authorisation and, therefore, amount to copyright infringement, rendering the source material used for ML purposes unlawful. If the dataset developer does not observe the SA obligation, this lack of compliance is thus likely to prevent the model developer from demonstrating lawful access to the CLSA material which, arguably, is a prerequisite for both the TDM exceptions and the temporary copying exception.

45 Considering the full spectrum of concepts in CC licences, however, it is important to point out that, next to the described approach focusing on the concept of 'adapted material', the CC BY-SA 4.0 offers room for an alternative solution based on the concept of 'technical modification'. The CC BYSA 4.0 makes it clear that in so far as mere technical modifications of licensed material are concerned, making these modifications for purposes that in any event would be covered by the licence (which does provide broad use permissions to reproduce and share material and includes making technical modifications to the material) 'never produces Adapted Material'.[82] In other words, technical modifications constitute, under the typology adopted in the licence, licensed material. Under this alternative approach, the question arises whether potential modifications made to establish a curated dataset can be regarded as 'technical modification' in the sense of the licence. If this question is answered in the affirmative, the clauses in the licence on technical modifications would apply to curated datasets – and not the clauses on adapted material. Importantly, this conclusion need not exclude contractual obligations to observe SA conditions. It only excludes the application of Section 3(b) of the licence which applies to adapted materials. However, Section 3(a) concerns sharing of licensed material. This includes technically modified versions of the material, as addressed here. That material must be shared in a manner that includes copyright information and the terms of the licence etc. Moreover, Section 2(b)(5)(c) prevents downstream restrictions on the licenced material. Combining Section 3(a) and Section 2(b)(5)(c), the conclusion seems inescapable that technically modified versions are automatically subject to a SA condition resting on the licenced material. Hence, even if the concept of 'adapted material' cannot be applied to curated datasets, SA conditions remain relevant because they are attached to technically modified versions of the licensed material.

46 Finally, we must recall that the definition of 'adapted material' requires that the material be *modified in a manner requiring permission*. Therefore, copyright exceptions, especially the new TDM provisions discussed above, enter the picture and reduce the applicability of the SA condition to activities and materials that are not covered by pertinent exceptions. When it is assumed (as we did above), that Article 4 CDSMD has the potential to cover all copyright-relevant acts carried out during the ML training process, the term 'adapted material' thus becomes moot at the development stage unless, as explained above, the CC licensor seeking to introduce CLSA obligations exercises the opt-out possibility available under Article 4(3) CDSMD.

47 If the opt-out mechanism is used, this leads to a reservation of copyright that offers far-reaching possibilities for preserving the SA obligation at the development phase. In particular, the reservation of copyright offers CC licensors the opportunity to make it a condition in the licensing contract

to Unlawful Sources Under Art. 3 CDSM Directive?' (Kluwer Copyright Blog, 22 December 2023) <https://copyrightblog.kluweriplaw.com/2023/12/22/saving-research-lawful-access-to-unlawful-sources-under-art-3-cdsm-directive/>; V. Stančiauskas and others, *Improving Access to and Reuse of Research Results, Publications and Data for Scientific Purposes – Study to Evaluate the Effects of the EU Copyright Framework on Research and the Effects of Potential Interventions and to Identify and Present Relevant Provisions for Research in EU Data and Digital Legislation, With a Focus on Rights and Obligations* (Brussels: Publications Office of the European Union 2024), 150-153 and 187-194 <https://data.europa.eu/doi/10.2777/633395>.

79 ISD, Article 5(1).

80 CDSMD, Article 3.

81 CDSMD, Article 4.

82 CC BY-SA 4.0, Section 2(a)(4).

that the final trained model be distributed under CLSA conditions – in the sense of imposing an obligation on AI trainers to pass on SA conditions to downstream recipients regardless of whether the artefact contains protected traces of copyright-protected CLSA material. As we will explain in the following section, this possibility of preserving CLSA conditions rests on the opt-out mechanism and contractual obligations which the CC licensor imposes on AI trainers using CLSA material for ML purposes. If the artefact does not contain copyright-protected traces of CLSA training material and, hence, does not constitute adapted material in the sense of the CC licence, the enforcement of the SA condition must be based on the contractual obligation that was established with the model developer (licensee) at the beginning of the development phase. Hence, the focus shifts from copyright enforcement to the enforcement of contract terms in the relationship with the model developer.

II. Output/Exploitation Phase

48 The exploitation phase (use of generative AI systems based on a model trained on CLSA content) raises complex issues relating to the existence of copyright-relevant acts that may trigger CLSA obligations. Generative AI output often remains limited to general ideas, concepts, styles etc. that the AI system has deduced from human training material during the development phase. According to the so-called idea/expression dichotomy recognised in international copyright law, these general ideas, concepts, styles etc. do not enjoy copyright protection as long as they do not contain copyright-protected creative choices of the author of knowledge resources used for training purposes.[83]

49 Hence, the question arises whether copyright law offers a sufficient basis for imposing CLSA licensing terms on AI output at all. We recall that for these obligations to apply, the licence requires the sharing of 'adapted material'. As explained above, the CC BY-SA 4.0 licence defines adapted materials as:

> *material subject to Copyright and Similar Rights that is derived from or based upon the Licensed Material and in which the Licensed Material is translated, altered, arranged, transformed, or otherwise modified in a manner requiring permission under the Copyright and Similar Rights held by the Licensor.*[84]

50 Content produced by a generative AI system trained on CLSA resources, however, need not display protected traces of individual human expression that would require permission under copyright law.[85] Compared to the development phase, the situation is thus markedly different. During the development phase, protected human works are used as learning resources for the AI model. Hence, there is a direct link between the ML process and the use of protected human literary and artistic works made available under CLSA licensing terms. With regard to AI output (inference), however, the copyright basis for triggering CLSA obligations is less clear. Once again: instead of reproducing individual expression – protected free, creative choices by a human author[86] – AI output may merely reflect unprotected ideas, concepts and styles.

51 In light of the long-standing and well-established idea/expression dichotomy in copyright law, it is thus important to distinguish between two different types of AI output in the context of CLSA licensing: first, AI output that only contains unprotected ideas, concepts or styles (section E.II.1) and, second, AI output that displays traces of copyright-protected CLSA material on which the AI model was trained (section E.II.2). We now turn to a more detailed discussion of these scenarios.

83 Article 9(2) TRIPS; Article 2 WCT. As to the role of the idea/expression dichotomy in the generative AI debate, see M.A. Lemley and B. Casey (n 1), 772-776. With regard to the approach in the EU, see M.R.F. Senftleben, *The Copyright/Trademark Interface – How the Expansion of Trademark Protection Is Stifling Cultural Creativity* (The Hague, Kluwer Law International 2020), 27-28. See also Dutch Supreme Court, 29 March 2013, ECLI:NL:HR:2013:BY8661, *Broeren v Duijsens*, para. 3.5.

84 CC BY-SA 4.0, Section 1(a).

85 M.A. Lemley and B. Casey, 'Fair Learning', Texas Law Review 99 (2021), 743 772-776.

86 Case C-5/08, *Infopaq v DDF*, para 45; Case C-145/10 *Painer v Standard Verlags and Others*, para 89.

1. AI Output Consisting Of Unprotected Ideas, Concepts Or Styles

52 First, it is conceivable that AI output merely reflects unprotected ideas, concepts, styles etc. Due to the idea/expression dichotomy, it can be ascertained, as a default position, that this type of AI output falls outside the scope of copyright protection altogether. At the international level, Article 9(2) of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) and Article 2 of the WIPO Copyright Treaty confirm this conclusion. Practically speaking, this means that copyright law does not offer a basis for extending CLSA obligations to this type of AI output. Considering the whole analysis conducted so far, it can even be said that the copyright link with CLSA obligations is broken twice:

- as explained in section C.II, the end result of the development phase (the final trained model) need not contain traces of copyright-protected CLSA training material. If the artefact only contains data points and vectors which, as such, no longer constitute copies of copyright-protected individual expression taken from CLSA works, the artefact does not constitute adapted material within the meaning of the CC licence and copyright is no longer available to enforce CLSA conditions;

- moreover, if the AI modelonly generates output consisting of unprotected ideas, concepts and styles, copyright relevance must also be denied with regard to this output. If AI output does not include protected features of original CLSA material used for training purposes, copyright is no longer available as a legal tool to attach SA obligations to AI output.

53 If this result is deemed unsatisfactory, it is important to explore a remaining avenue for placing SA obligations on AI output: the use of contractual stipulations. We hinted at this possibility already at the end of the preceding section. The unavailability of copyright as an enforcement tool need not lead to a situation where CLSA conditions can no longer be imposed on model recipients and end users altogether. It only means that an alternative legal tool must be employed, namely a chain of contractual obligations that starts when CLSA works are included in training resources for AI models. To develop the whole chain, the CC licensor must make sure that contractual CLSA obligations are consistently passed on from the model trainer using CLSA works to model recipients and end users.

54 To achieve this result, it is conceivable to require AI developers using CLSA works to introduce contractual terms that oblige recipients of the final AI model – the stage five artefact in our analysis in section C.II – to accept SA obligations. In this way, CLSA conditions can be passed on to model recipients who would then be bound to observe SA obligations when including the final, CLSA-trained model in AI systems and enabling end users to generate AI output. To ensure that the chain of contractual CLSA obligations is not broken, providers of AI systems (recipients of the final model) must also be obliged to make sure that end users who generate AI output are bound to observe CLSA conditions with regard to the content that results from their prompts. Implementing this chain of CLSA obligations on the basis of contractual agreements, it no longer matters whether the artefact contains copyright-protected traces of CLSA works. It also does not matter whether AI output displays copyright-protected features of CLSA training material. On the basis of contract law, the obligation to observe CLSA conditions can be extended to model recipients and end users regardless of copyright claims.

55 As indicated above, the opt-out mechanism in the general TDM provision laid down in Article 4 CDSMD could serve as a legal vehicle to forge this chain of contractual obligations starting with the acceptance of CLSA obligations by the AI developer who, then, would have to pass on these obligations to model recipients and end users. Following this approach, users of CC licences could reserve copyright in accordance with Article 4(3) CDSMD strategically to extend contractual SA obligations to recipients of trained models and end users generating AI output. To achieve this result, CC licensors must seize the opportunity to reserve copyright and subject the use of CLSA material in the world of AI-generated content to conditions, such as SA. Seeking to implement this approach, it is thus necessary to declare an opt out under Article 4(3) CDSMD and

employ copyright as a legal tool to make the use of CLSA material in TDM activities (falling outside the scope of the research rule in Article 3 CDSMD) dependent on compliance with conditions that allow the downstream maintenance of SA obligations.

56 This approach need not lead to a categorical exclusion of CLSA material from AI training datasets. By contrast, a tailor-made licence solution can grant AI developers broad freedom to use CLSA resources for training purposes. In exchange for the training permission, however, AI developers would have to accept CLSA obligations, including the obligation to create a whole chain of contractual agreements that binds model recipients and end users:

- *model recipients*: AI trainers using CLSA resources must be obliged to make the final trained model available only if the model recipient accepts SA conditions and agrees to pass on these obligations to end users. As a result, recipients of AI models trained on CLSA resources would be obliged to ensure that SA conditions are also attached to AI output generated by users;

- *end users:* to implement this in practice, model recipients must be obliged to embed SA conditions in the contractual terms governing the use of their AI systems and require users to accept these conditions.This could be enforced by refusing to respond to prompts unless the user agrees to be bound by the SA obligation. As this extension of SA conditions to users would follow from contractual terms accompanying the use of the AI system, it is immaterial whether the AI output displays copyright-protected features of original CLSA material or consists of unprotected ideas, concepts or styles. As the SA obligation follows from a contract, the copyright status of the output is not decisive.

57 The underlying legal-doctrinal machinery can be described as follows: the TDM opt out mechanism in Article 4(3) CDSMD is used as leverage to impose contractual CLSA obligations. The CC licensor invokes Article 4(3) CDSMD to opt out and exclude the statutory use permission that would otherwise follow from Article 4(1) CDSMD. As a result, the licensor can rely on copyright to impose specific CLSA licensing terms. On the one hand, the licence offers broad freedom to use the CLSA material for AI training purposes. On the other hand, the licence obliges the AI developer to make available the final trained model under SA conditions – regardless of whether the artefact contains copyright-protected traces of the CLSA training material. On its merits, the reservation of copyright is thus used to create a bargaining opportunity to conclude a regular contract with specific CLSA obligations.

58 If an AI developer refuses to accept the CLSA conditions, or does not comply with them, acts of reproducing CLSA material during the training stages one to three (see section C.II) fall outside the licence and amount to copyright infringement. If the final artefact (stage five) does not include copyright-protected traces of CLSA training material, the establishment and further distribution of the trained model is unlikely to constitute copyright infringement. However, it culminates in a breach of the contractual CLSA conditions which the CC licensor made a precondition for the initial use permission underlying the whole ML process. Including the obligation to pass on SA obligations to users of generative AI systems, the CLSA conditions are extended to the exploitation phase where AI output is produced.

59 In the AI licensing arena, the success of the described SA extension strategy will depend on the attractiveness and importance of CC resources for AI training. If alternative training resources are available that do not require the acceptance of CLSA obligations, AI developers may prefer these alternative materials. Finally, it must be considered that the chances of enforcing CLSA conditions in AI contexts may depend on the role of CLSA resources in the data amalgam applied for AI training. If CLSA material only plays a minor role, it may be difficult to trace AI output back to CLSA training resources and provide evidence of the violation of CLSA licence terms.

2. AI Output Displaying Protected Traces Of CLSA Training Material

60 The second scenario that we outlined above concerns the situation where AI output reproduces copyright-protected features of CLSA works that have been

used as training resources. This second scenario can hardly be described as a 'mainstream' scenario. As stated above, the first scenario – AI output that only displays unprotected ideas, concepts or styles – seems much more common. Nevertheless, considering the large volume of AI output – systems capable of producing a myriad of content items in a relatively short period of time – it simply cannot be ruled out that, perhaps even with high statistical probability, some AI-generated content items display copyright-protected features of CLSA works that were part of work repertoires used during the ML process. In this case, the equation is markedly different.

61 Using EU copyright law as a reference point, it can be said that, as a rule of thumb, the moment AI output contains copyright-protected features of source materials used for training purposes, copyright law provides a basis for introducing CLSA obligations. As already explained above, the CJEU has confirmed that, for takings from original works to amount to a relevant partial reproduction in the sense of copyright law, it is necessary that copied elements fulfil the originality test. That is only the case when these elements – scrutinised in isolation – reflect a sufficient degree of free, creative choices to qualify as their author's 'own intellectual creation'.[87] In other words: if copyright-relevant traces of CLSA training resources can be identified in AI output, this AI output offers a basis for arguing that the AI system has generated 'adapted material' in the sense of the CLSA approach. As already concluded above in the light of the CJEU's *Deckmyn* decision,[88] it seems overly restrictive and perhaps strategically undesirable to require, when drafting CC licenses, that adapted material have original features of its own – coming on top of protected elements of the original CLSA material. Even if the terms of a contract define the term as requiring that modifications of the original CLSA material be independently eligible for copyright protection, it may still be possible to demonstrate that sufficient human creative choices have been made during an iterative prompt writing process, or have been added after receiving the AI output to refine the final result.[89] Either way, if AI output contains traces of the original 'licensed material', this creates a possibility for CC licensors to argue that the use and further distribution of this AI output amounts to copyright infringement unless the user observes the CLSA conditions under which the licensor is willing to give a licence. More concretely, whilst the licensed material found in AI output may be reproduced and shared, in whole and in part, no terms or technological measures may be imposed to restrict these uses, acts of sharing the material must retain copyright information, indicate modifications and licence information, and any further recipient of the material must be subjected to the same SA terms.

62 At this point of our analysis, it seems important to point out that, in the case of AI output displaying copyright-protected features of CLSA works, a finding of copyright infringement does not necessarily depend on whether the user triggering the content with its prompt is actually aware of the fact that the AI output infringes a pre-existing work. While the CJEU has introduced a subjective knowledge criterion in hyperlinking cases,[90] other infringement situations, such as the further sharing and making available of AI output with copyright-protected features of CLSA works in social media or on online platforms, do not offer users the opportunity to routinely rebut

87 Case C-5/08 *Infopaq v DDF*, paras 38-39.

88 Case C-201/13 *Deckmyn and Vrijheidsfonds VZW v Vandersteen and Others*, para 21.

89 As to the traditional copyright originality test requiring free, creative choices of a human author, see once again Case C-5/08 *Infopaq v DDF*, para 45; Case C-145/10 *Painer v Standard Verlags, and Others*, para 89. As to the impact of this originality test on copyright protection for AI productions in the literary and artistic field, see P.B. Hugenholtz and J.P. Quintais, 'Copyright and Artificial Creation: Does EU Copyright Law Protect AI-Assisted Output?', International Review of Intellectual Property and Competition Law 52 (2021), 1190 1212-1213; D. Burk, 'Thirty-Six Views of Copyright Authorship, by Jackson Pollock', Houston Law Review 58 (2020), 263 270-321; J.C. Ginsburg and L.A. Budiardjo, 'Authors and Machines', Berkeley Technology Law Journal 34 (2019), 343 395-396; M.-C. Janssens and F. Gotzen, 'Kunstmatige Kunst. Bedenkingen bij de toepassing van het auteursrecht op Artificiële Intelligentie', Auteurs en Media 2018-2019, 323 325-327; R. Pearlman, 'Recognizing Artificial Intelligence as Authors and Investors under U.S. Intellectual Property Law', Richmond Journal of Law and Technology 24 (2018), 1 4.

90 Case C-160/15, *GS Media v Sanoma Media Netherlands and Others*, paras 49-51.

infringement arguments by simply stating that they had no knowledge of traces of protected works in the AI output. In a litigation setting where two people created the same content (or roughly similar content), the defendant to an infringement claim (in our case the user triggering infringing AI output) would have to give a credible story of how they came up with the individual expression independently.[91] Demonstrating that the user was not aware of the use of copyright-protected CLSA material for AI training purposes might not suffice. While this is of course an issue which the CJEU might have to clarify at some point, the default position in current copyright law remains that someone appears to have exploited the pre-existing copyright-protected work whenever a copy of that work is created. The ball is then in the alleged infringer's court. In other words: the AI user would have to advance convincing arguments to rebut the infringement claim.

63 Arguably, this liability risk offers opportunities to infuse CLSA conditions. In principle, every user of CLSA resources (anyone further downstream) can receive an offer from the original CC licensor to use the licensed material and include traces of this licensed material in adapted material (such as portions of AI output that relate to the licensor's content). The mere availability of the licence and the offer of an authorisation under CLSA conditions, however, does not imply that every downstream user is aware of this opportunity to receive permission and escape the verdict of infringement. Hence, it is necessary that the downstream user triggering the production of AI output be informed about the licence offer and encouraged to accept this offer.

64 To achieve this result, we must navigate between two different contributions leading to AI output that contains protected features of original CLSA material: the AI provider makes available the system that produces this content. However, the final production of the AI output is triggered by a different person, namely the end user. With regard to this amalgam of system provider and user involvement, several considerations seem relevant. The user does not have access to the training dataset, nor is the user likely to be aware of what was part of the training dataset. An AI system provider using a CLSA-trained model, by contrast, may be aware of CLSA material used during the ML process – either because the provider conducted the AI training himself (same person), or because the AI trainer (being another person) passed on SA obligations in accordance with the contractual strategy developed in the preceding section. The AI system provider, however, does not enter the prompt.

65 Nonetheless, it may be possible to establish a sufficient link with the AI system provider when it is considered that this person exercises possessive control over the AI system and has designed the user interface enabling the user to request the generation of AI output, in accordance with the freedoms and limitations set by the system provider. From the perspective of EU copyright law, it is conceivable that this role is sufficient to impose an obligation to ensure observance of the CLSA terms with regard to the AI output. Arguably, a parallel can be drawn with the CJEU decision in *The Pirate Bay* where the Court considered that the operation of an online platform that indexed information about copyright-protected material without hosting that material, and which made it easier to locate that material, carried out an act of communication to the public within the meaning of Article 3 ISD.[92] The Court had paved the way for this broad application of the right of communication to the public – *de facto* collapsing the traditional distinction between primary liability of the user who uploads infringing content, and secondary, contributory liability of the platform – in the earlier decision in *Filmspeler*. In that case, the Court had dealt with the offer of multimedia players with pre-installed add-ons that specifically enabled purchasers to have access to protected works published illegally on streaming websites.[93] Instead of raising the question whether harmonised EU law provided a basis for assuming secondary, contributory liability to infringing content sharing, the CJEU held that the sale of such a multimedia player constituted a primary act of communication

91 Cf. N. Elkin-Koren and others, 'Can Copyright be Reduced to Privacy?' (*arXiv*, 24 March 2024), 1-2 <https://arxiv.org/abs/2305.14822>.

92 Case C-610/15 *Stichting Brein v Ziggo and XS4ALL Internet (The Pirate Bay)*, paras 36-39 and 47.

93 Case C-527/15 *Stichting Brein v Wullems (Filmspeler)*, para. 41.

to the public in the sense of Article 3(1) ISD.[94]

66 To support this remarkable extension of the concept of 'communication to the public' to the preparatory phase of offering and selling a multimedia player – a phase in which the purchaser has not yet set in motion the process of accessing illegal content – the Court focused on knowledge of infringing conduct and the aim to exploit illegal streaming content. The 'Filmspeler' multimedia player was sold with full knowledge that the add-ons, which included pre-installed hyperlinks gave access to works published illegally on the internet.[95] Following this approach, it cannot be ruled out that the AI system provider must be deemed the adapter, or co-adapter, in the case of AI output that displays protected features of CLSA material. In practice, this co-responsibility means that, even if a system user triggers the production of the AI output, the AI system provider is obliged to ensure that the SA conditions are observed. Otherwise, the CC licensing conditions are not fulfilled and the AI system provider exposes himself and users of the AI system to the described copyright infringement risk.

67 In line with the outlined CJEU approach, this responsibility of the AI system provider follows from the fact that, having included CLSA resources in the training dataset himself, or having been informed about this by the AI trainer, the AI system provider must be well aware that output produced by the AI system may contain protected traces of original CLSA works. Hence, it can be argued that the AI system provider offers the AI system in full knowledge of the fact that AI output with protected CLSA ingredients may result from the use of the system. To reduce this liability risk, the AI system provider should introduce the CLSA obligations accompanying the training material and pass on these obligations to users. As discussed in the preceding section, the AI system provider can, for instance, make the generation of AI output following a user prompt dependant on acceptance of the CLSA terms that are attached to the material used for training purposes.

68 The same strategy can be applied when the described parallel with the CJEU's *Filmspeler* approach is deemed unconvincing and the user entering the prompt for the AI output is regarded as the only person responsible for the AI production containing copyright-protected traces of CLSA training material. To reduce liability risks for users in this situation, it is desirable that AI system providers include CLSA obligations in the terms of use relating to AI systems that are based on CLSA-trained models. To pass on CLSA obligations to users of the final AI system and reduce their liability risk, it is advisable to follow the approach described in the preceding section and adopt additional contractual obligations, namely the obligation to include CLSA clauses in the terms of use accompanying the AI system. In this way, it can be ensured that users become aware of CLSA obligations. In addition, it can be stated that, by using the AI system and entering prompts, the user implicitly accepts the CLSA terms and the obligation to distribute AI output under SA conditions. As already proposed, users could be obliged to accept CLSA terms before the AI system produces output following a user prompt.

69 However, it is important to recall again that the concept of 'adapted materials', as defined in the CC BY-SA 4.0 licence, does not include material created on the basis of copyright exceptions and limitations. Therefore, any relevant copyright exception that could apply to AI output insofar as the copyright status of the material is concerned, will affect the status of the generated material. Even if a prompt leads to AI output with protected CLSA features, copyright exceptions, such as the exemption of quotations, parodies, caricatures and pastiches in EU copyright law,[96] may prevail over CLSA

94 id., para 52.

95 id., paras 50-51.

96 ISD, Article 5(3)(d) and (k). Cf. G. Westkamp, 'Borrowed Plumes: Taking Artists' Interests Seriously in Artificial Intelligence Regulation', 1 19-26, forthcoming; M.R.F. Senftleben, 'User-Generated Content – Towards a New Use Privilege in EU Copyright Law', in T. Aplin (ed), *Research Handbook on IP and Digital Technologies* (Cheltenham: Edward Elgar 2020), 136 (145-162); S. Jacques, *The Parody Exception in Copyright Law* (Oxford: Oxford University Press 2019), 91-133; E. Hudson, 'The pastiche exception in copyright law: a case of mashed-up drafting?', Intellectual Property Quarterly (2017), 346 362-364; F. Pötzlberger, 'Pastiche 2.0: Remixing im Lichte des Unionsrechts', Gewerblicher Rechtsschutz und Urheberrecht 2018, 675 681; J.P. Quintais, *Copyright in the Age of Online Access – Alternative Compensation Systems in EU Law* (Alphen aan den Rijn: Kluwer Law International

obligations in cases where, as a result of iterative prompt writing and use of the AI system as a tool for human expression, or the addition of human creative choices to AI output,[97] the AI system user can invoke these copyright exceptions.

F. ShareAlike/Copyleft Options In The Era Of Generative AI

70 Our analysis demonstrates that challenges concerning successful deployment of copyleft licences relate predominantly to the design of the licenses, which are bound to differ in scope because of a fragmented copyright framework across the globe. If it is deemed desirable to preserve the CLSA approach in the era of generative AI and attach SA obligations to AI output, it will be necessary to revise the licences. Ultimately, it may be inevitable to rely on the bargaining power that the reservation of copyright offers to ensure the continued viability of CLSA licences. Indeed, this is the very idea of copyleft licensing – to *rely* on the prerogatives that copyright law provides in order to ensure that downstream creations that are derived from the original material are made available on the same terms to others. Taking EU copyright law as a reference point, two markedly different policy options are available:

71 On the one hand, the CC community can uphold the supremacy of copyright exceptions. In countries and regions that exempt ML processes from the control of copyright holders, this approach leads to far-reaching freedom to use CC resources as training material for AI systems. At the same time, it is likely to marginalise SA obligations in the realm of literary and artistic AI productions. In the EU, for instance, an approach that allows TDM exceptions to prevail over CLSA licensing conditions implies that AI developers are free to invoke Articles 3 and 4 CDSMD and use original CLSA material for AI training purposes without seeking permission – and without accepting SA obligations. In consequence, it seems particularly difficult, if not impossible, to impose SA obligations with regard to output generated by the fully trained AI system. As AI developers need not subscribe to CLSA conditions, there is hardly any possibility of requiring them to observe these conditions when generating AI output themselves, or pass on CLSA obligations to users who trigger the production of AI output with their prompts. In sum, supremacy of copyright exceptions can easily lead to a situation where SA obligations play hardly any role in the context of generative AI systems and literary and artistic output produced by these systems.

72 On the other hand, the CC community can use copyright strategically to extend SA obligations to AI training results and AI output. To achieve this goal, it is necessary to seize opportunities to reserve copyright and subject the use of CC material in the world of AI development and exploitation to conditions, such as SA. Following this approach, it is advisable to declare an opt out under Article 4(3) CDSMD and employ copyright as a legal tool to make the use of CLSA material in TDM activities (falling outside the scope of the research rule in Article 3 CDSMD) dependent on compliance with conditions that allow the maintenance of SA obligations. This approach need not lead to a categorical exclusion of CLSA material from AI training datasets. By contrast, a tailor-made licence solution can grant AI developers broad freedom to use CLSA resources for training purposes. In exchange for the training permission, however, AI developers would have to accept CLSA obligations. With regard to the AI development phase, this could include the obligation to make the trained model available in accordance with SA conditions. At the AI exploitation stage, AI developers would be obliged to ensure – via a whole chain of contractual obligations – that SA conditions are also attached to AI output generated by AI systems that use CLSA-trained models. As AI output may result from user prompts, this includes an obligation to embed SA conditions in the contractual terms governing the use of the AI system and require users to accept these conditions, for instance by refusing to respond to prompts unless the user agrees to be bound by the SA obligation.

2017), 235; M.R.F. Senftleben, 'Quotations, Parody and Fair Use', in P.B. Hugenholtz, A.A. Quaedvlieg, and D.J.G. Visser (eds), *A Century of Dutch Copyright Law – Auteurswet 1912-2012* (Amstelveen: deLex 2012) 359 365.

97 Cf. P.B. Hugenholtz/J.P. Quintais (n 89), 1212-1213; D. Burk (n 89), 270-321; J.C. Ginsburg and L.A. Budiardjo, 'Authors and Machines', Berkeley Technology Law Journal 34 (2019), 343 (395-396); M.-C. Janssens and F. Gotzen (n 89), 325-327; R. Pearlman (n 89) 4.

As this extension of SA conditions to users would follow from contractual terms accompanying the use of the AI system, it is immaterial whether the AI output displays copyright-protected features of original CLSA material or consists of unprotected ideas, concepts or styles. As the SA obligation follows from a contract, the copyright status of the output is not decisive. However, the copyright status becomes relevant in the case of further downstream use. If the AI output does not contain copyrighted elements, it is unclear how the SA condition can be asserted against downstream users who are not bound by the conditions accompanying the use of the AI system.

73 In addition to these general policy options, the analysis has yielded several more specific insights:

- The SA condition, as expressed in the CC BY-SA licence, is designed with reference to adapted material. For traditional forms of artistic expression that involve investment of time, resources and creativity to adapt pre-existing works, this is a logical design. In the context of ML processes and the generation of AI output, however, the focus on adapted material may be less efficient as it introduces unnecessary complexity to cover activities that for the most part involve technical modifications at the development stage and comparatively few human creative choices in the exploitation phase leading to literary and artistic AI output. It may therefore be preferable to focus on use of original CLSA material in AI training and the potential reappearance of traces of this original material in AI output. In other words: the use and reappearance of CLSA material in these context should be decisive and trigger SA obligations – not the question whether AI processes lead to adapted material.

- A CC licence that includes a ban on TDM activities will remove the applicability of the Article 4(1) CDSMD copyright exception in favour of letting the use be governed by a more specific, tailor-made use permissions. That is, the objective would be to trigger CLSA licence conditions where they otherwise would have been governed by an exception. As follows from the CC Statement on the Opt-Out Exception Regime,[98] the CC BY-NC-SA licence has the potential of effecting an opt-out for non-commercial use. But pursuant to our analysis, for the opt-out to foster CLSA culture more broadly in AI contexts, it may be advisable to abandon the traditional precedence of copyright exceptions in favour of an opt-out protocol that allows a more fine-grained TDM permission that includes SA obligations. As CC has already undertaken initiatives to enable the association of machine-readable licensing metadata with objects offered under CC licences through the CC Rights Expression Language (ccREL), an opt-out declaration of this nature could also be expressed by machine-readable means.

- Interestingly, developers of AI models may experience SA extension difficulties that are comparable to those faced by creators of CLSA material. Copyleft options designed for software may be deemed more or less inadequate for distributing AI models. In this respect, the evolution of AI model licences (ML model licences), for example OPT-175B, CreativeML Open RAIL-M, BigScience OpenRAIL-M, GLM-130B, provides useful insights into trends in the machine-learning sector. These developments in the sector may offer important reference points for adaptations of existing CLSA licence schemes with regard to use of CC resources as training data. For instance, an alternative approach to adapting CLSA licences that is worth exploring is the viability of adapting ML model licences to be compatible with the former by accounting for the training data as a mode of realising responsible AI licensing (RAIL). Such endeavours could additionally align with the proposed obligations imposed on AI model developers to put in place a copyright compliance policy and the making available of detailed summaries about the materials used for training general-purpose AI models pursuant to Article 53(1)(c)-(d) of the AI Act. Arguably, these obligations also apply to developers of AI models released under free and open licences.

- Finally, our analysis has been limited with

98 A. Lazarova and others (n 61).

regard to the spectrum of further technological development that we could cover. We have mostly approached the issues from the perspective of so-called supervised learning. However, advances in self-supervised learning has led to ML processes on unstructured data. Self-supervised learning is likely to involve increasingly less copying, with a comparatively lesser amount of different acts and human interventions. It may ultimately lead to a focus on developing foundational models that have undergone training, diminishing the need for developing them from scratch. You only need to invent the pneumatic tire once and then you concentrate on making it better to achieve the desired shock absorption, traction or manoeuvrability properties. In a similar vein, training datasets might eventually become a thing of the past once AI systems no longer need training but only tweaking. This might not remove the need for supplying new facts or knowledge but it may optimise the entire learning process. Moreover, with advances in generative AI, training may increasingly involve training based on synthetic data generated by AI and lead to systems learning from each other in the same way as AI is used today for finding errors in computer code or optimising it. Perhaps the best way of thinking about AI is as if it were an operating system. In the end, there will be only a few developers because everybody else will be developing or finding applications for it.

Fair Compensation for Private Copying: Is There a Need to Amend Luxembourg's Copyright Law?

by **Martin Stierle** *

Abstract: Private copying exceptions are a core feature of many copyright laws around the world. EU Member States may provide for such an exception on the condition that the rightholders receive fair compensation. Although the European Court of Justice (ECJ) interprets the fair compensation requirement as an autonomous concept of EU law, it concedes Member States broad discretion when determining the design of their compensation scheme. Most of them have adopted a private copying exception, regularly in conjunction with a levy system operated by collecting societies. Luxembourg's Copyright Act enshrines a private copying exception on the condition that the rightholders receive fair compensation. The law refers to a Grand-Ducal regulation to lay down the conditions for determining and collecting it, but no corresponding act has ever been promulgated. This article interprets the existing legal framework in Luxembourg considering the ECJ's interpretation of Article 5(2)(b) DIR 2001/29/EC and assesses the need to amend Luxembourg's copyright law. It proposes establishing a fair compensation scheme funded through the general state budget and managed through an existing collective management organisation thereby taking into account the government's existing financial support of social and cultural establishments that already benefit reproduction rightholders.

Keywords: Private Copying; Fair Compensation; Luxembourg's Copyright Law; Article 5(2)(b) InfoSocDir

Recommended citation: Martin Stierle, Fair Compensation for Private Copying: Is There a Need to Amend Luxembourg's Copyright Law?, 15 (2024) JIPITEC 338 para 1

A. Private Copying and Fair Compensation: Setting the Scene

1 An individual's ability to create a private copy of an otherwise copyright-protected work ("private copying") legally is a core feature of many copyright laws around the world.[1] Although its implementation varies considerably among national laws,[2] private copying is typically defined as an exception to

* Associate Professor in Intellectual Property Law, University of Luxembourg; Co-Director of the Center for Intellectual Property Law, Information & Technology (CIPLITEC). The latest version of this paper is dated 18 September 2024.

1 For a global overview, see BIEM, CISAC and Stichting de Thuiskopie, *Private Copying, Global Study* (2020) <https://members.cisac.org/CisacPortal/cisacDownloadFileSearch.do?docId=39523&lang=en> accessed 18 September 2024. Originally, the ability to reproduce copyrighted materials for private use was intended to be enshrined as one of three express exceptions set out in art 9(2) of the Berne Convention; the UK, however, suggested a more general wording. See MRF Senftleben, *Copyright, Limitations and the Three-step Test. An Analysis of the Three-Step Test in International and EC Copyright Law* (Kluwer International 2004) 50.

2 See eg MA Esteve Pardo & A Lucas-Schloetter, 'Compensation for Private Copying in Europe: Recent Developments in France, Germany and Spain' (2013) 35(8) EIPR 463 (regarding national legislation within the EU); BIEM/CISAC/Stichting de Thuiskopie (n 1) (overview of various national systems).

or limitation of the author's exclusive right to reproduce that author's work ("reproduction right").[3] The concept of private copying encompasses a variety of different reproduction activities, such as photocopying a magazine article, downloading a file for personal use, recording broadcasts to a storage medium to be viewed or listened to at a more convenient time, and making backup copies of lawfully purchased media recordings to ensure access if the original file becomes corrupted.[4]

2 The private copying exception largely developed when magnetic tape recorders were first introduced on the consumer market, with most national courts acknowledging that copyright protection covered private as well as commercial acts, resulting in a need to address private copying.[5] The concept of the exception is rooted in legal realism,[6] as it was designed to overcome two practical governance and enforcement challenges related to the reproduction of a work in the private sphere: Firstly, it was widely considered that unlimited private copying would result in market failure or, more precisely, the lack of a market, as such, for copied works.[7] From a practical perspective, most individual authors ("reproduction rightholders") lack the resources needed to manage individual requests for private copies from a potentially enormous number of private users in multiple locations and at various times.[8] Moreover, outsourcing the management of such requests to a commercial enterprise would not be financially feasible for many reproduction rightholders. Likewise, private users wishing to make a copy of a legitimately acquired work for private purposes may also lack the resources needed to seek authorisation from a potentially large number of unknown reproduction rightholders for their typical, private-copying activities. The job of identifying, locating, and communicating with all reproduction rightholders would likely be, in most situations, a burden beyond most private users' means and abilities due to the high transaction costs.[9] Secondly, in practice, with or without such an exception, most private users are able to copy works without ever seeking a licence to do so: it is practically impossible for reproduction rightholders to monitor such private copying[10] unless there is a legal regime that encroaches upon the private end-user's privacy rights.[11] When high transaction costs make bargaining between individual copyright owners and potential users of copyrighted material

3 Art 5(2) of the Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society [2001] OJ L 167/10 leaves it open as to whether private copying is implemented as an exception or limitation of the reproduction right (art 2 of the same Directive). The European Court of Justice also referred to allowing private copying as 'derogation' (Case C-426/21, *Ocilion IPTV Technologies*, ECLI:EU:C:2023:564, para 30). For a discussion on terminology, see S Karapapa, *Private Copying* (Routledge 2012) 9 f with further references. As the exception/limitation concept is most commonly described as a private copying "exception", we use "exception" throughout this article.

4 For examples, see JP Quintais, 'Private Copying and Downloading from Unlawful Sources' (2015) IIC 66, 70.

5 See PB Hugenholtz, 'The Story of the Tape Recorder and the History of Copyright Levies' in B Sherman & L Wiseman (eds), *Copyright and the Challenge of the New* (Wolters Kluwer 2012) 179, 184 ff. See also Quintais (n 4) 75 f.

6 It is fair to say that, historically, legal realism was, and remains, the governing consideration of private copying exceptions. See A Lucas-Schloetter, 'La rémunération pour copie privée dans la tourmente (1re partie)' (2013) Légipresse 597, sec I.A (noting that the concept of private copying exceptions comes into play when it is difficult or even impossible to ensure respect for the rightholder's exclusive right); C Geiger, F Schönherr & S Karapapa, 'The Information Society Directive' in I Stamatoudi & P Torremans (eds), *EU Copyright Law: A Commentary* (Edward Elgar 2021)para 11.119 (referring to 'reasons of practicability' as the justification for the private copying exception).

7 Karapapa (n 3) 25 ff. with further references.

8 J Reinbothe, 'Private Copy Levies' in IA Stamatoudi (ed), *New Developments in EU and International Copyright Law* (Kluwer 2016) 299, 302; M Ficsor, *Collective Management of Copyright and Related Rights* (3rd edn WIPO Publication 2022) 14.

9 Ficsor (n 8) 14.

10 Case C-467/08 *Padawan*, ECLI:EU:C:2010:620, para 46; Case C-263/21, *Ametic*, ECLI:EU:C:2022:644, para 37 (both decisions referring to practical difficulties in identifying private users and obliging them to compensate rightholders for the harm caused to them).

11 Privacy concerns were addressed for the first time by the German Federal Court of Justice in its seminal decision, *Personalausweise* (BGH GRUR 1965, 104, 107) which became a corner stone of levy systems in Germany and other countries. See Hugenholtz (n 5) 187 f.

impossible or prohibitively costly, or when copyright owners are unable in practice to enforce their rights effectively against unauthorised uses, market failure is said to occur. In such circumstances, economic efficiency demands that alternate ways be found[12] and many countries opted for the private copying exception.

3 By enshrining a private copying exception in national law, copyright laws limit the reproduction rightholder's control over the use of their work. As a *quid pro quo* for this limitation, many countries have adopted statutory licensing systems.[13] When combining the private copying exception with financial compensation, the law strikes a balance between the interests of society and those of the reproduction rightholder.[14] One could refer to this combination as a liability rule or liability approach to private copying, as opposed to a property rule or property approach.[15] Such a liability rule does not protect the reproduction rightholder's interest in the work through exclusivity, but rather through obligatory financial compensation established, for example, by national legislation and/or national courts.

4 Many countries apply the liability rule using an indirect collectivisation mechanism comprised of a special levy paid into a collective pool.[16,17] The special levy, separate from a general sales tax, is imposed when purchasing reproduction media (e.g., hard drives, SD cards) or devices (e.g., copy machines, scanners, smartphones). Those levies, however, are not forwarded directly to individual reproduction rightholders; rather, they are paid into a collective copyright pool[18] representing all reproduction rightholders. The funds in the pool are then distributed to the rightholders on the basis of an abstract scheme. Such distribution is intended to reflect "fair compensation" for private copying.

5 The concept of fair compensation for private copying has triggered one of the most polarising discussions within the European copyright community. Various scholars have contested the ongoing justification for a private copying exception that includes a compensation requirement in today's digital environment.[19] In accordance with 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 ("InfoSocDir"), most EU Member States – but not all – have implemented a functional compensation scheme in conjunction with their own private copying exception. Although

12 L. Guibault, *Copyright Limitations and Contracts: An analysis of the overridability of limitations on copyright*, (Kluwer Law International 2002) 79.

13 Karapapa (n 3) p. 11 f (describing the private copying exception in EU law as a statutory licence, while distinguishing statutory licences and the mandatory collective administration of rights). The idea that payment of equitable remuneration can be understood to have a mitigating effect can be traced back to German copyright law of the 1950s and 1960s, which had an impact during the discussions of the 1967 Stockholm Conference. Senftleben (n 1) p. 56.

14 See eg Reinbothe (n 8) p. 302 (referring to the public interest in unhindered access and the interests of the economic interests of the rightholders).

15 For the difference between so-called property rules and liability rules, compare G Calabresi and AD Melamed, 'Property Rules, Liability Rules, and Inalienability: One View of the Cathedral' (1972) 85 Harv L Rev 1089 and C Geiger, 'Promoting Creativity through Copyright Limitations: Reflections on the Concept of Exclusivity in Copyright Law' (2010) 12 Vand J Ent Tech L 515, 529 (arguing against use of the term 'liability rule' for private copying remuneration).

16 BIEM/CISAC/Stichting de Thuiskopie (n 1).

17 For an overview of the functioning of a system of collectivisation, see Ficsor (n 8) pp. 13 ff.

18 Directive 2014/26/EU of the European Parliament and of the Council of 26 February 2014 on collective management of copyright and related rights and multi-territorial licensing of rights in musical works for online use in the internal market Text with EEA relevance [2014] OJ L 84/72 ("Collective Management Directive").

19 See eg PB Hugenholtz, L Guibault and S van Geffen, 'The Future of Levies in a Digital Environment' [March 2003] <https://www.ivir.nl/publicaties/download/DRM&levies-report.pdf> accessed 18 September 2024 (arguing that it has been possible to control private copying of protected since the advent of digital rights management) with further references.

Luxembourg,[20] as well as Bulgaria[21] and Malta,[22] have incorporated a private copying exception into their copyright laws, they either have no compensation mechanism in place (Luxembourg),[23] or have adopted a compensation requirement that no longer works (Bulgaria),[24] or only works to a very limited extent (Malta).[25] This state of affairs is particularly surprising for Luxembourg, as it claims to offer an "exemplary level of protection" for ideas and creations through intellectual property rights.[26] Some even assert that Luxembourg's absence of a private copying levy makes the Grand Duchy a popular "copying levy haven" for blank media buyers from neighbouring countries.[27]

6 This article revisits Luxembourg's private copying exception considering EU law and the interpretation thereof by the European Court of Justice (ECJ). It looks at the existing legal framework in Luxembourg (section B) and the requirement for fair compensation set out in the InfoSocDir[28] (section C). Against this backdrop, it discusses the interpretation and application of Luxembourg's existing private copying exception *sans* compensation (section D) and addresses the need for an amendment to its existing national copyright framework (section E). The paper elaborates on the main considerations when setting up a fair compensation scheme (section F) before offering a conclusion that proposes a way forward (section G).

7 Although this article primarily addresses Luxembourg's specific situation, it also intends to inform similar discussions in other EU Member States, most notably Bulgaria and Malta, where compensating reproduction rightholders for private copying has been, or currently is, the subject of heated debate. In particular, the questions of whether the EU requires its Member States to adopt a fair compensation requirement, and how to implement and maintain such a mechanism without a heavy regulatory burden, are of similar concern to other small and medium-sized Member States that fear the introduction of a levy system due to the expected disproportionately high administrative costs.

B. The Legal Framework in Luxembourg

8 Luxembourg has a long history of copyright protection, dating back to the 19th century.[29] In 2001, just a month before the EU adopted the InfoSocDir,[30] the Grand Duchy consolidated its existing legislation on copyright and similar rights into its 2001 Copyright Act,[31] which remains the foundation of

20 JL Putz, *Le droit d'auteur* (2nd edn, Lacier 2013) para 338 ff; K Manhaeve and T Schiltz, 'Luxembourg' in B Lindner & T Shapiro (eds), *Copyright in the Information Society. A Guide to National Implementation of the European Directive* (2nd edn, Edward Elgar 2019), para 20.043 ff.

21 V Sokolov, 'Bulgaria' in Lindner/Shapiro (eds) (n 20) para 5.40.

22 PPM Grimaud & SL Azzopardi, 'Malta' in Lindner/Shapiro (eds) (n 20) para 21.32.

23 For the situation in Luxembourg as of this writing, see secs B and D.

24 After unprecedented lobbying by Bulgaria's consumer electronic industry, Bulgaria enacted amendments to its copyright law in 2011. At that point, Copy BG, the collective management organization appointed by reproduction rightholders, stopped collecting levies. A complaint with the European Commission was made, but the matter has yet to be solved as of this writing. Sokolov (n 21) para 5.41; BIEM/CISAC/Stichting de Thuiskopie (n 1) p. 260.

25 In Malta, a levy system for private copying was planned but never implemented. As a result, no remuneration is collected. Grimaud/Azzopardi (n 22) para 21.35; BIEM/CISAC/Stichting de Thuiskopie (n 1) p. 280.

26 Indeed, Luxembourg's national website states: 'Intellectual property. Your ideas and creations are entitled to exemplary protection' <https://luxembourg.public.lu/en/invest/innovation/intellectual-property.html> accessed 18 September 2024.

27 See eg Wikipedia <https://en.wikipedia.org/wiki/Private_copying_levy#Luxembourg> accessed 18 September 2024.

28 InfoSocDir (n 3) art 5(2)(a) and (b).

29 Putz (n 20) para 60.

30 InfoSocDir (n 3).

31 *Loi du 18 avril 2001 sur les droits d'auteur, les droits voisins et les bases de données,* Mémorial A 50 (author translation: "Act of 18 April 2001 on authors' rights, related rights, and databases") (the "2001 Copyright Act"). Since its initial enactment, the 2001 Copyright Act has been amended and consolidated several times, most recently by *Loi du 1er avril 2022 portant modification de la loi modifiée du 18 avril 2001*

Luxembourg's copyright law to this day. Section 2 of the 2001 Copyright Act, entitled "Exceptions to Author's Rights",[32] included the original version of Article 10, which specifically noted in (4°):

> Where a work has been lawfully made available to the public, the author may not prohibit [...] the reproduction of the work made free of charge by the copier and for strictly private use, not intended for public use or communication, and provided that such reproduction does not prejudice the publication of the original work.[33]

9 A few years later, in 2004, Luxembourg amended the 2001 Copyright Law to align it with the InfoSocDir (the "2004 Amendment").[34] In that regard, it modified the original Article 10 to incorporate the *quid pro quo* contemplated by Article 5(2) of the InfoSocDir into Article 10 (1) (4°):

> Where a work [...] has been lawfully made available to the public, the author may not prohibit [...] the reproduction on any medium by a natural person for his or her private use and for ends that are neither directly nor indirectly commercial, on the condition that the rightholders receive fair compensation that takes into account the application of the technological measures referred to in articles 71[ter] to 71[quinquies] of this law to the works concerned. The conditions for fixing and collecting such compensation, as well as its level, are laid down by Grand-Ducal regulation.[35]

10 Article 10(1)(4°) has remained unchanged and intact for the last 20 years.

11 Although the 2004 Amendment made private copying conditional on fair compensation of rightholders and implied that a Grand-Ducal Regulation ("GDR") establishing a compensation scheme was to be set up, no such GDR has ever been promulgated.[36] The GDR of 16 March 2005, for example, defines the composition of Luxembourg's Copyright and Related Rights Commission, but does not mention any compensation scheme for private copying.[37] Therefore, Luxembourg's copyright law still does not specify who is responsible for paying fair compensation, how it should be calculated, or how reproduction rightholders are to receive their share.

12 The debate about how to calculate, collect, and distribute fair compensation was already in full swing before the 2001 Copyright Act was enacted. As part of that legislative discussion, the Minister for the Economy expressed doubts about the efficacy of the compensation mechanism being used in other EU Member States, specifically private copying levies.[38]

sur les droits d'auteur, les droits voisins et les bases de données en vue de la transposition de la directive 2019/789 du Parlement européen et du Conseil du 17 avril 2019 établissant des règles sur l'exercice du droit d'auteur et des droits voisins applicables à certaines transmissions en ligne d'organismes de radiodiffusion et retransmissions de programmes de télévision et de radio, et modifiant la directive 93/83/CEE du Conseil, Mémorial A 159, (collectively, the 2001 Copyright Act, the 2004 Amendment (n 34), and all other amendments thereto, are referred to as "Luxembourg's Copyright Act" or the "amended Copyright Act").

32 Author translation of "*Des exceptions aux droits d'auteur*," the title of sec 2 of the 2001 Copyright Act.

33 Author translation of the original art 10(4°) of the 2001 Copyright Act, which reads, in the relevant part: *"Lorsque l'œuvre a été licitement rendue accessible au public, l'auteur ne peut interdire: [...] la reproduction d'une œuvre effectuée à titre gratuit par le copiste et pour son usage strictement privé, non destinée à une utilisation ou à une communication publiques [sic], et à condition que cette reproduction ne porte pas préjudice à l'édition de l'œuvre originale."*

34 *Loi du 18 avril 2004 modifiant 1. la loi du 18 avril 2001 sur les droits d'auteur, les droits voisins et les bases de données, et 2. la loi modifiée du 20 juillet 1992 portant modification du régime des brevets d'invention.* (the "2004 Amendment").

35 (emphasis added). Author translation of the amended art 10(1)(4°) incorporated in the 2004 Amendment, which reads, in relevant part: *"Lorsque l'œuvre, autre qu'une base de données, a été licitement rendue accessible au public, l'auteur ne peut interdire [...] la reproduction sur tout support par une personne physique pour son usage privé et à des fins non directement ou indirectement commerciales, à condition que les titulaires de droits reçoivent une compensation équitable, qui prend en compte l'application des mesures techniques visées aux articles 71ter à 71quinquies de la présente loi aux œuvres concernées. Les conditions de fixation et de perception, ainsi que le niveau de cette compensation sont fixés [sic] par règlement grand-ducal."*

36 Putz (n 20) para 346; Manhaeve/Schiltz (n 20) para 20.076.

37 *Règlement grand-ducal du 16 mars 2005 portant organisation de la Commission des droits d'auteur et des droits voisins*, Mémorial A 52.

38 Doc. parl. 5128, 3 f.

He stated that he did not intend to introduce what he described as a "tax on computers, hard disks, printers, faxes, photocopying machines, blank cassettes or DVDs, unless there was an obligation at the European level to do so."[39] This reluctance was reiterated in 2003 when Luxembourg's Chambre des Députés discussed aligning the law with the InfoSocDir.[40] According to parliamentary documents, a lump-sum royalty was considered contrary to Luxembourg's vision of the information society and free access to information.[41] The Ministry of the Economy understood a flat-rate levy on equipment and recordables as a heavy regulatory and administrative burden, imposing significant administrative constraints on economic operators.[42]

13 Ultimately, the Chambre des Députés decided against introducing a levy system, opting instead to explore alternative, more balanced forms of compensation.[43] The government also began contemplating new forms of electronic rights management, such as digital rights management ("DRM").[44] In the early 2000s, it was widely assumed that technical advancements would eliminate the need for levy systems, allowing for greater control over the use of copyright-protected works and addressing the practical challenges of governing and enforcing reproduction rights in the private sphere.[45] This would work on a bilateral basis without any need to develop a regulatory framework. However, expectations surrounding DRM were only marginally realised, as it became unpopular with certain consumers and failed to address all dimensions of private copying.[46]

C. The Fair Compensation Requirement in EU Copyright Law

I. Fair Compensation as a Condition

14 Private copying and the private copying exception first appeared on the European Commission's harmonisation agenda in 1988.[47] Although a specific private copying directive was never adopted, the InfoSocDir of 2001 established parameters that Member States were (and still are) expected to implement (or continue to implement) in relation to the private copying exception.[48] Article 5(2)(b) of the InfoSocDir reads:

> Member States may provide for exceptions or limitations to the reproduction right provided for in Article 2 in the following cases: [...] in respect of reproductions on any medium made by a natural person for private use and for ends that are neither directly nor indirectly commercial, on condition that the rightholders receive fair compensation which takes account of the application or non-application of technological measures referred to in Article 6 to the work or subject matter concerned [...].[49]

15 The above wording embeds fair compensation as a condition for any private copying exception adopted or implemented by Member States.[50] Unsurprisingly, the consumer electronics and information technology sectors were hostile to what they perceived to be the imposition of a new "tax" on their products.[51]

39 H Grethen, 36 session, 15 February 2001 (author translation). See also Manhaeve/Schiltz (n 20) para 20.072.

40 Doc. parl. 5128, 4.

41 Ibid 3.

42 Ibid.

43 Ibid 4.

44 Ibid 3.

45 Hugenholtz/Guibault/van Geffen (n 19).

46 See eg AA Quaedvlieg, 'The Netherlands' in Lindner/Shapiro (eds) (n 20) para 22.091 with further references, in particular the Gerkens Report.

47 COM (88) 172 final, p. 99 ff.

48 See Lucas-Schloetter (n 6) p. 597 (stating that private copying levies are not harmonized with the InfoSocDir only enshrining the principle of fair compensation); E Rosati, *Copyright and the Court of Justice of the European Union* (OUP 2023) 242 (describing InfoSocDir's ability to harmonize law on private copying as weak).

49 Emphasis added.

50 S Bechtold, 'Information Society Directive' in T Dreier & PB Hugenholtz (eds), *Concise European Copyright Law* (2nd edn, Kluwer 2016), art 5, n 3 (b).

51 Esteve Pardo/Lucas-Schloetter (n 2) p. 463; T Shapiro,

Over time, innumerable disputes – particularly between industry and collective management organisations, which typically collect, allocate, and distribute such fair compensation to reproduction rightholders – triggered national litigation. This, in turn, led to numerous requests for preliminary rulings from the ECJ, seeking interpretation[52] of the fair compensation requirement set out in Article 5(2)(b) of the InfoSocDir. In its landmark ruling in *Padawan*,[53] the ECJ clarified that Member States opting to introduce or maintain a private copying exception in their national law are *required* to ensure the provision of fair compensation to rightholders.[54] The Court emphasised that the concept of fair compensation is an autonomous concept of EU law – one that must be interpreted uniformly across all Member States.[55] The Court further noted that "given the practical difficulties in identifying users and obliging them to compensate rightholders for the harm caused to them," Member States could opt to "establish a levy system" to finance such fair compensation.[56] Further, the ECJ held that Member States could impose such levies on "those who have the digital reproduction equipment, devices and media and who, on that basis, in law or in fact, make that equipment available to private users or who provide copying services for them."[57] Finally, the Court noted that "nothing prevents those liable to pay the compensation from passing on the private copying levy" to the private user in the form of a higher price.[58]

16 The original Commission's proposal for the InfoSocDir gave Member States more flexibility when adopting or maintaining a private copying exception, as it did not require financial compensation.[59] However, although negotiations in the European Parliament and European Council revealed that a higher degree of harmonisation was intended, no agreement was reached on the specifics. Most countries preferred levies as the majority of Member States either already had such a remuneration scheme for private copying in place or intended to introduce one.[60] The strongest opponent of requiring levies was the UK, which was not prepared to be obligated to introduce them through internal market legislation.[61]

17 A compromise was eventually reached, resulting in the term "fair compensation," originally formulated in Italian as "*equo compenso,*" the mother tongue of the European Parliament Rapporteur of the InfoSocDir's First Reading, Roberto Barzanti.[62] This notion was hoped to bridge the gap between the Member States that use levy systems and call for "equitable remuneration" and those that had resisted such levies altogether.[63] The concept of

'Directive 2001/29/EC on copyright in the information society' in Lindner/Shapiro (eds) (n 20) para 2.117.

52 See, however, A Metzger, 'Rechtsfortbildung im Richtlinienrecht: Zur judikativen Rechtsangleichung durch den EuGH im Urheberrecht' (2017) ZEuP 836, 860 (describing the ECJ's method in these decisions as lying somewhere between interpretation and development of law).

53 Case C-467/08 *Padawan* (n 10).

54 Ibid, para 30; see also, Case C-277/10 *Luksan*, ECLI:EU:C:2012:65, para 93; Case C-462/09 *Stichting de Thuiskopie*, ECLI:EU:C:2011:397, para 22; Case C-463/12 *Copydan Båndkopi*, ECLI:EU:C:2015:144, para 19; Case C-470/14 *EGEDA and Others*, ECLI:EU:C:2016:418, para 20.

55 Case C-467/08 *Padawan* (n 10) paras 32 and 37.

56 Ibid, para 46 ff; Case C-572/13 *Hewlett-Packard Belgium*, ECLI:EU:C:2015:750, para 70.

57 Case C-467/08 *Padawan* (n 10) para 46 ff; Case C-572/13 *Hewlett-Packard Belgium* (n 56) para 70.

58 Case C-467/08 *Padawan* (n 10) para 48.

59 Compare Article 5(2)(b) of COM(97) 628 final, which did not refer to compensation and Recital 26 of COM(97) 628 final, which reads, in the relevant part: "Member States should be allowed to provide for an exception [...] for private use; whereas this *may* include the introduction or continuation of remuneration schemes to compensate for the prejudice to rightholders; [...] it appears justifiable to refrain from further harmonization" (emphasis added).

60 Reinbothe (n 8) 310.

61 Ibid.

62 Ibid.

63 J Reinbothe, 'Die EG-Richtlinie zum Urheberrecht in der Informationsgesellschaft' (2001) GRUR International 733, 738; Hugenholtz/Guibault/van Geffen (n 19) p. 36; S von Lewinski & MM Walter, 'Information Society Directive' in MM Walter and S von Lewinski (eds), European Copyright Law: A Commentary (OUP 2010) para 11.5.24; Bechtold (n 50) art 5, n 3 (b); L Guibault, 'Why Cherry-Picking Never Leads to Harmonisation: The Case of the Limitations on Copyright

fair compensation was intended to compensate rightholders at a lower level than the amount of equitable remuneration provided by existing levies.[64] While equitable remuneration may amount to the remuneration a rightholder would have received by granting a typical licence, that is not necessarily the case for fair compensation.[65]

II. Fair Compensation as a Concept Based on Harm

18 The ECJ pointed out that the autonomous concept of fair compensation is based on an evaluation of harm[66] and, relying on Recitals 35 and 38 of the InfoSocDir, established "harm suffered" as the core criterion for calculating fair compensation.[67] In the ECJ's early decisions, it was unclear whether the Court understood "harm" as an abstract concept – referring to harm resulting from the introduction of a private copying exception – or as actual harm arising from the specific act of reproduction in question.[68] The very idea that abstract harm might be sufficient to trigger the need for compensation relates to the concept of private copying in German law. The German framework, established in the 1960s as the world's first levy system, served as a blueprint for many countries.[69] According to the Court in *Padawan*, fair compensation should be calculated based on the harm caused to authors of protected works by the introduction of the private copying exception.[70] In *Hewlett-Packard Belgium*, however, the ECJ held that fair compensation is, in principle, intended to compensate for the harm suffered resulting from the copies actually produced ("the criterion of actual harm suffered") and not for any abstract harm created by the mere implementation or continuation of a private copying exception in national laws.[71]

19 Notably, although nobody disputes the leeway of Member States to continue applying their existing levies based on "equitable remuneration",[72] such continuation appears problematic in light of the ECJ's conceptual understanding of fair compensation. If the concept of fair compensation is based on harm, it must be an *aliud* to the concept of equitable remuneration.[73] The ECJ's case law supports such a conceptual distinction: in the context of Article 8(2) of Directive 92/100/EEC,[74] the Court interpreted

under Directive 2001/29/EC' (2010) JIPITEC 55, 58; Geiger/Schönherr/Karapapa (n 6) para 11.114.

64 Reinbothe (n 8) p. 316; S Bechtold (n 50), art 5, n 3 (b) (mentioned in 1st edn but not in 2nd edn).

65 Bechtold (n 64) art 5, n 3 (b) (mentioned in 1st edn but not in 2nd edn). See also J Poort & JP Quintais, 'The Levy Runs Dry. A Legal and Economic Analysis of EU Private Copying Levies' (2013) JIPITEC 205, para 18.

66 Ibid, (n 10) para 37, 39 ff.

67 Ibid; see also Case C-462/09 *Stichting de Thuiskopie* (n 54) para 24. This approach has been criticized by Reinbothe (n 8) p. 318 (arguing that harm is mentioned as only one of the relevant aspects in the recitals).

68 Cf. Poort/Quintais (n 65) para 31; Shapiro (n 51) para 2.138 (understanding the earlier decisions of the ECJ as referring to the introduction of the exception).

69 J Reinbothe, 'Compensation for Private Taping Under Sec. 53 (5) of the German Copyright Act' (1981) IIC 36, 36 (describing, in 1981, the provision granting remuneration from the producers of sound and visual recording equipment as the only provision of its kind in the world). For the history of copyright levies, see Hugenholtz (n 5) p. 179 (asserting, eg, that the "German levy system [...] became a model for the world"); Quintais (n 4) p. 76 (describing the German system as a staple of most Member States' national copyright laws and the impact on the Stockholm revision of the Berne Convention).

70 Case C-467/08 *Padawan* (n 10) para 42.

71 Case C-572/13 *Hewlett-Packard Belgium* (n 56) para 69. See also Geiger/Schönherr/Karapapa (n 6) para 11.114 f. For a critique of the approach, see B Hazucha, 'Private copying and harm to authors–compensation versus remuneration' (2017) 133 LQR 269, 277 ff.

72 InfoSocDir (n 3) Recital 38 mirrors this understanding. See Reinbothe (n 8) 315 ff; von Lewinski/Walter (n 63) para 11.5.25. For a different view, see B Koch & J Druschel, 'Entspricht die Bestimmung der angemessenen Vergütung nach §§ 54, 54a UrhG dem unionsrechtlichen Konzept des gerechten Ausgleichs? (2015) GRUR 957, 967 f.

73 Bechtold (n 64) art 5, n 3 (b) (mentioned in the 1st but not 2nd edn); C Pflüger, *Gerechter Ausgleich und angemessene Vergütung. Dispositionsmöglichkeiten bei Vergütungsansprüchen aus gesetzlichen Lizenzen* (Nomos 2017), 63.

74 Council Directive 92/100/EEC of 19 November 1992 on rental right and lending right and on certain rights related to copyright in the field of intellectual property (1992) OJ L

equitable remuneration as a concept based on the value of the use in trade.[75] However, in later decisions, the ECJ appeared to suggest that the differences between the two are not significant.[76] The ECJ argued that the concept of "remuneration" is also intended to provide recompense for authors, arising from the need to compensate them for the harm caused.[77] Hence, the notion of equitable remuneration arguably encompasses fair compensation.[78]

III. Flexibilities and Guarantees

20 When the ECJ pointed out in *Padawan* that fair compensation is an autonomous concept of EU law, which must be interpreted uniformly in all Member States,[79] it also acknowledged a certain degree of flexibility for Member States in implementing a compensation scheme. The ECJ outlined that certain powers are vested upon Member States to determine, within the limits imposed by EU law and in particular by the InfoSocDir, the form and level of fair compensation as well as the detailed arrangements for its financing and collection.[80] The Court continued to develop this understanding in various other decisions, pointing out that Member States enjoy "broad discretion" when determining the design of a fair compensation scheme.[81]

21 However, the ECJ noted that the compensation requirement also imposed a duty on Member States. It obliges them to achieve a certain result.[82] In other words, a Member State implementing a private copying exception must ensure, within the framework of their competences, effective recovery of fair compensation intended to compensate authors.[83]

IV. Exceptions to Fair Compensation

22 As noted above, as of this writing, some Member States still do not have a compensation mechanism in place.[84] When attempting to justify this absence, arguments based on InfoSocDir's Recital 35 have been put forth.[85] Recital 35 reads as follows:[86]

> In certain cases of exceptions or limitations, rightholders should receive fair compensation to compensate them adequately for the use made of their protected works or other subject-

346//61 (repealed).

75 Case C-245/00 SENA, ECLI:EU:C:2003:68, para 37; Case C-192/04 *Lagardère Active Broadcast*, ECLI:EU:C:2005:475, para 50.

76 Bechtold (n 50) art 5, n 3 (b) (with a similar interpretation of the decisions); Hazucha (n 71) 293 ff. (arguing that the ECJ follows, *de facto*, a remuneration approach labelled as a compensation approach).

77 Case , *VEWA*, ECLI:EU:C:2011:442, para 29; Case C-277/10 Luksan (n 54) para 103.

78 For a suggested limit, see AG Opinion, Case C-260/22 *Seven.One Entertainment Group*, ECLI:EU:C:2023:583, para - 24 (AG Collins argued that a compensation that over- or underestimates the harm caused to rightholders is incompatible with the fair balance that must be maintained between the interests and fundamental rights of rightholders and users, together with the public interest); see also Lucas-Schloetter (n 6) sec I.A; A Lucas-Schloetter, 'Exceptions – Rémunération pour copie privée – Appareils reconditionnés – Double paiement (non)' (2024) (90) Propr Intell 50, 52 (referring to a similar discussion in France regarding refurbished devices).

79 Case C-467/08 *Padawan* (n 10) paras 32, 37.

80 Ibid, para 37.

81 Case C-462/09 *Stichting de Thuiskopie* (n 54) para 23; Case C-521/11 *Amazon.com International Sales and Others*, ECLI:EU:C:2013:515, para 20; Case C-463/12 *Copydan Båndkopi* (n 54) para 20; Case C-470/14 *EGEDA and others* (n 54) para 22; Case C-263/21 *Ametic* (n 10) para 36.

82 Case C-462/09 *Stichting de Thuiskopie* (n 54) para 34; Case C-470/14 *EGEDA and others* (n 54) para 21.

83 Case C-462/09 *Stichting de Thuiskopie* (n 54) para 34, Case C-470/14 *EGEDA and others* (n 54) para 21. See also Pflüger (n 73) pp. 86 ff.; P Homar, *System und Prinzipien der gesetzlichen Vergütungsansprüche des Urheberrechts* [Österreich 2021], para 863.

84 See sec A, above.

85 Shapiro (n 51) para 2.116, fn. 175; Hazucha (n 71) pp. 273 ff (explaining the UK's pre-Brexit position). Luxembourg's legislature did much the same (doc. parl. 5128, 4 (arguing, inter alia, that there might be no obligation to pay or to make an additional payment in certain cases, although it did not explicitly question the general obligation to compensate)); Metzger (n 52) p. 858 (arguing that Recital 35 is vague).

86 For purposes of our analysis, we have numbered each sentence comprising Recital 35. Emphasis added.

matter ("Sentence 1"). When determining the form, detailed arrangements and possible level of such fair compensation, account should be taken of the particular circumstances of each case ("Sentence 2"). When evaluating these circumstances, a valuable criterion would be the possible harm to the rightholders resulting from the act in question ("Sentence 3"). In cases where rightholders have already received payment in some other form, for instance as part of a licence fee, no specific or separate payment may be due ("Sentence 4"). The level of fair compensation should take full account of the degree of use of technological protection measures referred to in this Directive ("Sentence 5"). In certain situations where the prejudice to the rightholder would be minimal, no obligation for payment may arise ("Sentence 6").

23 By including Recital 35, both the European Parliament and the Council of the European Union acknowledged that not all exceptions to, or limitations on, reproduction rights require payment to the rightholder. The Sentence 4 clearly states that rightholders who have already been remunerated in some other way (e.g., through a licence) may not be entitled to a specific or separate payment for the consequences of such exceptions or limitations. Sentence 6 goes further, explicitly acknowledging that no payment at all needs to be made if the prejudice suffered is *de minimis*. Clearly, while Recital 35 provides evidence of the legislator's intent, the real substance of the fair compensation obligation – and whether an exception applies – derives from Article 5(2)(b) of the InfoSocDir, which contains no express exception to the compensation requirement; any such exception flows exclusively from Recital 35.[87] Despite this, one might interpret the adjective "fair" in Article 5(2)(b) of the InfoSocDir as implying situations where no compensation is expected, therewith incorporating the two scenarios mentioned in Sentence 4 and Sentence 6 of Recital 35.

24 Generally speaking, Recital 35 of the InfoSocDir had no intention of questioning the obligation of Member States to compensate rightholders for private copying. At least historically, the scope of the exceptions mentioned in Sentence 4 and Sentence 6 were limited to rather specific cases: Sentence 4 was designed to prevent so-called "double dipping" – that is, to prevent rightholders from being paid twice for copies of the same work via, for example, licence fees,[88] an understanding that was accepted by the ECJ in *Padawan*.[89] On the contrary, others contend that the ECJ has moved away from that particular interpretation, as per its decisions in *VG Wort*[90] and *Copydan Båndkopi*.[91] In these two cases, the ECJ suggested that the form of the rightholder's authorising act (e.g., licence) could have no bearing on the fair compensation owed.[92] Such reasoning, however, appears to conflict with Sentence 4, raising questions about whether it has *any* applicable scope. Should the ECJ interpret Sentence 4 in this latter manner, it would diminish the intended impact of the provision, which appears contrary to the original legislative intent. Furthermore, this interpretation could place consumers at a disadvantage by making it even more difficult for Member States to justify the absence of compensation in cases where double dipping might occur.

25 Sentence 6 expresses the legislators' desire to obviate the need for compensation when there is minimal prejudice to the rightholder's reproduction right. This was included in Recital 35 to accommodate the concerns of a few Member States –particularly the pre-Brexit UK. During the directive's negotiations, the UK insisted that exceptions to the reproduction right should be allowed without remuneration for time-shifting.[93] It should be pointed out that, at the

87 *British Academy of Songwriters, Composers and Authors and others v Secretary of State for Business, Innovation and Skills* [2015] EWHC 1723 (Admin), para 199.

88 Reinbothe (n 8) 317.

89 Case C-467/08 *Padawan* (n 10) para 39.

90 Joined Cases C-457/11 to C-460/11, *VG Wort and others*, ECLI:EU:C:2013:426, para 37 ff.

91 Poort/Quintais (n 65) para 32 ff; Hazucha (n 71) 278; Shapiro (n 51) para 2.153.

92 Case C-463/12 *Copydan Båndkopi* (n 54) para 65. Shapiro (n 51) para 2.153.

93 A Lauber-Rönsberg, *Urheberrecht und Privatgebrauch. Eine rechtsvergleichende Untersuchung des deutschen und britischen Rechts* (Nomos 2011) 65; Reinbothe (n 8) p. 317 (both referring to a Commission statement).

time, the UK already had a corresponding provision in Section 70 of its Copyright, Designs and Patents Act 1988. In *Copydan Båndkopi*, while the ECJ ruled that setting such a threshold falls within the discretion of Member States,[94] they are still expected to apply the principle of equal treatment when setting it.[95] Some scholars suggest that, in addition to reproduction for time shifting purposes, the scope of *de minimis* prejudice should include, for example, format shifting (e.g., converting media files into different file formats and data compression) and making backup copies, so long as the private copy does not lead to a proliferation of the content.[96]

V. The Experience of Pre-Brexit UK

26 Sentences 4 and 6 arguably allow Member States to establish a private copying exception without implementing a compensation mechanism.[97] In 2014, the UK did just that – adopting a regulation implementing such an exception without compensation pursuant to Section 28B of its Copyright, Designs and Patents Act 1988.[98] Accordingly, any person who legitimately acquired content, other than a computer program, was entitled to copy that work for his or her own private use, and make any such copies in other formats and store them in the cloud, provided that such copies were made for private, non-commercial use. The exception, however, did not allow that person to copy such content to give to a family member, friend, or colleague.

27 Various studies had suggested that adopting or maintaining a private copying exception without implementing a commensurate compensation mechanism is consistent with Sentences 4 and 6, provided that no significant harm resulted.[99] Other scholars and governments have argued that reproduction rightholders are already well aware that consumers make private copies of content for legitimate, private-use purposes, such that the benefit of being able to do so is already priced into the purchase ("pricing in principle"), making any additional compensation either double dipping, a *de minimis* prejudice, or both.[100] Hence, a government's decision to forego a compensation scheme can be based on the understanding that the private copying exception will not entail a loss for rightholders – rather, it merely legitimises an already well-known and anticipated consumer practice.[101]

28 The UK courts rejected such arguments, confirming that the private copying exception implemented by the UK government did not comply with the UK's obligations under EU law.[102] On 19 June 2015, the High Court quashed the amendment.[103] Judge Green accepted the application of the pricing in principle[104]

94 Case C-463/12 *Copydan Båndkopi* (n 54) para 62.

95 Ibid.

96 Poort/Quintais (n 65) para 91 (arguing that there may not even be any harm in these cases).

97 *British Academy of Songwriters, Composers and Authors and others v Secretary of State for Business, Innovation and Skills* [2015] EWHC 1723 (Admin), para 184 f. See E Rosati, 'ECJ links fair compensation in Arts. 5(2)(a) and (b) of the InfoSoc Directive to actual harm requirement' (2016) GRUR International 399, 401.

98 Copyright and Rights in Performance (Personal Copies for Private Use) Regulations 2014 (SI 2014/2361). See on this amendment Hazucha (n 71) pp. 271 ff.; Rosati (n 48) pp. 243 ff.

99 I Hargreaves, *Digital Opportunity: A Review of Intellectual Property and Growth* [UK Intellectual Property Office 2011] para 5.28 ff <https://assets.publishing.service.gov.uk/media/5a796832ed915d07d35b53cd/ipreview-finalreport.pdf> accessed 18 September 2024; M Kretschmer, 'Private Copying and Fair Compensation: An Empirical Study of Copyright Levies in Europe' [UK Intellectual Property Office 2011] 19 ff <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2710611> accessed 18 September 2024. See also, S Karapapa, 'A Copyright Exception for Private Copying in the United Kingdom' [2013] 35(3) E.I.P.R. 129. Compare K Grisse & S Koroch, 'The British Private Copying Exception and Its Compatibility with the Information Society Directive' [2015] 10(7) JIPLP 562 (doubting the compatibility of 28B of the CDPA with the InfoSocDir).

100 Hargreaves (n 99) para 5.30 f.

101 Ibid.

102 *British Academy of Songwriters, Composers and Authors and others v Secretary of State for Business, Innovation and Skills* [2015] EWHC 1723 (Admin), para 208 ff.

103 *British Academy of Songwriters, Composers and Authors and others v Secretary of State for Business, Innovation and Skills* [2015] EWHC 1723 (Admin).

104 Ibid, para 208 ff.

but held that the discretion of EU Member States not to implement a compensation mechanism could only be exercised if they could demonstrate that the harm to the reproduction rightholder caused by the introduction of a copyright exception is *de minimis* or zero.[105] According to the court, this means that the evidence which the Member State must collect and the inferences it may draw upon must be sufficient to provide an answer to the following question: "Is the harm minimal or zero?"[106] The government's decision to introduce the amendment was based on multiple studies.[107] The High Court accepted that there was sufficient evidence and literature upon which "to draw certain common sense economic intuitions about pricing-in", but also found that "these common sense intuitions were not capable of answering the very much more specific legal question which was whether pricing-in was so extensive as to render residual harm minimal or non-existent".[108] According to the Court, it is "one thing to say that '*to some extent*' harm is avoided by pricing-in; it is altogether another thing to say that it is avoided so completely as to pass a *de minimis* threshold."[109]

29 The decision of the High Court was not motivated on the grounds that the absence of a fair compensation requirement is inadmissible per se – which is in line with academic literature suggesting that Member States are not prevented by EU law from drafting a tight copyright exception.[110] Rather, according to the Court, the UK government had failed to provide adequate evidence proving that harm was minimal or zero. In doing so, Judge Green set an extremely high threshold for the introduction of a private copying exception without a compensation requirement, making it almost impossible to adopt such an exception.

30 At present, the ECJ has not yet specifically decided on the level of evidence required to prove that harm is minimal or zero. Regularly, the Court emphasises the discretion of Member States.[111] Nevertheless, it would not be surprising if the ECJ were also to set high standards to demonstrate that an exception falls within the scope of Sentences 4 and Sentence 6 of InfoSocDir's Recital 35 if a Member State chooses to adopt or maintain a private copying exception while not providing *any* compensation for the rightholder. Despite his criticism of the High Court's decision, Hazucha points out that "the ECJ has clearly rejected the 'no harm' and 'indirect appropriation' arguments that could be used to justify a private copying exception without the payment of any compensation" and noted that the Court has an "attitude towards the '*de minimis* harm' argument [that] is rather restrictive."[112] Against this backdrop, the threshold to verify that no compensation is required as a *quid pro quo* for private copying is high.

D. Interpreting the Private Copying Exception Embedded in Luxembourg's Copyright Act – De Lege Lata

31 The foregoing analysis leads to questions about how one can interpret the existing private copying exception in Luxembourg's Copyright Act. To our knowledge, there have been no court decisions to date applying its Article 10(1)(4°).[113] As a principle, Article 5(2)(b) of the InfoSocDir stipulates that fair compensation for rightholders is a condition for such an exception. Article 10(1)(4°) of the amended Copyright Act provides for such compensation

105 Ibid, para 249.

106 Ibid.

107 Ibid, para 49 (referring to the reports by Hargreaves and Kretschmer).

108 Ibid, para 271 (emphasis in the original).

109 Ibid, para 271 (emphasis in the original).

110 See E Rosati, 'ECJ links fair compensation in Arts. 5(2)(a) and (b) of the InfoSoc Directive to actual harm requirement' (2016) GRUR International 399, 401 (arguing that Member States are not prevented from drafting a tight private copying exception).

111 See references in n 81.

112 Hazucha (n 71) p. 281.

113 JL Putz, *Recueil de Propriété intellectuelle* (Larcier 2022) 113. The only Luxembourg court decisions dealing with a private copying exception appear to be TA Lux., com. 8 December 2010, no 113017 and CSJ, 13 June 2012, no 37207 (affirming the court of first instance decision), which addressed the German Copyright Act, not Luxembourg's Copyright Act.

on paper but the intended GDR for setting up the conditions for the fixing and collecting of this compensation was never introduced, as pointed out above. There are three potential approaches to Article 10(1)(4°) of Luxembourg's Copyright Act: (I) apply the private copying exception without a compensation requirement, (II) do not apply the provision at all, or (III) apply it using direct compensation.

I. Apply Article 10(1)(4°) Without a Compensation Requirement

32 Article 10(1)(4°) of Luxembourg's Copyright Act may be applied without compensating the rightholder, since a compensation scheme has not yet been established. This would correspond to the legal situation prior to the amendment of 18 April 2004. Two guides on copyright law, one produced by the Luxembourg Ministry of the Economy[114] and the other by the Luxembourg Ministry of Culture[115] appear to follow this interpretation of the law. The guides refer to private copying as one of the exceptions to the reproduction right without addressing the need for compensation. For other copyright exceptions, the guides mention requirements.[116]

33 Nonetheless, such an understanding does not mirror the wording of Article 10(1)(4°) of the amended Copyright Act, which unambiguously requires fair compensation for private copying even if the details have never been set. It also is not in line with the condition of fair compensation in EU law. Reproduction acts permitted by Luxembourg's private copying exception are not so insignificant as to fall within the scope of Sentences 4 and Sentence 6 of Recital 35, such that no compensation is a "fair compensation". Firstly, qualitatively, Luxembourg's private copying exception is an extensive adaptation of the corresponding EU-level concept found in the InfoSocDir. It applies to more situations than just those in which there is minimal or no harm[117] as it replicates, almost verbatim, the wording of Article 5(2)(b) of the InfoSocDir, thereby implementing one of that provision's broadest possible scopes.[118] Indeed, in several ways, that scope is even broader than the UK's legislative exception, which was quashed by the High Court.[119] Moreover, unlike the UK government, Luxembourg has not produced any substantive assessment as to why such private copying falls within either Sentence 4 or Sentence 6 of Recital 35 of the InfoSocDir or both. At least, no such assessment has been reported.

34 Secondly, one cannot credibly suggest that the population of the Grand Duchy is quantitatively so small that reproductions in Luxembourg cause a prejudice to the rightholder which is minimal when viewed in relation to the EU's overall population. As copyrights are national IPRs and not EU IPRs, Recital 35 can only refer to the insignificance of the prejudice for the copyright conferred by a specific Member State. The case law of the ECJ supports this perspective when describing that the obligation of a Member State to ensure fair compensation is based on the harm suffered by the authors on the territory

114 Ministère de l'Économie et du Commerce Extérieur, *Les droits d'auteur : le guide* (2010) 10 <https://meco.gouvernement.lu/dam-assets/publications/guide-manuel/minist-economie/guide-droits-auteur/2010-guide-droits-auteur-fr.pdf> accessed 18 September 2024.

115 Ministère de la Culture, *Guide pratique : Droits d'auteur, droits voisins et autres droits dans le secteur du patrimoine culturel numérique*. (Version 1.0, 5 July 2021) 08 <https://mcult.gouvernement.lu/dam-assets/publications/guide-manuel/minist-culture/guide-droit-auteur/droits-auteur-droits-voisins-et-autres-droits-numerique.pdf> accessed 18 September 2024.

116 Ibid.

117 Putz (n 20) para 340.

118 It is more restrictive than the EU framework in one aspect: it allows a natural person to copy only for his or her own private use, whereas the InfoSocDir also permits copying for the private use of another natural person. The literature on Luxembourg's copyright law, however, advocates for an extended interpretation that would include copies for friends and family members (see eg Putz (n 20) para 343; Manhaeve/Schiltz (n 20) para 20.046 (adhering to the French concept of 'family circle')), which would be in line with EU law (von Lewinski/Walter (n 63) para 11.5.31; Quintais (n 4) 69; Shapiro (n 51) para 2.123) and eliminate this difference.

119 For example, Section 28B CDPA required the template to be either the individual's own copy of the work, or a personal copy of the work made by the individual while Luxembourg's law does not specify similar aspects. See also Hazucha (n 71) pp. 276 f. (explaining that the scope and applicability of the UK amendment was quite narrow in contrast to InfoSocDir's Article 5(2)(b)).

of that State.[120] The ECJ looks at the requirement of fair compensation through the prism of the specific Member State but not the entire EU.

II. Do Not Apply Article 10(1)(4°) at All

35 Several scholarly works on Luxembourg's copyright law adopt a different approach to the country's private copying exception. They argue that because fair compensation is obligatory, the private copying exception should not,[121] legally cannot,[122] or even *de facto* cannot[123] be applied at the moment, due to the lack of the requisite GDR. Luxembourg's private copying exception mentions compensation as a prerequisite for private copying, yet no GDR on compensation has yet been adopted. This position contradicts the government's own interpretation of its law – their guides on copyright law unequivocally indicate that Luxembourg has a private copying exception, despite the lack of a GDR on the details of collecting and paying fair compensation.[124]

36 If Luxembourg's Chambre des Députés had intended to pause its private copying exception until it could comply with its obligation to pay rightholders fair compensation therefor, it was equipped to do so. For example, it could have made Article 10(1)(4°) of Luxembourg's Copyright Act effective only after the required GDR introducing a compensation scheme had been promulgated. However, it chose not to implement such an express condition.

37 Moreover, it is unconvincing to interpret Article 10(1)(4°) of Luxembourg's Copyright Act as making the adoption of the GDR an implicit condition for the effectiveness of the provision. The legislative history of the amendment does not suggest that the legislature intended to suspend the pre-existing right of private parties to copy. Indeed, such an approach would have been contrary to Luxembourg's vision of the information society, as articulated in the parliamentary documents.[125]

III. Apply Article 10(1)(4°) Using Direct Compensation

38 A third potential application of Article 10(1)(4°) refuses to question the applicability of the current private copying exception. It rather sets out the requirement of each individual copying a protected work to locate and pay the individual rightholder fair compensation as a *quid pro quo* for the copy.[126] Such a compensation system would represent a significant departure from the indirect systems of collectivisation and payment implemented in most EU Member States, establishing a direct bilateral obligation for the private copier to compensate the rightholder.

39 Article 10(1)(4°) of Luxembourg's Copyright Act, as amended in 2004, clearly reflects the Member State's attempt to align its national law with the InfoSocDir, but there are no indications that the Chambre des Députés ever intended to put Luxembourg's existing private copying exception on hold until the necessary GDR was put in place. In the absence thereof, the compensation requirement can be interpreted as an obligation to be fulfilled between the parties, just like any other legal obligation must be interpreted in private law settings when no further details are provided by law. At present, there is nothing in Luxembourg's Copyright Act preventing such an interpretation. In particular, the law does not expressly prohibit individual compensation claims by stipulating that rightholders can only claim compensation via a collective society, which is the case in some Member States.[127]

120 Case C-462/09 *Stichting de Thuiskopie* (n 54) para 36.

121 Putz (n 20) para 338.

122 Oral Comments by B Krieps, quoted in M Carey, 'Right to private copy' [13 April 2007] <https://paperjam.lu/article/news-right-private-copy> accessed on 18 September 2024.

123 Manhaeve/Schiltz (n 20) para 20.076.

124 See references in n 115.

125 Doc. parl. 5128, 3.

126 As the law refers to fair compensation as a condition for an exception to the exclusive reproduction right, the copier needs to compensate (or at least offer to compensate) the rightholder in order to avoid an infringement of the reproduction right. Hence, a private party cannot copy and compensate only upon a claim of the rightholder.

127 See eg art 16d of the Dutch Copyright Act and § 54h(1) of the German Copyright Act which requires the debtor to pay to a collecting society or the rightholder

40 This approach indeed has the potential to create onerous burdens on both the copier and the rightholder. For every work acquired and copied, the private copier would have to determine who the actual rightholders are, how to get in contact with all of them, and arrange to send payment to them once the rightholders agree to whatever is considered fair compensation. Rightholders, in turn, could receive tens, hundreds, thousands, or even millions of communications from private copiers, and would need to coordinate the receipt of such fair compensation.

41 The third interpretation is, perhaps surprisingly, in line with EU law. To be clear, the InfoSocDir does not prohibit the payment of the obligatory fair compensation directly to the rightholder. In *Padawan*, the ECJ indicated that the word "compensate" in InfoSocDir's Recitals 35 and 38 expressed the EU legislature's intent to establish a specific compensation scheme.[128] However, the ECJ only noted the practical difficulties in obtaining direct compensation, therefore focusing more on the possibility of Member States to establish indirect mechanisms.[129] Additionally, Recital 38 permits such remuneration schemes, but does not prohibit direct compensation.[130]

42 If a Member State chooses to rely on a direct compensation scheme, it would still be obligated to ensure that it resulted in the effective recovery of the fair compensation intended to compensate the rightholders. It is not clear that Luxembourg could meet that obligation with such a direct compensation mechanism. As already mentioned above, the ECJ pointed out in *Stichting de Thuiskopie* that a Member State that has introduced a private copying exception into its national law is under an obligation to ensure fair compensation as a result.[131] In practice, a mechanism requiring individuals who make copies to directly compensate reproduction rightholders would likely differ significantly from situations that arise when there is no private copying exception.[132] Such an arrangement would regularly be one "honoured in the breach", as most individuals would unlikely follow through with such an individual obligation every time they wanted to record a broadcast programme or film to watch at a later time. In other words, it would be significantly challenging to enforce individual compensation, with private parties regularly reproducing works without providing any compensation to the rightholders.

E. The Need to Change the Law

43 For the reasons mentioned in Section D, none of the potential interpretations or approaches to applying Luxembourg's existing Article 10(1)(4°) is particularly compelling – or even appealing. Applying the existing private copying exception without providing fair compensation violates the compensation requirement in InfoSocDir's Article 5(2)(b) (see section D.I), yet refraining from applying any private copying exception conflicts with Luxembourg's express desire to permit private copying (see section D.II). Finally, interpreting the compensation requirement as a bilateral obligation between the copier and the rightholder risks failing to fulfil the obligation as emphasised by the ECJ's case law, namely, to ensure the effective recovery of fair compensation (section D.III). Nevertheless, without the GDR envisaged by Article 10(1)(4°) of Luxembourg's Copyright Act, Luxembourg must attempt to align itself with one of these approaches.

44 Luxembourg should change its existing legislation to ensure, on the one hand, the existence of an effective private copying exception and, on the other, compatibility with EU law. Repealing Luxembourg's private copying exception is not a feasible option. Without a private copying exception, the reproduction right would have full effect

to claim remuneration thereby via such (so-called 'Verwertungsgesellschaftenpflichtigkeit'), see T Dreier, '§ 54h Verwertungsgesellschaften; Handhabung der Mitteilungen' in T Dreier and G Schulze (eds), *Urheberrechtsgesetz Kommentar* (7th edn, CH Beck 2022) para 1.

128 Case C-467/08 *Padawan* (n 10) para 19; Case C-470/14 *EGEDA and others* (n 54) para 19.

129 Cf Shapiro (n 51) para 2.131.

130 It reads: "This may *include* the introduction or continuation of remuneration schemes [...]." (emphasis added).

131 Case C-462/09 *Stichting de Thuiskopie* (n 54) para 34.

132 See sec A above.

in the private sphere – a result that contradicts Luxembourg's express intent to follow a liberal approach with respect to private copying.[133] A clear solution in line with this approach is to uphold the broad exception in Luxembourg's copyright law while introducing an indirect mechanism to provide fair compensation to rightholders by a GDR as promised in the second sentence of Article 10(1)(4°) of Luxembourg's Copyright Act. The practical implications of this option will be explored below.

F. Fair Compensation in Luxembourg – De Lege Ferenda

45 If Luxembourg were to adopt the long-envisaged GDR setting up an indirect compensation scheme for private copying, it would need to address three particularly significant points: how to assess fair compensation for private copies made pursuant to the private copying exception (section F.I); how to collect it (section F.II); and how to allocate it (section F.III).

I. Assessing Fair Compensation

46 Applicable EU law gives those Member State choosing to grant a private copying exception broad discretion to design and implement a national compensation mechanism as well as to establish an appropriately "fair" level of compensation within its borders.[134] The starting point in exercising that discretion necessarily involves determining who decides the Member State's precise level of compensation and under what circumstances.[135] Germany, for example, originally set out its compensation levels in the applicable law;[136] however, it abandoned that approach in 2008, opting instead for compensation levels negotiated by collective management organisations with the reproduction media and device manufacturers.[137] France, on the other hand, appointed a special commission to perform the function.[138] Selecting the appropriate decision-maker is likely to exert a disproportionate impact not only on the level of compensation but also on the perceived fairness of the compensation system as a whole – therefore, it is imperative to make this choice judiciously.

47 For Luxembourg – with a very small population and an even smaller subset of individuals making private copies of protected content for their own purposes, as well as lacking relative legislative or regulatory experience in the domain – it may appear that an elegant compromise would be to establish, through legislation or the long-anticipated GDR, a commission. This would comprise of representatives of the different stakeholders involved (e.g., collective management organisations, reproduction rightholders, reproduction media and device manufacturers and vendors, private copiers/consumers, and the relevant ministries), whose purpose would be to reach a negotiated compromise on the level of fair compensation. This particular solution appears feasible, as Articles 92 and 93 of Luxembourg's amended Copyright Act already contemplate a Commission for Copyright and Related Rights. Moreover, the GDR of 16 March 2005, as mentioned above,[139] which sets out the composition and the internal procedures of this Commission, could easily be amended to adjust its composition and to grant it the competence to propose an appropriate level of compensation.

48 Regardless of which method Luxembourg uses to set the level of fair compensation for private copying within its own territory – whether by regulation or appointed commission –, the Grand Duchy still needs to conform to various standards already embedded in EU law via a plethora of preliminary

133 Doc. parl. 5128, 3.

134 See references in n 81.

135 Although partially outdated, for concepts implemented in France, Germany, and Spain, see Esteve Pardo/Lucas-Schloetter (n 2) pp. 469 f.

136 § 54d of the German Copyright Act (with its attachment) before its reform of 2008.

137 Germany's post-2008 reform system of extended self-regulation.

138 France's *Commission pour la Rémunération Copie Privée*.

139 *Règlement grand-ducal du 16 mars 2005 portant organisation de la Commission des droits d'auteur et des droits voisins*, Mémorial A 52.

rulings by the ECJ.[140] The ECJ has, for example, ruled that reproductions based on illegal copies do not fall under the private copying exception found in Article 5(b)(2) of the InfoSocDir, thereby eliminating the need for the fair compensation therefor.[141] However, it did hold that fair compensation may be due for reproductions made via a single process that uses a chain of devices,[142] for reproductions made on multifunctional media,[143] or for reproductions stored in the cloud.[144] Luxembourg must also consider other on-going debates regarding fair compensation in other Member States, e.g., on tethered downloads (a digital file electronically delivered to a device intended to reside there on a limited basis).[145] Moreover, Luxembourg must determine whether to adopt a *de minimis* rule for reproductions that do not result in any significant harm to the rightholder – that is, when the private copy does not lead to any proliferation of content – thereby ensuring that no compensation is due.[146] The decision to exclude certain acts of reproduction requires a prior evaluation of the involved harm of the rightholder, as pointed out above.

49 Looking at the choices made by Luxembourg's nearest neighbours, taking a *quid pro quo* approach to fair compensation for private copying often leads to levies that give substantial compensation to rightholders accompanied by a substantial financial burden borne by consumers. Moreover, such levies are imposed on a wide variety of consumer products, including, but not limited to PCs, servers, laptops, tablets, smartphones, hard drives, USB sticks, and copying machines. The ECJ has confirmed that Member States have discretion as to what level of compensation is considered "fair" within their own borders,[147] the size of which varies significantly among them.[148] For example, a USB stick with 64 GBs of storage results in a levy of EUR 0.30 in Germany,[149] EUR 0.40 in the Netherlands,[150] and EUR 2.80 in France.[151] Another example concerns so-called smartphones. Depending on the particular device's specific features, it can carry a levy of EUR 5.30 in the

140 For a detailed overview, see Rosati (n 48) pp. 245 ff.

141 Case C-435/12 *ACI Adam and Others*, ECLI:EU:C:2014:254, para 31 (if the initial source of the copy was not lawful, no fair compensation is due for copying it).

142 Joined Cases C-457/11 to C-460/11 *VG Wort and others* (n 92) para 78 (reproductions made through a single process using a chain of devices, a levy may be imposed on each device, provided that the overall compensation owed is not substantially different from the amount fixed for a reproduction obtained through a single device).

143 Case C-463/12 *Copydan Båndkopi* (n 54) para 29 (fair compensation is due for multimedia (eg mobile phone memory cards) if at least one of the medium's function permits private copying; however, the amount thereof should take into account whether private copying is the medium's main or ancillary purpose as well as the relative importance of the medium's capacity to make such copies, such that no consideration need be collected, if the rightholder's prejudice if determined to be minimal).

144 Case C433/20 *Austro-Mechana,* ECLI:EU:C:2022:217, para 54 (InfoSocDir's Art 5(b)(2) precondition for a private copying exception extend to cloud storage).

145 The copyright community in the Netherlands is hotly debating whether tethered downloads must be taken into account when calculating the required compensation. See eg The Hague Court of Appeal, *HP c.s. / SONT and Thuiskopie*, 22 March 2022; O Jani & M Vonthien, 'Zur Einordnung von Tethered Downloads als Privatkopien gemäß § 53 Abs. 1 UrhG' (2023) ZUM 73.

146 Poort/Quintais (n 65) para 91 (stating that there may be even not harm at all in these cases).

147 See references in n 81.

148 Geiger/Schönherr/Karapapa (n 6) para 11.119. Unlike other countries, France, for example, charges levies even for second-hand products: Copie France, 'Private Copying Remuneration Tariffs in France as from February 1st 2023 (VAT not applicable)' (January 2023) <https://www.copiefrance.fr/images/documents/tarifs-EN-2023-02-D23.pdf> accessed 18 September 2024. For private copying levies on refurbished devices see also, A Lucas-Schloetter, 'Exceptions – Rémunération pour copie privée – Appareils reconditionnés – Double paiement (non)' (2023) (87) Propr Intell 32; Lucas-Schloetter (n 78) p. 50.

149 ZPÜ, VG Wort and VG Bild-Kunst, 'Gemeinsamer Tarif. USB-Sticks und Speicherkarten' (24 June 2019) <https://www.zpue.de/download-center/61-gesamtvertrag-usb-sticks-und-speicherkarten-ab-2019-vere/file.html> accessed 18 September 2024.

150 SONT, 'Decree on Private Copying Levies 2023 – 2024' <https://www.onderhandelingthuiskopie.nl/About-the-SONT> accessed 18 September 2024.

151 See Copie France (n 151) p. 151.

Netherlands,[152] EUR 6.25 in Germany,[153] and EUR 14.00 in France.[154] Looking only at the above-mentioned devices, and noting that STATEC[155] reports that more than 125,000 memory storage devices[156] and more than 250,000 smartphones[157] were imported into Luxembourg in 2023 alone, implementing a similar levy system in Luxembourg could amount to a financial transfer of several million euros per year.

50 Notably, France,[158] Germany,[159] and the Netherlands[160] traditionally work with a system that calls for equitable remuneration, rather than fair compensation. As previously mentioned, the level needed to achieve fair compensation is typically considered to be lower than that to achieve equitable remuneration, as the latter is frequently equated to the remuneration a rightholder would receive as a result of a licence.[161] Therefore, if the Grand Duchy were to introduce a compensation system solely based on pure harm to the rightholder, which gives rise to an obligation to provide fair compensation rather than equitable remuneration, Luxembourg could substantially reduce the financial burden placed on consumers making copies for their private use in comparison to its neighbours.

II. Compensation through Luxembourg's State Budget

51 According to the legislative history of the 2004 Amendment that introduced the current Article 10(1)(4°) of Luxembourg's Copyright Act, Luxembourg's Chambre de Députés feared that introducing a compensation scheme would result in a complex regulatory structure as well as significant administrative costs for economic operators.[162] Although the effort needed is likely to be less than it was feared 20 years ago (due, in large part, to advances in electronic cashier and booking systems), it is still likely to be costly and time-consuming for sellers to collect such levies and then channel the collected funds to a collective management organisation for allocation and distribution. Additionally, some of the sentiments expressed back then remain: the levies may still feel like an extra tax only imposed on certain products and the collection thereof may still not align with Luxembourg's societal spirit or political will. Moreover, many entitled rightholders will be non-residents. Hence, levies paid within Luxembourg will be paid out primarily to beneficiaries outside the country.

52 To alleviate such political, economic and legislative concerns, Luxembourg could opt for an alternative system, whereby fair compensation for private copies is funded not by levies, but as a state-level line-item expense taken from the state budget. Indeed, a few EU/EEA countries, including Spain[163]

152 See n 153.

153 ZPÜ, VG Wort and VG Bild-Kunst, 'Gemeinsamer Tarif. Mobiltelefone' [4 January 2016] <https://www.zpue.de/download-center/83-tarif-mobiltelefone-ab-2008/file.html> accessed 18 September 2024.

154 See Copie France (n 151) p. 151.

155 At the author's request, Luxembourg's National Institute of Statistics and Economic Studies (STATEC) provided the author with unpublished, unofficial import statistics for the years 2022 and 2023, which information the author retains on file.

156 STATEC Code No. 85235110

157 STATEC Code No. 85171300

158 Lucas-Schloetter (n 6) under sec I.A (describing private copying levies as a legal right to remuneration in France). See also, Geiger (n 15) p. 530.

159 Lauber-Rönsberg (n 93) p. 231 (describing the remuneration as compensation at the level of a licensing fee based on an individual contract); Lucas-Schloetter (n 6) under I.A (describing private copying levies as a legal right to remuneration in Germany); Esteve Pardo/Lucas-Schloetter (n 2) 466; Koch/Druschel (n 72) pp. 959 ff. (describing the German remuneration principle and its relation to fundamental rights); H Schack, *Urheber- und Urhebervertragsrecht* [10th edn., Mohr Siebeck 2021) no 507 (describing remuneration for private copying as the functional equivalent to the exploitation right).

160 For the discussion on the term *vergoeding* (art 16c Dutch Copyright Act) as opposed to *redelijke tegemoetkoming*, see Quaedvlieg (n 46) para 22.088 with further references.

161 See sec C.I above.

162 Doc. parl. 5128, 3 f.

163 A levy system was reinstated in 2017 in the course of the proceedings relating to Case C-470/14 *EGEDA and others* (n 54). See M García Léon, 'Spain' in Lindner/Shapiro (eds) (n 20) para 28.055 ff; Rosati (n 48) p. 254.

Finland,[164] and Norway,[165] have experimented with such mechanisms in connection with their private copying exceptions. Unsurprisingly, the ECJ was called upon to give a preliminary ruling on the appropriateness thereof. In *EGEDA and Others*,[166] the Court held that, in principle, Member States can choose to establish such a compensation scheme,[167] based on the discretion reserved to them in Recitals 35 and 38 of the InfoSocDir.

53 However, the ECJ made clear that any such scheme financed by the general state budget must guarantee that the cost of fair compensation is borne solely by those individuals who generate private copies falling under the Member State's private copying exception.[168] That clarification aligns with the concept of cost allocation adopted by the ECJ in its decisions on levy schemes, where it held that levies imposed on reproduction equipment, devices, and media acquired by legal persons – as opposed to natural persons – do not fall within Article 5(2)(b) of the InfoSocDir, as the harm to rightholders is not, and cannot be, based on the Member State's private copying exception.[169] Hence, if a levy is imposed on all blank media, the Member State is required to provide persons not covered by the private copying exception with an effective right to reimbursement.[170] According to the ECJ, the right to reimbursement must be available "for persons other than natural persons who purchase reproduction equipment for purposes clearly unrelated to the making of copies for private use."[171] Spain's scheme for financing fair compensation by its general state budget failed to incorporate an exemption or a right to reimbursement for legal persons which do not in any event fall within Article 5(2)(b) of the InfoSocDir or the Member State's private copying exception.[172] As a result, it obliged legal persons to finance at least a portion of the compensation. Therefore, in *EGEDA and Others*, the ECJ found that such a mechanism is incompatible with Article 5(2)(b) InfoSocDir.[173]

54 Notwithstanding those limitations imposed by EU law, funding Luxembourg's fair compensation through its state budget is still a viable policy option worth considering, as it would keep administrative costs lower than those of a levy system. Allocating a dedicated line within an existing budget imposes a lower administrative burden than collecting levies. Keeping costs down is a particularly important goal in smaller countries where it is highly unlikely that the overheads resulting from running a complex compensation scheme would be offset by the relatively small number of individual compensation processes. Additionally, this is especially important when considering that in Luxembourg much of the

164 Kopiosto, 'Compensation for Private Copying' <https://kopiosto.fi/en/kopiosto/about-copyright/compensation-for-private-copying/> accessed 18 September 2024. See also, K Harenko, 'Finland' in Lindner/Shapiro (eds) (n 20) para 11.18. Most recently, Finland's private copying compensation experienced a drastic cut which caused a heavy debate including the call to reverse the decision of Finland's government. See CISAC, 'Creators' rights organisations call for drastic cut in Finland's private copying compensation to be reversed' <https://www.cisac.org/Newsroom/articles/creators-rights-organisations-call-drastic-cut-finlands-private-copying> accessed 18 September 2024.

165 Norwaco, 'Copying for Private Use' <https://www.norwaco.no/en/private-copying> accessed 18 September 2024.

166 Case C-470/14 *EGEDA and Others* (n 54).

167 Case C-470/14 *EGEDA and others* (n 54) para 24. Compare Metzger (n 52) 860 (apparently suggesting that the decision rejects any compensation mechanism funded by the general state budget).

168 Case C-470/14 *EGEDA and others* (n 54) para 41. The ECJ pointed out that under levy systems, persons who have reproduction equipment, devices, and media and then make them available to natural persons must pay the levy, but they are not prevented from passing the amount of the private copying levy to such persons by including it in the price charged (para 33). Thus, the burden of the levy may ultimately be borne by the private user who pays the price for the use of such media (para 34).

169 Case C-467/08 *Padawan* (n 10) para 53.

170 Case C-521/11 *Amazon.com International Sales and Others* (n 81) para 28 ff; Case C-463/12 *Copydan Båndkopi* (n 54) para 44 ff. For the details of such exceptions, see Case C-110/15 *Nokia Italia and Others*, ECLI:EU:C:2016:717, para 24 ff; Case C-263/21 *Ametic* (n 10) para 33 ff (holding that the exception can be administered by a legal person established and controlled by intellectual property management organisations).

171 Case C-467/08 *Padawan* (n 10) para 53; Case C-463/12 *Copydan Båndkopi* (n 54) para 47; Case C-263/21 *Ametic* (n 10) para 45.

172 Case C-470/14 E*GEDA and Others* (n 54) para 39 f.

173 Case C-470/14 *EGEDA and Others* (n 54) para 41.

compensation will be granted to non-residents.

55 Compensation in Luxembourg could be financed, for example, from the income tax of private persons or from the VAT collected from the purchase of reproduction equipment and media paid by private persons. This would ensure that the requirements set in the ECJ's decision in *EGEDA* are met as only natural persons eligible for private copying in the sense of Article 10(1)(4°) of Luxembourg's Copyright Act are affected. This is also a feasible approach for other countries that are hesitating to implement a levy system.

III. Allocating and Distributing Fair Compensation

56 Irrespective of whether Luxembourg chooses to compensate rightholders through levies or its state budget, the country will ultimately have to first allocate and then distribute the funds collected to the appropriate rightholders.[174] The term "rightholders" in InfoSocDir's Article 5(2)(b) refers to the list of natural and legal persons granted the exclusive right to reproduce their content, which is set out in Article 2(a) through (e).[175] Interestingly, that list appears to be exclusive. For example, the ECJ held that publishers, not being mentioned therein, are not considered rightholders entitled to compensation pursuant to InfoSocDir's Article 5(2)(b).[176]

57 Inevitably, Luxembourg will have to work with or through a collective management organisation to allocate and distribute the collected funds; it could choose to establish a new one or commission an existing one. France, for example, established Copie France, a private enterprise founded to administer compensation for private copying.[177] However, for smaller countries, such as Luxembourg, it may be preferable to administer the rightholders' compensation through one of its existing collective management organisations (e.g., ALGOA[178], Luxorr,[179] SACEM Luxembourg[180]) to avoid excessive administration costs. This is particularly true if the funds to be distributed are transferred from the state budget and the collective management organisation is not obliged to collect levies.

58 Interestingly, EU law does not demand that all the funds collected as compensation need to be paid directly to individual rightholders. The ECJ found that allocating part of the funds intended for fair compensation to social and cultural establishments set up for the benefit of those entitled to such compensation is not contrary to the objective of such compensation, provided that those social and cultural establishments actually benefit those entitled and the detailed arrangements for the operation of such establishments are not discriminatory, which it is for the national court to verify.[181]

59 Finland takes this approach to the allocation of compensation, supporting certain cultural activities from a share of the national budget established to compensate rightholders.[182] Other countries, such as France, that operate a private copying levy system also use part of the sums collected for cultural

174 It is unclear whether the right to fair compensation is waivable. The ECJ held in Case C-277/10 *Luksan* (n 54) that the reproduction rightholder's right to fair compensation might not be waivable. It decided this explicitly for authors of films.

175 It was disputed whether broadcasting organisations receive compensation: See von Lewinski/Walter (n 63) para 11.5.35; Shapiro (n 51) para 2.141. The ECJ confirmed their eligibility in C-260/22 *Seven.One Entertainment Group*, ECLI:EU:C:2023:900, para 21 ff.

176 Case C-572/13 *Hewlett-Packard Belgium* (n 56) para 47 ff.

177 See art L311-6 of the French Copyright Act.

178 Association of Collective Management of Audiovisual Works in Luxembourg ASBL ("ALGOA"), a Luxembourg non-profit association, represents the Association of International Collective Management of Audiovisual Work ("AGICOA") <https://www.algoa.lu/english/about/about.html> accessed 18 September 2024.

179 Luxembourg Organization for Reproduction Rights ASBL ("Luxorr"), a Luxembourg non-profit association <https://www.luxorr.lu/en/> accessed 18 September 2024.

180 Society of Music Authors, Composers and Editors Luxembourg SC ("SACEM Luxembourg"), a Luxembourg civil company <https://www.sacem.lu/en> accessed 18 September 2024.

181 Case C-521/11 *Amazon.com International Sales and Others* (n 81) para 53. See also Article 12(4) of the Collective Management Directive.

182 Kopiosto (n 167).

purposes.[183] This approach is also highly attractive for a small country like Luxembourg – as it would mean keeping the funds within the country and avoiding their transfer abroad, where many of the registered rightholders might be based. Moreover, because Luxembourg already offers strong financial support to its cultural establishments, it might even be possible to consider at least a portion of that existing financial support as compensation for private copies made pursuant to Luxembourg's private copying exception. As long as the amount thereof supports the rightholders mentioned in Article 2 of the InfoSocDir – which it already does – this could reduce the additional administrative expenditures that would result from implementing a compensation mechanism funded by the state budget.

G. Conclusion

60 Historically, many countries have implemented a private copying exception to overcome the practical difficulties encountered when applying and enforcing copyright law in the private sphere. In recognition thereof, the EU adopted Article 5(2)(b) of the InfoSocDir, which allows Member States to provide or maintain that exception as long as they guarantee that reproduction rightholders receive fair compensation. Although fair compensation is an autonomous concept of EU law, the InfoSocDir gives a Member State broad discretion when determining the design of a fair compensation scheme. Indeed, many Member States have exercised this discretion. Most use varying forms of levy systems that ultimately charge private parties a certain amount when purchasing reproduction media or devices, with the collected amounts being allocated and distributed to compensate reproduction rightholders through collective management organisations. EU law enshrines two exceptions under which Member States are not required to offer compensation for private copying, each of which has a very narrow scope: Recital 35 of the InfoSocDir indicates that the reproduction has to inflict either zero or minimal harm on the rightholders if a Member State does not want to provide compensation.

61 In 2014, prior to Brexit, the UK introduced a private copying exception without any compensation requirement. Despite multiple reports indicating that the new provision did not inflict any significant harm on the rightholders, the High Court quashed the amendment ruling that the UK government had failed to demonstrate that the introduced exception fell within the scope of Recital 35. Therewith, the High Court set high standards, but it would not be surprising if the ECJ were to adopt a similar approach in case a Member State adopts or maintains a broad private copying exception without *any* compensation for rightholders.

62 Although Luxembourg's Copyright Act includes a private copying exception in Article 10(1)(4°) that enshrines an obligation to fairly compensate, it does not currently operate a levy system or any other form of collective programme that actually compensates reproduction rightholders. Luxembourg's exception replicates almost verbatim the wording of Article 5(2)(b) of the InfoSocDir, thereby implementing one of that provision's broadest possible scopes. Therefore, it is unlikely that Article 10(1)(4°) of Luxembourg's Copyright Act inflicts, in the sense of Recital 35 of the InfoSocDir, only zero or minimal harm on the rightholders. Against this backdrop, it is unclear whether and, if so, how Luxembourg's private copying exception is to be applied in conformity with the Member State's obligations under EU law. One can think of three potential approaches *de lege lata* whereof none is particularly compelling.

63 This paper proposes that the Grand Duchy should consider setting up an express compensation scheme. Given the discretion afforded to Member States under EU law, Luxembourg may implement a level of compensation lower than that of many other European countries – as Member States are only obliged to provide fair compensation, whereas Luxembourg's neighbours have adopted higher levels of equitable remuneration. Instead of setting up a cumbersome levy system, the Grand Duchy should consider funding such fair compensation through its state budget. This is also recommended for other Member States concerned about the regulatory and administrative burdens associated

183 A Lucas-Schloetter, 'La rémunération pour copie privée dans la tourmente (2e partie)' (2013) Légipresse 661, sec C.III

with implementing a levy system. In principle, the ECJ permits such an approach provided that the Member State ensures that the cost of the compensation is borne by the users of private copies. Countries like Finland, Norway, and Spain already have experience in running such a scheme, and their experiences can inform Luxembourg's own implementation. Luxembourg could manage and distribute such funds through an existing collective management organisation. A Member State's support of social and cultural establishments that benefit reproduction rightholders can count towards the required fair compensation – and Luxembourg is already highly active in supporting its unique and vibrant cultural scene. Taking such funding into account would limit the need for additional spending if the Grand Duchy were to implement an indirect fair compensation scheme for private copying via its state budget, effectively killing two birds with one stone.

JIPITEC

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

www.jipitec.eu