jipitec

1 | 2023

Volume 14 (2023)
Issue 1 ISSN 2190-3387

Editorial
by Axel Metzger

Articles
Privacy-compliant design of Cookie Banners according to the GDPR
by Gerald Spindler and Lydia Förster

Home is where the heart is
The household exemption in the 21st centurys
by Bart van de Sloot

Shaping the field of EU Data Law
by Nine Riis

The Digital Services Act: transparency as an efficient tool to curb the spread of disinformation on online platforms?
by Alain Strowel and Jean De Meyere

Authorless AI-assisted productions
Recent developments impacting their protection in the European Union
by Marta Duque Lizarralde and Christofer Meinecke

Creations of artificial intelligence
In search of the legal protection regime
by Anna Shtefan

All Agents Created Equal?
The Law's Technical Neutrality on AI Knowledge Representation
by Philipp Lerch

Prior filtering obligations after Case C-401/19: balancing the content moderation triangle
by Willemijn Kornelius

Copyright Protection of Broadcasts in Australia
by Kanchana Kariyawasam and Anubhav Dutt Tiwari

Actions and reactions in commodifying cultural heritage hosted in museums
by Cristiana Sappa

To Grant or Not to Grant
Injunctions in the World of Standard Essential Patents
by Michelle Dias and Mudita Gairola

Transparency as a legal value for patent disclosure
by Daria Bohatchuk

Platform regulation, content moderation, and AI-based filtering tools
by María Barral Martínez

Statements
ALLEA Statement on Open Access Publication Under "Big Deals" and the new Copyright Rules
by ALLEA

Book Reviews
Book Review on Data financed apps as a matter of data protection law
by Oliver Vettermann

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

www.jipitec.eu

jipitec

Journal of Intellectual Property, Information Technology and Electronic Commerce Law

Volume 14 Issue 1 May 2023
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

by Axel Metzger 1

Articles

Privacy-compliant design of Cookie Banners according to the GDPR
by Gerald Spindler and Lydia Förster 2

Home is where the heart is
The household exemption in the 21st centurys
by Bart van de Sloot 34

Shaping the field of EU Data Law
by Nine Riis 54

The Digital Services Act: transparency as an efficient tool to curb the spread of disinformation on online platforms?
by Alain Strowel and Jean De Meyere 66

Authorless AI-assisted productions
Recent developments impacting their protection in the European Union
by Marta Duque Lizarralde and Christofer Meinecke 84

Creations of artificial intelligence
In search of the legal protection regime
by Anne Shtefan 95

All Agents Created Equal?
The Law's Technical Neutrality on AI Knowledge Representation
by Philipp Lerch 108

Prior filtering obligations after Case C-401/19: balancing the content moderation triangle
by Willemijn Kornelius 123

Copyright Protection of Broadcasts in Australia
by Kanchana Kariyawasam and Anubhav Dutt Tiwari 148

Actions and reactions in commodifying cultural heritage hosted in museums
by Cristiana Sappa 161

To Grant or Not to Grant
Injunctions in the World of Standard Essential Patents
by Michelle Dias and Mudita Gairola 180

Transparency as a legal value for patent disclosure
by Daria Bohatchuk 190

Platform regulation, content moderation, and AI-based filtering tools
by María Barral Martínez 211

Statements

ALLEA Statement on Open Access Publication Under "Big Deals" and the new Copyright Rules
by ALLEA 222

Book Reviews

Book Review on Data financed apps as a matter of data protection law
by Oliver Vettermann 227

Editorial

by **Axel Metzger**

Recommended citation: Axel Metzger, Editorial, 14 (2023) JIPITEC 1 para 1.

1 It is with great pleasure that I may introduce you to the 1st edition of the 14th volume of the JIPITEC. Established in 2009, JIPITEC has now existed for 13 years. Current development milestones are (year-end 2022) the publication of 333 articles and 330,000 retrievals of these articles. Since 2010, we have published 3 editions per year, with some years seeing four publications with the inclusion of Special Issues.

2 While the first issues required an active solicitation for articles, we have since grown and our editors now receive significantly more submissions than can be accepted. Currently, the rejection rate is at around 66%, meaning that two out of every three submissions are not accepted. This is a testament to the high-quality standards that our editors and reviewers apply. For this issue, of the 31 submissions received, 12 were accepted by our team.

3 With the end of the year 2022, Chris Reed from Queen Mary University of London has left the editorial board. Chris has been active as editor since early 2016 and has helped JIPITEC with his expertise in information technology and accuracy as an editor-in-chief for a number of outstanding issues of the journal. We have truly appreciated his tremendous contribution to the journal. In his place, we are pleased to introduce Prof. Orla Linskey from London School Economics who will join the editorial board as our new UK editor. Welcome, Orla!

4 There are also some changes with our technical editor team. This will be the final issue produced by Lydia Förster. Her patience and diligence in producing numerous JIPITEC issues has been unparalleled, and we are immensely grateful for her efforts. In her place, we would like to welcome Lars Flamme, who will step into her shoes for the next issue and will be the future contact for our authors, reviewers, and editors. Welcome, Lars!

5 Issue 1/2023 explores a variety of highly relevant themes in both information technology and intellectual property law:

I hope you enjoy reading!

Privacy-compliant design of Cookie Banners according to the GDPR

by **Gerald Spindler and Lydia Förster***

Abstract: Cookie banners appear on almost every website or application we access, but as often as they appear, as rarely do they comply with mandatory (data protection) laws. This is mainly due to the abundance of - partly diverging - regulations on national and international level. This article attempts to evaluate relevant legislative acts as well as European Guidelines, Recommendations and Decisions to determine what a privacy-compliant consent banner should contain.

Keywords: Cookie Banner; Dark Patterns; Cookies; Consent Banners; GDPR; Consent

Recommended citation: Gerald Spindler and Lydia Förster, Privacy-compliant design of Cookie Banners according to the GDPR, 14 (2023) JIPITEC 2 para 1.

A. Introduction

1 The General Data Protection Regulation has now been in force for 4 years. Its declared aim is to strengthen the fundamental right of the protection of personal data. One of the key elements in this context is the obligation of the data processor to obtain consent of the data subject. In this regard, users shall be given the opportunity to make a voluntary, specific and informed declaration of consent or refusal for each process that concerns their personal data. In the digital space, consent tools are typically used to request the consent of the data subject. When deploying and using these consent tools, it is also a basic principle that they must enable a granular, free and informed decision. However, this theoretical approach is at odds with current practice—a recent study conducted by the Federation of German Consumer Organisations (vzbv) concluded that one in ten consent tools (in form of a cookie banner) is illegal.[1] Consumer surveys in recent years have also repeatedly shown that consumers do not feel informed about what happens to their data and do not trust the processors.[2] However, this is not surprising, as 141-page cookie banners without reject-button are common practice.[3]

* Prof. Dr. Gerald Spindler is holder of the chair of Civil Law, Commercial and Economic Law, Comparative Law, Multimedia- and Telecommunication Law and head of the Institute for Business Law at the University of Göttingen, Germany and Lydia Förster is Ph.D. student at Prof. Spindler's chair at the University of Göttingen and research assistant at YPOG Law in Hamburg.

1 A total of 949 websites were examined, in detail: Federation of German Consumer Organisations <www.vzbv.de/pressemitteilungen/jedes-zehnte-cookie-banner-ist-klar-rechtswidrig> accessed 11 December 2022.

2 European Commission, 'Special Eurobarometer 431 Data Protection Report' (2015), p. 66 <https://slidelegend.com/eurobarometer-431-european-commission-europa-eu_59b42a331723dd6c7341efd0.html> accessed 11 December 2022; Bitkom, 'Datenschutz in der digitalen Welt' (2015), p.7 <www.bitkom.org/sites/default/files/file/import/Bitkom-Charts-PK-Datenschutz-22092015-final.pdf> accessed 11 December 2022.

3 A Cookie Banner like this was for example used by the online news service *Focus online* (belonging to the media company *Burda Media)*, but was recently declared invalid by Regional Court Munich, since such an overlong banner, which does

2 One of the reasons for this disappointing result is that in addition to the GDPR, there are other area-specific regulations such as the ePrivacy Directive, and the Telecommunications Telemedia Data Protection Act (TTDPA). It is difficult to extract a clear guideline from this complex set of regulations, especially since none of the laws provides precise specifications regarding the concrete design of digital consent tools. Thus, the aim of this article is to determine which standards apply to obtaining consent in the digital space and to what extent. Furthermore, the specific design of a consent tool according to these standards will be assessed.

3 To this end, the functionality of cookies is first explained (B.) and a legal classification of cookies is made in order to determine which legal norms are applicable (C.). The focus will then shift to the question of whether consent is required under these standards and what requirements must be met for effective consent (D. and E.). Simultaneously, the relationship between the relevant provisions have to be evaluated to provide a precise legal assessment. Finally, this theoretical background is complemented by a chapter on the implementation of the specifications in practice (F.). The problems of consent tools will also be highlighted (G.). The study concludes with an overview of alternative consent methods (H.).

B. (Technical) Principles

4 The term cookies refers to small data files created by a web server or a script that can be placed on computers, smartphones, and other smart devices.[4] They usually store and transmit certain information about preferences like, e.g., user name, language, and (browsing) activities on visited websites to the provider of the cookie[5], who does not have to be identical to the operator of the website (*Third-party Cookie*).[6] The information the cookie stores vary, but it contains at least the name of the web server, from which it was created and a unique identifier (*Cookie-ID*), which enables the web server to recognize a user.[7]

I. Structure and functioning of HTTP Cookies

5 Cookies are simple text files consisting of a *Name* and a *Value*.[8] The cookie is either sent to the browser by the web server or created in the browser by a script (e.g. Javascript). The web server can then read the information directly from the server when the page is visited or transfer the information to the server via the website's script. Cookie information is stored locally on the particular device in the browser.[9] During a revisit to a particular website, the client browser searches for all cookies of this domain that match the web server and the directory path of the current request.[10]

II. Types of cookies

1. Technically necessary cookies

6 Technically necessary cookies are indispensable to be able to use a website and its basic functions. They serve, for example, to maintain the login over the duration of the visit to a website.[11]

2. Performance cookies

7 These types of cookies store information about how a website is used, for example, how long it takes for web pages to load, how the website performs with different browsers, or whether any errors have

not even contain an easily accessible reject button, ensures neither the voluntariness nor the informedness required for consent according to the TTDPA in conjunction with the GDPR, Regional Court Munich, Decision of 29 November 2022 – 33 O 14766/19, pp. 194 ff.

4 Philipp Hacker, *Datenprivatrecht* (1st edn, Mohr Siebeck 2020) 27; Lisa Gradow, Ramona Greiner, *Quick Guide Consent Management* (Springer, 1st edn 2021) 5; detailed on the types and functioning of cookies: Stefan Ernst, 'Cookies nach der EuGH-Entscheidung "Verbraucherzentrale Bundesverband/Planet49"' [2020] WRP, 963.

5 Gradow, Greiner (n 4) 6.

6 Hacker (n 4) 27.

7 Marian Arning, Tobias Born, 'Information als Wirtschaftsgut' in Nikolaus Forgó, Marcus Helfrich, Jochen Schneider (eds), *Betrieblicher Datenschutz* (3rd edn, C.H. Beck 2019, Part XI. chap. 2) para. 51.

8 Stefan Hanloser, 'Geräte-Identifier im Spannungsfeld von DS-GVO, TMG und ePrivacy-VO' [2018] ZD 213 (214 f.).

9 Hacker (n 4) 27.

10 Céline Wenhold, *Nutzerprofilbildung durch Webtracking* (1st edn, Nomos 2018) 56 f.

11 Ernst (n 4) 963.

occurred. The information is usually aggregated and used to improve the functioning of a website.[12]

3. Functional cookies

8 These types of cookies are primarily designed for the user's convenience, as they store information about their preferences, such as language settings and usernames or text size adjustments.[13]

4. Tracking/marketing cookies

9 Finally, tracking or marketing cookies collect information that help the provider (usually a third party) to place personalised advertising. They store, e.g., information about the frequency of access and the processed content. Advertising cookies enable behavioural information to be stored as part of the management of advertising by observing habits, which creates a profile of the user's preferences to be able to offer advertising customised to the interests of their profile.[14]

C. Legal classification of cookies

10 The first step in clarifying how the use of cookies can be legally compliant is to determine how they are classified legally, and which norms and regulations apply to them.

I. Personal data according to the GDPR

11 To fall within the scope of the application of the GDPR, the information stored by the cookies would have to be considered "personal data" within the meaning of Article 4 No. 1 GDPR. According to Art. 4 No. 1 GDPR, personal data is any information that relates to an identified or identifiable individual. "Identifiable" means any person who can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person. In determining whether a natural person is identifiable, Recital 26 GDPR states that the account shall be taken of all the means reasonably likely to be used by the controller or by any other person to identify the natural person. This means that the identifiability does not only apply to data that establishes a reference in itself, but also to data that must first be linked to further information (possibly with the help of third parties).[15] In determining whether the means are reasonably likely to be used to identify the natural person, any objective factors, such as the cost of identification and the time required, shall be taken into account, including the technology and technological developments available at the time of the processing, compared with Recital 26 GDPR. However, the extent to which also the (potential) knowledge and the (potential) means of third parties must be taken into account is disputed; more precisely, there is dissent as to whether every possibility of a reference to a person by a third party leads to identifiability (absolute approach[16]), or whether the focus lays mainly on the responsible person and their resources (relative approach[17]). The dispute already existed before the GDPR came into force and centered on the concept of determinability.[18] However, even with the enactment

12 Ernst (n 4) 963.

13 Ernst (n 4) 963.

14 Ernst (n 4) 963.

15 Stefan Ernst, 'Art. 4 DS-GVO' in Boris Paal, Daniel Pauly (eds), *Datenschutz-Grundverordnung* (C.H. Beck, 3rd edn 2021) para 12; Moritz Karg, 'Art. 4 Personenbezogenes Datum' in Spiros Simitis, Gerrit Hornung, Indra Spiecker gen. Döhmann (eds), *Datenschutzrecht* (Nomos, 1st edn 2019) para 46; Peter Gola, 'Art. 4' in Peter Gola (ed), *DS-GVO Kommentar* (2nd edn, C.H. Beck 2018) para 16; Achim Klabunde, 'Art. 4' in Eugen Ehmann, Martin Selmayr (eds), *DS-GVO Kommentar* (2nd edn, C.H. Beck 2018) para 17; Jürgen Kühling, Manuel Klar, 'Art. 4' in Jürgen Kühling, Benedikt Buchner (eds), *Datenschutz-Grundverordnung BDSG Kommentar* (3rd edn, C.H. Beck 2020) paras 20 ff.; Alexander Arning, Tobias Rothkegel, 'Art. 4 DSGVO' in Jürgen Taeger, Detlev Gabel (eds), *DSGVO – BDSG – TTDSG* (4th edn, R&V 2022) para 30.

16 Benedikt Buchner, 'Grundsätze und Rechtmäßigkeit der Datenverarbeitung unter der DS-GVO' [2016] DuD 155 (156); Max Dregelies, 'Wohin laufen meine Daten?' [2017] VuR 256 (257); in this direction Klabunde (n 15) Art. 4 para 17 according to whom it is sufficient that any third party carries out the identification, but this must at least be generally probable; also in this direction: Stefan Herbst, 'Was sind personenbezogene Daten?' [2016] NVwZ 902 (906) who speaks of a *factual-absolute* personal reference.

17 Klar, Kühling (n 15) DS-GVO Art. 4 para 26; Johanna Hofmann, Paul Johannes, 'DS-GVO: Anleitung zur autonomen Auslegung des Personenbezugs' [2017] ZD 221 (225 f.); Arning, Rothkegel (n 15) DS-GVO Art. 4 para 31; Jens Eckhardt, 'Anwendungsbereich des Datenschutzrechts – Geklärt durch den EuGH?' [2016] CR 786 (789).

18 For a detailed explanation of the previous controversy on the interpretation of the concept of *determinability* with

of the GDPR, it could not be conclusively clarified; the spectrum ranges as already mentioned from a strictly absolute approach, according to which any way of linking leads to identifiability, including illegal ways, to a strongly relative approach, according to which it only depends on the person processing the data.[19] However, based on the GDPR and the recent case law of the CJEU, the following picture emerges:

12 Due to the fact that the text of the GDPR is ambiguous, its interpretation is ultimately not completely conclusive. Nevertheless, what can be stated is that the GDPR and the case law of the CJEU, especially when viewed together, tend towards a relative approach, albeit with some objective criteria.[20]

13 According to Recital 26 (3) GDPR, all means must be considered that are generally likely to be used by the controller or a third party to identify the natural person directly or indirectly. This is not a conclusive statement, as it does not specify when this probability exists and how wide the range of means considered is to be drawn. In any case, however, it is a rejection of the extremely relative theory, according to which only the responsible person's means are to be considered.[21] The wording of Recital 26 is explicitly broader in this respect. Thus, the resources of third parties must also be considered.

14 A further specification of the resources to be included was made by the CJEU in its *Breyer* ruling: According to this the effort, the actual availability, and also the legal permissibility of access to the knowledge or the relevant methods must be taken into account.[22] Prohibited methods were thus explicitly excluded by the CJEU.[23] However, the scope of application is also broadly drawn so that not only the knowledge and methods of the third party are relevant, but also whether the third party can establish a reference with the help of the participation of a fourth party.[24] Overall, this means that for the identifiability, the knowledge and resources of third parties must be taken into account when they are legally permitted and to a certain extent probable; purely fictitious possibilities must be disregarded.[25] In this regard, however, it should be critically noted that legal admissibility cannot be the primary criterion and illegal means cannot be excluded per se.[26] On the one hand, this results from the wording of Recital 26, which states that, in principle, all factors should first be included, insofar as their use is sufficiently probable. The fact that some methods are illegal does not make them generally unlikely. Instead of focusing on the abstract status of illegality or conformity with the law, the focus should rather be on whether the factual proximity and thus the possibility of using the data for identification is given.[27] According to the Article 29 Data Protection Working Party, a mere hypothetical possibility, in turn, is not enough to consider a person as identifiable.[28]

15 Thus, the term "all the means likely reasonably to be used" in Recital 26 include several factors such as the costs of conducting identification, the way the processing is structured, the advantage expected by the controller, "the intended purpose, the interests at stake for the individuals, as well as

further references see Matthias Bergt, 'Die Bestimmbarkeit als Grundproblem des Datenschutzrechts Überblick über den Theorienstreit und Lösungsvorschlag' [2015] ZD 365 and Stefan Brink, Jens Eckhardt, 'Wann ist ein Datum ein personenbezogenes Datum? Anwendungsbereich des Datenschutzrechts' [2015] ZD 205.

19 In detail with further reference: Herbst (n 16) 903 ff.

20 This finding is also reached by Klar, Kühling (n 15) DS-GVO Art. 4 para 26; Niko Härting, 'Datenschutz-Grundverordnung Anwendungsbereich, Verbotsprinzip, Einwilligung' [2016] ITRB 36 (36 f.); Florian Jotzo, *Der Schutz der personenbezogenen Daten* (Nomos, 2nd edn 2020) Part 2 Sachlich anwendbares Datenschutzrecht paras 97 f.; Wolfgang Ziebarth, 'Art. 4 DSGVO' in Gernot Sydow, Nikolaus Marsch (eds), *Europäische Datenschutzgrundverordnung* (3rd edn, Nomos 2022) para 37; In this direction: Peter Schantz, 'Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht' [2016] NJW 1841 (1843).

21 Peter Meyerdierks, 'Sind IP-Adressen personenbezogene Daten?' [2009] MMR 8 (12) on the principle of determability.

22 CJEU Case C-582/14 *Breyer/Germany* [2016] ECLI:EU:C:2016:779 paras 42 ff.

23 CJEU Case C-582/14 *Breyer/Germany* [2016] ECLI:EU:C:2016:779 para 46.

24 CJEU Case C-582/14 *Breyer/Germany* [2016] ECLI:EU:C:2016:779 para 43.

25 Arning, Rothkegel (n 15) DS-GVO Art. 4 para 35; Ernst (n 15) DS-GVO Art. 4 paras 10 f.; Klar, Kühling (n 15) DS-GVO Art. 4 para 28; Klabunde (n 15) DS-GVO Art. 4 para 17.

26 Affirmative: Herbst (n 16) 905; Karg (n 15) Art. 4 „Personenbezogenes Datum" para 64; disapproving: Peter Meyerdierks (n 21) 11 f. to the former legal situation on the interpretation of the concept of *determinability*.

27 Georg Borges, 'DSGVO Art. 4' in Georg Borges, Marc Hiller (eds), *BeckOK IT-Recht* (7th edn, C.H. Beck 1.7.2021) para 20; Herbst (n 16) 905; Art. 29 Data Protection Working Party Opinion 4/2007 on the concept of personal data, WP 136, 01248/07/EN, 19.

28 Art. 29 Data Protection Working Party (n 27) 15.

the risk of organisational dysfunctions (e.g. breaches of confidentiality duties) and technical failures".[29]

16 When applied to cookies, the result is as follows: Cookies themselves do not allow the identity of the user to be determined, as they do not contain any real names or similar directly identifying information.[30]

17 Beyond this, a distinction must be made: if the cookie merely stores user preferences or similar information in anonymous forms so that they can be retrieved when the website is closed and revisited, there will generally be no personal reference.[31] However, a different finding is reached if additional information is available. Both cookie information and the additional information must allow for identification when viewed together.[32] This applies in particular if a Cookie-ID is assigned, and the information is not stored anonymously. Usually, other digital traces (e.g. the IP address, log-in data) are left on visited websites, which, in combination with the unique Cookie ID, enables an identification.[33] This view seems to be shared by the CJEU, which determined that identifiability can be given if there is the possibility of merging cookies and the registration data entered on the website.[34] In addition, a personal reference may also exist if several cookies are combined to create a user profile, for example, to be able to show personalized advertising to the user.[35] This also results indirectly from Recital 30 and Article 4 No. 11 GDPR, which provide that profiling, including the creation of user profiles by combining and evaluating personal data, falls within the scope of the GDPR and explicitly mention cookies as a possible data basis for profiling.

18 Overall, no general statement can be made. A case-by-case examination is always necessary: cookies are personal data if they, together with other information or other cookies, enable a concrete reference to a person. This is particularly likely if the user is assigned a unique Cookie-ID. In addition, a reference to a person can also exist if the combination of cookies enables a unique user profile so that the reference to a specific person is given. If several parties are involved in the data collection and processing, identifiability is not precluded automatically. In this case, it must be examined whether the reference can be established by the responsible person and the third party with sufficient probability using the available means.

II. Storage of or access to information according to the ePrivacy Directive

19 Based on Article 5 (3) ePrivacy Directive 2002/58/EC[36], the regulations of the Directive are applicable when either information is stored on the user's terminal equipment or when stored information is accessed. This corresponds to the way cookies function: they store information in the browser and thus on the user's device to retrieve it directly or subsequently.[37] While this already opens the scope of application of the directive, it can be further stated that the Directive does not distinguish between personal and non-personal information.[38] Instead, all types of information are covered by Article 5 (3).[39] The relationship of both the ePrivacy Directive as well as any corresponding transposition legislation

29 Art. 29 Data Protection Working Party (n 27) 15.

30 Klar, Kühling (n 15) DS-GVO Art. 4 para 36; Peter Schmitz, in Thomas Hoeren, Ulrich Sieber, Bernd Holznagel (eds), *Handbuch Multimediarecht* (58th edn, C.H. Beck March 2022) Part. 16.2 para 76.

31 Anno Haberer, 'Anforderungen an Cookie-Banner' [2020] MMR 810 (811).

32 Borges (n 27) DS-GVO Art. 4 para 25; Klar, Kühling (n 15) DS-GVO Art. 4 No. 1 para 36.

33 This is also indicated by recital 30 GDPR.

34 CJEU Case C-673/17 *Planet49* [2019] ECLI:EU:C:2019:801 paras 45, 69.

35 Ulrich Baumgartner, Guido Hansch, 'Onlinewerbung und Real-Time-Bidding' [2020] ZD 435 (436).

36 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, 37 ff.

37 Schmitz (n 30) Part. 16.2 para 76; Louisa Specht-Riemschneider, ‚Verbraucherdatenschutzrecht' in Louisa Specht, Reto Mantz (eds), Handbuch Europäisches und deutsches Datenschutzrecht (1st edn, C.H. Beck 2019) Sec. 9 Verbraucherdatenschutz para 63; Andreas Sesing, ‚Cookie-Banner – Hilfe, das Internet ist kaputt!' [2021] MMR 544.

38 Specht-Riemschneider (n 37) Sec. 9 Verbraucherdatenschutz para 66; Wolf-Tassilo Böhm, *Valentino* Halim, 'Cookies zwischen ePrivacy und DS-GVO – was gilt?' [2020] MMR 651.

39 Other opinion by the Danish Business authority which stated that the recording of MAC addresses of users' mobile devices is not subject to the requirements of providing information and obtaining consents from the users under the Danish Cookie Order, which implements Art. 5(3) of the ePrivacy Directive because no identification is possible; rightly critical of this opinion: Charlotte Tranberg, Storing Information on User's Devices [2015] EDPL 130 (136).

(Section 25 TTDPA) to other legal acts, in particular the GDPR, will also be of importance for the further course of the paper and has to be assessed in detail.[40]

III. Storage of or access to information according to the TTDPA

20 The Telecommunication-Telemedia-Data-Protection-Act (TTDPA) has come into force on 1 December 2021 and serves to adapt the TCA and the TMA to the GDPR, as well as to implement the ePrivacy Directive.[41] Primarily, the legal uncertainties caused by the coexistence of several laws should be eliminated.[42] According to Section 1 No. 2 TTDPA, the TTDPA focuses on the protection of data when using telecommunications services and telemedia. Pursuant to Section 2 (2) No. 1 TTDPA, a provider of telemedia is any natural or legal person, who provides their own telemedia services or those of a third party, participates in the provision of or provides access to the use of their own or third-party telemedia mediates. According to Section 1 (1) S. 1 TMA, telemedia are all electronic information and communication services, unless they are telecommunications services, telecommunications-based services, or broadcasting. The term telemedia services thus includes online offers of goods and services with the possibility of direct ordering, video on demand, internet search engines, but also "simple" homepages.[43] For the definition of the telecommunications provider, the TTDPA refers in Section 2 (1) TTDPA to the amended Telecommunications Act. In addition to so-called number-based interpersonal telecommunications services, the amended TCA now also covers number-independent interpersonal communications services according to Section 3 TCA. This means that "*over-the-top (OTT)*"[44] communication services, such as messengers like WhatsApp, also constitute telecommunications services.[45]

21 Section 25 TTDPA is particularly relevant for the use of cookies, and closely follows the wording of the ePrivacy Directive: the provision is applicable when information is stored on the user's terminal equipment or when such information is accessed. In this context, it is irrelevant whether this information is personal data or not. As explained above, this is precisely how cookies are designed to function.

IV. Excursus: processing of information according to the ePrivacy Draft Regulation

22 The ePrivacy Regulation was originally intended to come into force at the same time as the GDPR and to introduce specific regulations for the area of electronic communication that would specify and supplement the general regulations of the GDPR.[46] This makes it particularly relevant for the use of cookies, but the planned introduction failed—no agreement has been reached to this day. Trialogue negotiations with the Parliament and the Commission are ongoing.[47] Although an agreement is not to be expected soon, an overview of the legal requirements of the current draft of the ePrivacy Regulation for cookies should be provided: According to the current draft of the ePrivacy Draft Regulation, it applies to the processing of electronic communications data carried out in connection with the provision and the use of electronic communications services and to information related to the terminal equipment of end-users, compared with Article 2 ePrivacy Draft Regulation. In contrast to the GDPR, the applicability does not depend on the content of the information; similar to the ePrivacy Directive the regulation is supposed to apply to non-personal data as well[48], so

40 Cf. part D.3.

41 Bundesregierung, 'Explanatory Memorandum to the government draft', BT-Drs. 19/27441, 1.

42 Bundesregierung, 'Explanatory Memorandum to the government draft', BT-Drs. 19/27441, 1.

43 Gesellschaft für Datenschutz und Datensicherheit e.V., 'GDD-Praxishilfe: Das neue TTDSG im Überblick' (June 2021) 3.

44 Services that are offered via an Internet connection without the Internet service provider having providers themselves have any influence or control over the service would have. OTT services are therefore decoupled from the infrastructure providers.

45 Thomas Wilmer, in Anne Riechert, Thomas Wilmer (eds), *TTDSG* (1st edn, Erich Schmidt Verlag 2022) § 2 para 6.

46 Cf. European Commission, 'Explanatory memorandum for the proposal 2017/0003(COD)', Part. 1.1. Reasons for and objectives of the proposal.

47 In detail on the legislative procedure until the recent Trilogue negotiations Pascal Schumacher, Lennart Sydow, Max von Schönfeld, 'Cookie Compliance, quo vadis?' [2021] MMR 603 (605).

48 Critical in this regard: Nils Rauer, Diana Ettig, 'Rechtskonformer Einsatz von Cookies' [2018] ZD 255 (257) who criticize that this creates disincentives.

according to Article 8 (1) ePrivacy Draft Regulation, all information from terminal equipment of end users is placed under a processing ban.

D. Requirement for consent

23 First of all, it must be clarified whether and from which regulations a requirement for consent arises, which requirements are placed on the respective consent, and when which consent is required.

I. Requirement for consent according to the GDPR

24 Article 6 GDPR regulates the lawfulness of data processing. In addition to consent under Article 6 (1) lit. a GDPR, processing can also be based on other reasons, which are, however, largely excluded from this analysis. Accordingly, it must first be explained for which types of cookies consent is required under the GDPR and which cookies can generally be based on other legal grounds.

25 Besides consent, the necessity for the fulfillment of the contract according to Article 6 (1) lit. b GDPR or the legitimate interest according to Article 6 (1) lit. f GDPR come into consideration. Necessity is interpreted rather narrowly: a simple connection of the data processing to the contract is not sufficient.[49] Instead, it must be indispensable to achieve the purpose of the contract.[50] In the digital context, a rough guideline is: if the website or the app does not function properly without the cookie, there is a necessity for the placement of the cookie.[51] This will be the case in particular for technically necessary cookies, which is why these usually do not require consent.[52] For all other types of cookies, it must be examined whether there is a legitimate interest within the meaning of Article 6 (1) lit. f GDPR. In principle, economic interests are not excluded[53], which is likely to be particularly relevant for advertising cookies. Nevertheless, this interest must always be weighed against the interests, fundamental rights, and freedoms of the data subject.[54] No general statements can be made, as trends will only become apparent through future decisions in the course of the next few years. However, freedoms protected by fundamental rights, such as the right to informational self-determination, shall principally be weighted higher than interests protected by simple law, like e.g. pure profit maximization.

26 Overall, it can be concluded that only technically necessary cookies are usually exempted from the consent requirement; for all other types of cookies, a thorough examination must take place, which will probably often lead to consent being required, especially for advertising and tracking cookies.[55]

II. Requirement for consent according to the ePrivacy Directive

27 In accordance with Article 5 (3) ePrivacy Directive, consent is also required for the storage or assessment of information on terminal equipment. However, pursuant to Article 2 lit. f and Recital 17 ePrivacy Directive in combination with Article 94 (2) GDPR, consent is governed by the Data Protection Directive, which has been replaced by the GDPR. This means that the principles of Article 4 No. 11 and Article 7 GDPR also apply to consent under the ePrivacy Directive. Therefore, the requirements for consent according to Article 5 (3) ePrivacy Directive do not differ from the requirements according to Article 4 No. 11 and No. 7 GDPR. Thus, reference can be made to the explanations given above.

28 Similar to the GDPR, the ePrivacy Directive provides for an exception to the consent requirement in case of necessity. According to Article 5 (3) s. 2 ePrivacy Directive, storage or access is permitted if it is strictly necessary in order to provide the information service requested by the user. Again, the Article 29 Working Party advocated for a narrow interpretation of necessity, which would only exist if the functionality of the service could not be

49 Marion Albers, Raoul-Darius Veit, 'Art. 6 DSGVO', in Heinrich Amadeus Wolff, Stefan Brink (eds), *BeckOK DatenschutzR* (41th edn, C.H. Beck 01.11.2021) DS-GVO Art. 6 para 44; Sebastian Schulz, 'Art. 6' in Peter Gola (ed), *DS-GVO Kommentar* (2nd edn, C.H. Beck 2018) para 38; Eike Michael Frenzel, 'Art. 6 DSGVO', in Boris Paal, Daniel Pauly (eds), *Datenschutz-Grundverordnung* (3rd edn, C.H. Beck 2021) para 14.

50 Horst Heberlein, 'Art. 6 DS-GVO', in Eugen Ehmann, Martin Selmayr (eds), *DS-GVO Kommentar* (2nd edn, C.H. Beck 2018) para 13; Jürgen Taeger, 'Art. 6 DSGVO' in Jürgen Taeger, Detlev Gabel (eds), *DSGVO – BDSG – TTDSG* (4th edn, R&V 2022) para 49; Schulz (n 49) para 38; Albers, Veit (n 49) para 44.

51 Also: Gradow, Greiner (n 4) 10 f.; Haberer (n 31) 810 (815).

52 Sesing (n 37) 545; Haberer (n 31) 812.

53 Conference of the Independent Data Protection Authorities of the Federal State and the *Länder* (DSK), 'Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien' (March 2019) 11.

54 CJEU Case C-40/17 *Fashion ID/Verbraucherzentrale NRW* [2019] ECLI:EU:C:2019:629 para 95.

55 DSK (n 53) 10.

guaranteed without the cookie.[56] The simplification or acceleration of certain processes by a cookie is not sufficient to affirm a necessity.[57] This will usually apply to technically necessary cookies. Article 29 Working Party mentions—among others as examples of the exception—*User input cookies*[58], which, for example, store which items have been placed in the shopping basket on a shopping site, or *authentication cookies*[59], which serve to recognize a person who has logged in once as being logged in again and to provide them with access to the specific content (e.g. in online banking). According to the group, the exceptions explicitly do not include tracking cookies of social plug-ins, third party advertising cookies, and first party analysis cookies.[60] This seems only consistent in view of the strict interpretation of necessity, as these do not have a positive influence on the functionality of the website, but rather serve the processors.[61]

III. Requirement for consent according to the TTDPA

29 Initially, it should be noted that the TTDPA also applies to entities that do not have their registered office in Germany. According to Section 1 (3) of the TTDPA, the scope of application extends to all companies or persons that have a German branch office, provide goods or services on the German market, or participate in the provision of services. This combination of the market location principle and the country-of-origin principle establishes a very broad scope of application. Consent is also required under Section 25 (1) TTDPA. However, reference is also made to the GDPR with regard to requirements of a lawful consent. This means that the handling of personal and non-personal data will be assessed according to the GDPR. The above statements on consent apply accordingly. With regard to exceptions, the provisions of the ePrivacy Directive are followed closely. According to Section 25 (2) No. 2 TTDPA consent is not required if the storage of information in the end user's terminal equipment or the access to information already stored in the end user's terminal equipment is absolutely necessary so that the provider of a telemedia service can provide a telemedia service expressly requested by the user. Based on the narrow interpretation of the term under the ePrivacy Directive as proposed by the Article 29 Working-Party[62], mainly technically necessary cookies are likely to be excluded. For all other types, a case-by-case assessment is required, especially advertising and tracking cookies will generally not be *necessary*.

30 However, the scope of application of the TTDPA alongside the GDPR still needs to be clarified. The TTDPA is independent of content and therefore also applies if there is no personal data within the meaning of the GDPR, and also if no processing within the meaning of Article 4 No. 2 GDPR has been carried out. The exclusive scope of application of the TTDPA is thus not very large, which leads to the question of which law applies when a process falls within the scope of application of both standards. Since Section 25 of the TTDPA is the long-demanded implementation of the Article 5 ePrivacy Directive, Article 95 GDPR could possibly intervene and lead to a sector-specific priority of the TTDPA. However, the standards would have to pursue the same objectives. This is not the case: the TTDPA, and in particular Section 25 of the TTDPA, aims to protect the equipment's integrity, which becomes clear in several places. As already explained, information is protected regardless of its personal reference, and the protected person can also be a legal entity. The GDPR, on the other hand, only aims to protect personal data and thus the right to informational self-determination of the individual, which is why the priority rule from Article 95 GDPR does not apply. The explanatory memorandum to the draft legislation also indicates that it was not intended that the GDPR would also be superseded via Article 95 GDPR with regard to the processing of personal data, as it states that the subsequent use of data (i.e., the use after accessing or storing non-personal information) will continue to be governed by general data protection law, in particular by the GDPR.[63]

31 In the area of telemedia services, however, the demarcation is hardly of any significance, since on the one hand the storage of non-personal information is usually the preliminary stage to the storage and processing of personal data, and on the other hand the requirements for consent are identical. Consent under the TTDPA and the GDPR can also be bundled and given by the same act. This avoids a situation where the user, after giving consent under the TTDPA, has to give practically

56 Art. 29 Data Protection Working Party, Opinion 04/2012 on Cookie Consent Exemption, WP 194, 00879/12/EN, p. 4.

57 Charlotte Tranberg, Storing Information on User's Devices [2015] EDPL 130, 133.

58 Art. 29 Data Protection Working Party (n 56) 6.

59 Art. 29 Data Protection Working Party (n 56) 6f.

60 Art. 29 Data Protection Working Party (n 55) 9ff.

61 Supporting this view *Ernst*, WRP 2020, 962 (967).

62 Art. 29 Data Protection Working Party (n 56) 6ff.

63 Explanatory Memorandum to the government draft, BT-Drs. 19/27441, p. 38.

identical consent under the GDPR a few seconds later. However, it must be clear to the users that they are consenting to multiple things by clicking a single button.[64]

IV. Excursus: consent according to the ePrivacy Draft Regulation

32 According to Article 8 (1) ePrivacy Draft Regulation, consent is also required for the use and storage of information on the user's terminal equipment, where reference is also made to the GDPR for the definition and prerequisite. According to Article 9 of the proposed ePrivacy Regulation, the definition of and the conditions for consent provided for in Article 4 (11) and Article 7 GDPR apply. In consequence, obtaining consent under both the GDPR and the proposed ePrivacy regulation follows the same rules.[65] Thus, the results found above are in principle similarly applicable.[66]

33 However, the revocation provision in Article 7 (3) GDPR is supplemented by an obligation to remind the end user of his right of revocation every six months, cf. Article 9 (3) ePrivacy Draft Regulation. In addition, the strict limitation of purpose is loosened in Article 9 (2) ePrivacy Draft Regulation to the effect that it should be possible to give general consent to the use of cookies through the settings of the Internet browser.

V. Excursus: consent according to the IAB Transparency and Consent Framework & other industry guidelines

34 In recent years, large industry associations such as *IAB Europe*[67] and other firms like *ISiCO*[68] have also published data protection guidelines[69] that can supposedly be used to design consent tools in compliance with the GDPR.[70] According to IAB Europe, the Transparency & Consent Framework (TCF) is intended to create a legally compliant standard "*by the industry for the industry*" that will provide a standardized solution for obtaining consent in accordance with the ePrivacy Directive and the GDPR.[71] With its system, IAB Europe wanted to satisfy two industry needs at once: first, it should be made easier to serve personalized advertising, and second, it is intended to simplify the process of obtaining advertising consent.

35 The IAB tool is in the advertising industry particularly popular for so-called "real time bidding"[72] to facilitate the management of user preferences for personalized advertising. When accessing websites connected to the tool and the associated platform developed by IAB Europe, users are asked to consent to the processing of their personal data for advertising purposes. The system generates a user ID, collects information on this ID and enables the cross-service storage of the respective user's settings for the services connected to the TCF (so-called *Consent String*). When the user accesses a connected service that offers personalizable advertising space, the Consent String provides information about whether and which advertising is displayed to the user by feeding all available information into the

64 DSK, 'Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien' (December 2021) 9.

65 European Data Protection Board, Statement of the EDPB on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications, 25.05.2018, p. 2.

66 Cf. Part D.1.

67 The *Interactive Advertising Bureau Europe* is a global business organization in the online advertising industry with over 650 members, including global players such as *Google* and *Facebook.*

68 The *Informationssicherheit und Datenschutz Compliance GmbH* is a consulting firm that supports the implementation of European and national data protection regulations and the implementation of IT security and compliance systems.

69 *IAB Europe*, Transparency & Consent Framework v2.0 accessible via: https://iabeurope.eu/tcf-2-0/ (accessed 5th January 2023); *ISiCO*, Whitepaper: Cookie-Banner – Leitfaden zur sachgerechten Umsetzung accessible via: https://www.isico-datenschutz.de/blog/whitepaper-cookie-banner-dsgvo-konform/ (accessed 5th January 2023).

70 Cf. https://iabeurope.eu/transparency-consent-framework/ (accessed 5th January 2023).

71 Cf. https://iabeurope.eu/transparency-consent-framework/ (accessed 5th January 2023).

72 "Real-time bidding refers to the use of an instantaneous automated online auction for the sale and purchase of online advertising space. Specifically, it means that when an individual accesses a website or application that contains an advertising space, behind the scenes through an automated online auction system and algorithms, technology companies representing thousands of advertisers can instantly (in real time) bid for that advertising space to display targeted advertising specifically tailored to that individual's profile." APD, Decision of 2 February 2022 – DOS-2019-01377, para 22.

real-time auction of advertising space that takes place automatically in the background.[73]

36 However, guidelines from organizations and interest groups have no legitimizing effect; compliance with these guidelines and the use of abovementioned tools do not automatically lead to conformity with the GDPR, even if this is suggested. This is also confirmed by the recent ruling of the Belgian Data Protection Authority *Autorité de Protection des donneés* (APD), which declared the IAB Europe framework as incompatible with the GDPR.[74] In addition to numerous other violations, the consent mechanism is said to be invalid due to a lack of sufficient information (especially with regard to the aforementioned consent strings).[75] The standard for a legally compliant design of consent tools remains the GDPR, any industry guidelines, must be measured against it.

E. Conditions for effective consent under the GDPR

37 Although the use of cookies also falls within the scope of other laws, as just explained, there is always a reference to the GDPR, so that the GDPR always remains the central element for assessing the lawfulness of processing. Therefore, the requirements for an effective consent according to the GDPR will be further examined.

I. Form

38 Consent can be generally given without any formal requirements—any declaration of intent with explanatory value is necessary but also sufficient. According to Recital 32 GDPR it can be given in any form, including oral, written, and electronically transmitted declarations of consent. Even an implied declaration is principally possible—at least as long as it provides for a clear affirmative action.[76] However, according to Recital 32 GDPR mere silence does not have a sufficient explanatory value. In practical terms, this means that consent to the use of cookies is not given by continuing to browse on a website and disregarding the cookies banner. This does not constitute an unambiguously confirming act.[77] The same applies to the mere download of an app or other software: the download does not provide for a sufficient declaration of consent within the meaning of the GDPR.[78] Although the EU Commission and the European Parliament have not been able to enforce their demand that every consent must be explicit, the requirement of an "unambiguously indication" in Article 4 No. 11 and Recital 32 GDPR leads to a strong restriction of the generally possible implied consent[79], especially in the online area. Consent given through inactivity, e.g. by not unchecking pre-ticked consent fields, does not satisfy the requirement of a clearly confirming action.[80] This has now also been confirmed by the CJEU in its *Planet49* decision[81] and subsequently also by the Federal Supreme Court (BGH).[82] According to the courts, it is not sufficient for the consent requirement under the ePrivacy Directive (certainly not under the GDPR[83]) if the user

73 Detailed explanation of the process and involved parties: APD, Decision of 2 February 2022 – DOS-2019-01377, paras 20 ff.

74 APD, Decision of 2 February 2022 – DOS-2019-01377, paras 403 ff.

75 However, IAB Europe defended itself against the decision at the Court of Appeal in Brussels. The Court suspended the proceedings in order to submit two preliminary questions to the CJEU: first, whether the TC strings constitute personal data and second, whether IAB Europe can actually be classified as a responsible party within the meaning of the GDPR, cf. Hof van beroep Brussels, Decision of 7 September 2022 –2022/AR/292.

76 Bastian Stemmer, 'Art. 7 DS-GVO' in Heinrich Amadeus Wolff, Stefan Brink (eds), *BeckOK DatenschutzR* (41th edn, C.H. Beck 01.08.2022) para 84; But critical regarding the practicability of implied consent and also its compliance with data protection principles Benedikt Buchner, Jürgen Kühling, 'Art. 7', in Jürgen Kühling, Benedikt Buchner (eds), *Datenschutz-Grundverordnung BDSG Kommentar* (3rd edn, C.H. Beck 2020) Art. 7 para 27, Art 4 No. 11 para 58b; Critical of the practical suitability of the theoretically possible implied consent: Martin Franzen, 'Art. 4 DS-GVO' in Martin Franzen, Inken Gallner, Hartmut Oetker (eds), *Kommentar zum europäischen Arbeitsrecht* (4th edn, C.H. Beck 2022) para 20; Arning, Rothkegel (n 15) DSGVO Art. 4 para 283.

77 Kühling, Buchner (n 76) Art. 7 para 27; Specht-Riemschneider (n 37) para 33; Paul Voigt, Axel Freiherr von dem Bussche, *DSGVO Praktikerhandbuch* (Springer 2018) 122.

78 Philipp Albrecht, Florian Jotzo, *Das neue Datenschutzrecht der EU* (Nomos 2017) Part 3 para 39.; Kühling, Buchner (n 76) Art. 7 para 58c.

79 Schulz (n 49) DS-GVO Art. 7 para 42; in this direction also Philipp Albrecht, Florian Jotzo, *Das neue Datenschutzrecht der EU* (Nomos 2017) Part 3 para 39; Klabunde (n 15) Art. 7 para 36, Art. 4 para 53.

80 Cf. recital 32 sentence 3.

81 CJEU Case C-673/17 *Planet49* [2019] ECLI:EU:C:2019:801.

82 BGH MMR 2020, 609.

83 CJEU Case C-673/17 *Planet49* [2019] ECLI:EU:C:2019:801 para

does not deselect pre-ticked consent tick boxes.[84] This puts a stop to the practice of legitimizing cookies through opt-out consents, which has been common for a long time and still occurs today.[85]

39 Although this does not impinge on any formal requirement, it is nevertheless advisable—especially for the digital area—to obtain the declaration of consent in a material form. Otherwise it is hardly ever possible to prove that consent has been obtained, as required by Article 7 (1) GDPR. A cookie banner proves to be an effective method in this respect. If consent is obtained using such means (i.e. in electronic form), Recital 32 states that care must be taken to ensure that the request is clear, concise, and not unnecessarily disruptive to the use of the service for which it is provided. These requirements are strongly linked to the requirement that consent must be given in an informed manner. The controller must ensure that the electronic consent tool is clear in terms of form, content, color, and other design, and does not mislead the user; it must be clear that consent to the processing of data is given by the electronic tool. In particular, the extent or purposes of the processing must be clearly and unambiguously explained, as will be shown below.

II. Timing and duration

40 Effective consent has to be given at the time of processing and must therefore be obtained in advance.[86] This is not explicitly regulated in the GDPR, but already follows from the protective purpose and the general prohibition of processing.[87] By giving consent, the data subject expresses that the processing may exceptionally be permissible within the limits of the consent given. Consequently, it must necessarily be obtained before the processing takes place.[88] Subsequent consent has no curative effect on unlawful data processing[89]; however, it can have an effect in the future and may lead to the data not having to be deleted and obtained again, as consent can be interpreted as a waiver of the right to deletion.[90]

41 In principle, consent does not have an expiration date.[91] However, the right to be forgotten from Article 17 (1) GDPR, according to which data must be deleted as soon as they are no longer required for the purposes for which they were collected, leads to a time limit.

III. Granularity and purpose limitation

42 According to Article 4 No. 11 and Article 6 (1) lit. a GDPR, consent must always be given for a specific case. This includes, for example, a specific data processing act as well as a concrete purpose.[92] This requirement follows from the fundamental right of protection of personal data in Article 8 CFR[93] and has now also been explicitly included in Article 5 lit. b GDPR as a general principle; the aim is to ensure that the data subject can monitor the scope of its declaration and that the controller has strict limits on the use of the personal data.[94] The purpose must

63; BGH MMR 2020, 609 para 34; Dirk Heckmann, Martin Scheurer, 'Datenschutzrecht' in Dirk Heckmann, Anne Paschke (eds), *jurisPK-Internetrecht* (7th edn, juris 2021) chapter 9 para 317.

84 BGH MMR 2020, 609 para 47; CJEU Case C-673/17 *Planet49* [2019] ECLI:EU:C:2019:801 para 52, 59 ff.; *Heckmann, Scheuer* (n 83) chapter 9, para 739.

85 Stemmer (n 76) DS-GVO Art. 7 para 86; Kühling, Buchner (n 76) Art. 7 para 58; Martin Eßer in Martin Eßer, Philipp Kramer, Kai von Lewinski (eds) 'Auernhammer DSGVO/BDSG', (7th edn, Carl Heymanns 2020), Art. 4 para 101.

86 Schulz (n 49) DS-GVO Art. 7 para 7; Stemmer (n 76) DS-GVO Art. 7 para 88; Kühling, Buchner (n 76) Art. 7 para 30.

87 Kühling, Buchner (n 76) Art. 7 para 30; Schulz (n 49) DS-GVO Art. 7 para 7; Albert Ingold, 'Art. 7 Bedingungen für die Einwilligung' in Gernot Sydow, Nikolaus Marsch (eds), *Europäische Datenschutzgrundverordnung* (3rd edn, Nomos 2022 para 17.

88 Ingold (n 87) Art. 7 para 17; Kühling, Buchner (n 76) Art. 7 para 30; Schulz (n 49) DS-GVO Art. 7 para 7.

89 Schulz (n 49) DS-GVO Art. 7 para 7; Dirk Heckmann, Anne Paschke, 'Art. 7', in Eugen Ehmann, Martin Selmayr (eds), *DS-GVO Kommentar* (C.H. Beck, 2nd edn 2018) para 44.

90 Heckmann, Paschke (n 89) para 44.

91 Stemmer (n 76) DS-GVO Art. 7 para 88; Heckmann, Paschke (n 89) para 44; Kühling, Buchner (n 76) Art. 7 para 30.

92 EDPB, 'Guidelines 05/2020 on consent under Regulation 2016/679 adopted on 4th of May 2020' (2020) 12 ff.; Stemmer (n 76) DS-GVO Art. 7 para. 77; Kühling, Buchner (n 76) Art. 7 para 61.

93 Jan Henrik Klement, 'Art. 7 DS-GVO Bedingungen für die Einwilligung' in Spiros Simitis, Gerrit Hornung, Indra Spiecker gen. Döhmann (eds), *Datenschutzrecht* (1st edn, Nomos 2019) paras 18 f.; Kühling, Buchner (n 76) Art. 7 para 61.

94 Stemmer (n 76) DS-GVO Art. 7 para 77; Heckmann, Paschke (n 89) Art. 7 para 63; Heinrich Amadeus Wolff, in Peter Schantz, Heinrich Amadeus Wolff (eds), *Das neue Datenschutzrecht* (1st edn, Nomos 2017) para 527; Winfried Veil, 'Einwilligung

be as precise as possible in order to protect the data subject from a gradual expansion or blurring of the purposes[95]; there should be no processing for purposes which the data subject did not expect and/or could not have expected at the time of the consent.[96] The granularity is closely linked to the criteria of voluntariness and informativeness. Recital 43 indicates that voluntariness is not given if the controller does not allow the data subject to give separate consent to different processing operations, although this would have been appropriate in the relevant case. If the processing fulfils several purposes, comprehensive information must be provided and separate consent must be obtained for each of these purposes, cf. Recital 32 GDPR. In practical terms, this means that a global or blank consent is generally not possible.[97] However, this does not preclude consent from being given for several purposes at the same time, provided that these purposes are specified and conclusively described; this already follows from the wording of Article 6 (1) lit a GDPR. However, the requirement for specificity reaches its limits where comprehensive specificity would unreasonably impair comprehensibility. In this case, the user would no longer have any actual knowledge due to the abundance of information and could therefore not make a genuine and informed decision.[98] Moreover, it should be noted that consent may also relate to several processing acts if they are subject to the same processing purpose. According to Recital 32, obtaining consent for each individual processing step is therefore not necessary and should be avoided due to the aforementioned lack of clarity.[99]

IV. Voluntariness

43 According to Article 4 No. 11 GDPR, consent requires a freely given indication of intent. The principle of voluntariness is one of the core elements of data protection law and can already be derived from Article 8 CFR.[100] However, there is no legal definition of the term voluntariness. Recital 42 at least specifies that the data subject should have a "genuine or free choice" and must therefore be able to refuse or withdraw consent without any detriment. In this regard, the EDPB defines the term "free" as a "real choice and control for data subjects".[101] This clarifies that consent may not be obtained by coercion and that there must be freedom of choice on the part of the person concerned. There is consensus insofar as that coercion is given when criminally relevant conduct is undertaken.[102] Otherwise, the formula requires further concretization, especially since not every interference with the will of the person concerned impairs their freedom of decision to such an extent that a lack of voluntariness must be assumed[103]; nor can every minor interference negate this freedom. Instead, it must have a certain relevance.[104]

44 Recital 43 of the GDPR explains in more detail that consent is not to be considered voluntary if there is a clear imbalance between the data subject and the controller, with public authorities being cited as an example of such an 'overbearing' counterpart.[105] However, such a relationship of subordination does not always lead to involuntariness but serves as an indicator.[106] In practice, there must always be

oder berechtigtes Interesse? – Datenverarbeitung zwischen Skylla und Charybdis' [2018] NJW 3337 (3340).

95 EDPB (n 92) 16; Ernst (n 15) para 78; Marcus Helfrich, in Thomas Hoeren, Ulrich Sieber, Bernd Holznagel (eds), *Handbuch Multimediarecht* (58th edn, C.H. Beck March 2022) Part 16.1 para 58.

96 Kühling, Buchner (n 76) Art. 7 para 61; Klement (n 93) Art. 7 para 69.

97 Klement (n 93) Art. 7 paras 69 f.; Stemmer (n 76) DS-GVO Art. 7 para 79; Frenzel (n 49) Art. 7 para 8.

98 Kühling, Buchner (n 76)Art. 7 para 65; Arning, Rothkegel (n 15) DS-GVO Art. 4 paras 273 f.; Stemmer (n 76) DS-GVO Art. 7 paras 77 f.

99 Elke Sassenberg, 'Datenschutz in Schule und Schulverwaltung' in Louisa Specht, Reto Mantz (eds), Handbuch Europäisches und deutsches Datenschutzrecht (1st edn, C.H. Beck 2019) Sec.24 para 39.

100 Heckmann, Paschke (n 89) Art. 7 para 48; Kühling, Buchner (n 76) Art. 7 para 41; Stemmer (n 76) DS-GVO Art. 7 para 42.

101 EDPB (n 92) para 13.

102 EDPB (n 92) para 24; Ingold (n 87) Art. 7 para 27; Martin Franzen, 'Art. 7 DS-GVO' in Martin Franzen, Inken Gallner, Hartmut Oetker (eds), *Kommentar zum europäischen Arbeitsrecht* (4th edn, C.H. Beck 2022) para 8; Stemmer (n 76)DS-GVO Art. 7 para 39; Heckmann, Paschke (n 89) Art. 7 para 53.

103 Stemmer (n 76), DS-GVO Art. 7 para 40.

104 EDPB (n 92) para 24; Schulz (n 49) DS-GVO Art. 7 para 29 even demands serious detriments; Lukas Ströbel, Tim Wybitul, 'Beschäftigtendatenschutz' in Louisa Specht, Reto Mantz (eds), Handbuch Europäisches und deutsches Datenschutzrecht (1st edn, C.H. Beck 2019) Sec. 10 para 61; Klement (n 93) Art. 7 para 48.

105 EDPB (n 92) para 16; Kühling, Buchner (n 76) Art. 7 para 44; Stemmer (n 76) DS-GVO Art. 7 para 53.

106 According to EDPB (n 92) para 21, an employment context provides for another use-case in this regard. The EDPB as-

a case-by-case assessment.[107] On the other hand, voluntariness can also be impaired in the case of less severe imbalances: for example, in the case of contracts between a trader and a consumer[108], or in the case of a monopolistic position of the responsible party.[109] However, the mere asymmetry of power alone is not sufficient; only when the affected party is also deprived of the possibility to determine whether and how the data processing takes place in the specific situation, the voluntariness of the declaration of consent is to be denied.[110] When assessing the case, especially the type and the availability of the service must be taken into account: in the area of necessities, a situation of coercion is more likely to be assumed than in the case of luxury goods.[111]

45 The requirements for voluntariness are furthermore determined by the *coupling prohibition* principle as laid down in Article 7 GDPR. A coupling exists if the conclusion of a contract or the provision of a service is made dependent on the consent of the data subject to a further collection or processing of its personal data that is not necessary for the processing of the transaction.[112] The prohibition is intended to protect the free and independent expression of the individual's will when giving consent and to prevent situations where a de facto compulsion to consent to the use of data arises.[113] However, the question regarding the scope of the coupling prohibition emerges. Considering the wording of the enacting terms of the GDPR, there would initially be many arguments against describing consent as a "return" for a gratuitous service as being given involuntarily.[114]

46 The scope of this coupling prohibition is therefore controversial. While Article 7(4) GDPR suggests through its wording that the coupling should only be strongly considered within an assessment of voluntariness, Recital 43 GDPR provides for a stricter approach. The Supreme Court of Austria had to deal with this question and concluded—unconvincingly—from the discrepancy between the wording of the provision and the recital that there is basically a presumption of involuntariness unless special circumstances speak in favour of voluntariness. In the view of the court, this was so obvious that there was no need to refer the matter to the CJEU.[115] The supervisory authorities also initially tended towards an absolute coupling prohibition.[116]

47 The literature, on the other hand, advocates for a relative coupling prohibition, i.e., that not every combination of consent and processing of data for an unrelated purpose leads to involuntariness, but instead a case-by-case assessment must always take place, whereby this circumstance of the coupling must particularly be taken into account.[117] A decision by the Higher Regional Court of Frankfurt follows this argumentative pattern, stating that coupling the granting of consent with an unrelated participation in a lottery does not lead to the consent given to be involuntary.[118] The relative approach is further supported by the fact that the principle of voluntariness prevailing in data protection law is a consequence of the principle of private autonomy—an absolute coupling prohibition, on the other hand, would lead to personal data being

sesses the consent given by an employee as being "problematic"; cf. also Art. 29 Data Protection Working Party, 'Opinion 02/2017 on data processing at work' WP 249, p. 23.

107 EDPB (n 92) paras 17 f.; Ingold (n 87) Art. 7 para 28.

108 Kühling, Buchner (n 76) Art. 7 para 44; Heckmann, Paschke (n 89) Art. 7 para 52; Isabell Conrad, Christina Treeger, '§ 34 Recht des Datenschutzes' in Astrid Auer-Reinsdorff, Isabell Conrad (eds), *Handbuch IT- und Datenschutzrecht* (3rd edn, C.H. Beck 2019) para 471; Different view Heinrich Amadeus Wolff, in Peter Schantz, Heinrich Amadeus Wolff (eds), *Das neue Datenschutzrecht* (1st edn, Nomos 2017) para 512.

109 Buchner (n 16) 158; Kai-Uwe Plath, 'Art. 7 Bedingungen für die Einwilligung' in Kai-Uwe Plath (ed), *DSGVO/BDSG* (3rd edn, Verlag Otto Schmidt 2018) para 19; Heckmann, Paschke (n 89) Art. 7 para 52.

110 Kühling, Buchner (n 76) Art. 7 para 44; Frenzel (n 49) Art. 7 para 18; Ingold (n 87) Art. 7 para 28.

111 (n 87) Art. 7 para 27; In this direction probably Frenzel (n 49) Art. 7 para 18.

112 EDPB (n 92) paras 14 f.; Heckmann, Paschke (n 89) Art. 7 para 94; Jan-Christoph Thode, ' in Uwe Schläger, Jan-Christoph Thode (eds), *Handbuch Datenschutz und IT-Sicherheit* (1st edn, Erich Schmidt Verlag 2018) chapter 2 para 88.

113 EDPB (n 92) paras 26 f.; Heckmann, Paschke (n 89) Art. 7 para 94; Specht-Riemschneider (n 37) Sec. 9 para 27.

114 CF. in this regard example 6a EDPB (n 92) paras 40.

115 Austrian Highest Court (OGH), Decision of 31 August 2018 – 6 Ob 140/18h [2019] ZD 72 para 46.

116 DSK, 'Kurzpapier No 20 - Einwilligung nach der DSGVO', 1; Benedikt Buchner, 'Die Einwilligung in Werbung' [2018] WRP 1283 (1286); Already distancing from such an absolute interpretation EDPB (n 92) para 35.

117 Schulz (n 49) DS-GVO Art. 7 para 26; Taeger (n 50) DS-GVO Art. 7 para 90; Plath (n 109) Art. 7 para 19.

118 Higher Regional Court Frankfurt a.M., Decision of 27 June 2019 – 6 U 6/19 [2019] ZD 507 para 12.

protected even against the expressly declared will of the data subject.[119] The sovereignty of the individual over its data, which is anchored in the Charter of Fundamental Rights, as well as the right to voluntarily disclose one's own personal data would be undermined in an intolerable manner.[120] Such an understanding would mean a disproportionate restriction of (informational) private autonomy and is consequently not in conformity with the Charter of Fundamental Rights.[121] Moreover, it is also the declared aim of the GDPR to strengthen both the personal rights of the individual and the digital single market.[122] However, an absolute coupling prohibition would represent a very strong impact on the freedom to choose an occupation and right to engage in work of data controllers (which is also protected in Article 15 CFR)[123] and, above all, would also make the "*data in return*" business model practically impossible. The fact that this cannot be the intention of the European legislator is also shown in the new Digital Content Directive.[124] In this regard, Article 3 (1) Digital Content Directive stipulates that data can also be used as a currency to "pay" for digital content. The scope of application of the directive would be reduced to zero if it were assumed that any link between data and contractual performance is excluded.[125] A connection between data and contractual performance is therefore not ruled out. However, this raises the very practice-relevant question of when data processing cannot be based on Article 6 (1) lit. b GDPR, meaning that consent of the data subject must be obtained. It should thus always be carefully examined whether the use of the data is unnecessary in the sense of this norm. Above all, consent should not be obtained "as a precaution", since, in case of a revocation or invalidity of the consent, other grounds for permission cannot be used.[126]

48 First of all, it should be noted that the scope of application of consent and the scope of application of the statutory authorization do not overlap. If the data is necessary for the performance of the contract, consent is not required.[127] This can be the case, for example, if the user wants to have goods delivered to their home address, then the usage and processing of the data is necessary to fulfil the contractual obligation.[128] The crucial point is therefore the interpretation of the term "necessity" within the meaning of Article 6 (1) lit b GDPR. The EDPB advocates for a narrow interpretation. Accordingly, necessity only exists if the success of the contract would be endangered if the data could not be used.

49 Some authors argue that in order to make the business model "service for data" possible, the inter-

119 Heckmann, Paschke (n 89) Art. 7 para 95; Specht-Riemschneider (n 37) Sec. 9 para 28; Schulz (n 49) DS-GVO Art. 7 para 27; Plath (n 109) Art. 7 para 19; Heinrich Amadeus Wolff, in Peter Schantz, Heinrich Amadeus Wolff (eds), *Das neue Datenschutzrecht* (1st edn, Nomos 2017) para 515; Probably also Schmitz (n 30), part 16.2 para 280.

120 Heckmann, Paschke (n 89) Art. 7 para 95; with regard to the Basic Law for the FRG Klement (n 93) Art. 7 para 59.

121 Heckmann, Paschke (n 89) Art. 7 para 95; Veil (n 94) 3340; Specht-Riemschneider (n 37) Sec. 9 para 28; Björn Steinrötter, 'DSGVO Art. 7' in Georg Borges, Marc Hiller (eds), *BeckOK IT-Recht* (7th edn, C.H. Beck 1.7.2021) Art. 7 para 34.

122 Cf. recital 2 sentence 2 GDPR.

123 Schulz (n 49) DS-GVO Art. 7 para 27.

124 Directive (EU) 2019/770 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 (Text with EEA relevance.), OJ L 136, 22.5.2019, 1 ff.

125 Heckmann, Paschke (n 89) Art. 7 para 95.

126 EDPB (n 92) paras 121 ff.; DSK (n 116) 3; Philip Uecker, 'Die Einwilligung im Datenschutzrecht und ihre Alternativen' [2019] ZD248 (249); Marie-Theres Tinnefeld, Isabell Conrad, 'Die selbstbestimmte Einwilligung im europäischen Recht' [2018] ZD391 (392); Malte Engeler, 'Das überschätzte Kopplungsverbot' [2018] ZD 55 (58); Admissible at most if there was information about the other legal basis: Kühling, Buchner (n 76) Art. 7 para 16 ff.; Peter Schantz, 'Art. 5 DS-GVO' in Heinrich Amadeus Wolff, Stefan brink (eds), *BeckOK DatenschutzR* (41th edn, C.H. Beck 01.08.2022) para 8; Heckmann, Paschke (n 89) Art. 7 para 20; Heberlein (n 50) Art. 6 para 7; Heckmann, Scheurer (n 83) chapter 9 para 354; different view Veil (94) 3342; Philip Hacker, 'Daten als Gegenleistung: Rechtsgeschäfte im Spannungsfeld von DS-GVO und allgemeinem Vertragsrecht' [2019] ZfPW 148 (160); Jonas Brinkmann, 'Sec. 307 Datenschutzklausel' in Beate Gsell, Wolfgang Krüger, Stephan Lorenz, Christoph Reymnn (eds), *beck-online.GROSSKOMMENTAR BGB* (7th edn., C.H. Beck 15.1.2022) paras 21 ff.; Philipp Kramer, ´Art. 6 DSGVO´ in Martin Eßer, Philipp Kramer, Kai von Lewinski (eds), *DSGVO BDSG*(7th edn, Carl Heymann 2020) para 23; Schulz (n 49) DS-GVO Art. 6 para 11; Frenzel (n 49) Art. 6 para 8, Art. 7 para 17a; Cf. also in this direction for the BDSG: BGH NJW 2008, 3055 para 43; Higher Regional Court (OLG) Frankfurt a.M. BeckRS 2005, 11716 para 29.

127 EDPB (n 92) para 32.

128 EDPB (n 92) para 24; EDPB, 'Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects' (Version 2.0, 8 October 2019) para 30; Frenzel (n 49) Art. 7 para 11.

pretation should be less restrictive.[129] In addition, according to the Digital Content Directive, such contracts should be possible, but these would generally fail due to the coupling prohibition if the necessity were to be interpreted in the sense of *indispensability*. However, considering the new European digital strategy, data should be able to be used as a valuable counterpart.[130] "*Data trading*" should be possible, but at the same time the undermining of the protective function of the GDPR must also be avoided; this can only be achieved by ensuring that only those business models whose essence is an "exchange for data" can be justified on the legal grounds of Article 6 (1) lit b GDPR. To prevent circumvention of a possible consent requirement, the definition of the content of the contract "data exchange" cannot be determined subjectively and unilaterally by the controller.[131] This can be ensured by reviewing the content of the general terms and conditions. However, the scope of application of the general terms and conditions is only opened if it is a secondary agreement and not the main performance obligation. For the delimitation, it depends primarily on what the parties have agreed. Above all, however, it depends on how the offer of the processor appears from the perspective of an objective recipient; if it is a typical performance-versus-data contract and this is made transparent, the transfer of the data can be the main purpose.

50 If, on the other hand, it is a different type of contract, the purpose of which is in particular the transmission of information or communication, and the processor attempts to expand this purpose in a non-transparent manner using an additional clause to include the provision of data, this may be subject to content review according to Section 307 (1) BGB. This will often lead to the clause being invalid because it contradicts the basic idea of the statutory regulations.[132] In addition, such agreements may also violate the transparency requirement or constitute a surprising clause within the meaning of Section 305c BGB.[133]

51 All in all, an absolute coupling prohibition should be rejected for the reasons just mentioned. The GDPR only imposes a relative prohibition of coupling; data exchange transactions, as provided for in the Digital Content Directive, are principally possible. However, the justification or the legal ground for justification always depends on the specific contractual performance. If the data exchange is the main purpose, then the necessity in the sense of Article 6 (1) lit b GDPR can be affirmed; however, this cannot be determined unilaterally by the potential processor, otherwise they would have the power to let the scope of consent lapse.[134] For the determination, it should be examined in each individual case, whether a bilateral contractual relationship exists between the processor and the data subject, whereby the decisive factor is if the data subject also receives a service or is granted benefits and does not only have to disclose its personal data without a real countervalue.[135]

52 Particularly in light of the Digital Content Directive, it seems very likely that new contract models will soon emerge in which the provision of data is offset by real value.[136] In all other cases, such agreements must be measured against Article 7 (4) GDPR and must also withstand a content review, which regularly leads to the invalidity of so-called "*take it or leave it*" offers with a unilateral definition of the purpose of the contract.[137] However, offers where the data subject is offered a real alternative to paying for the service with other monetary means instead of data may also be compatible with Article 7 (4) GDPR.[138] This is because there is freedom of choice between "payment" with the data by granting consent or the data-protecting alternative of rejecting the cookies and instead paying the equivalent

129 Heckmann, Paschke (n 89) Art. 7 para 96; Schulz (n 49) DS-GVO Art. 7 para 30; The Bavarian data protection supervisory authority also advocated that such arrangements should not be permitted as a result of the coupling prohibition, but should be justified on the basis of article 6 (1) (b) of the GDPR if the situation is presented to the user in a clear and comprehensible manner and the user has a factual basis for his or her decision: Bavarian state office for data protection supervision (BayLDA), TB 2017/2018, p. 72.

130 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'A European strategy for data' (COM/2020/66 final) 4 f.

131 Kühling, Buchner (n 76) Art. 6 para 40a; Specht-Riemschneider (n 37) Sec. 9 para 49.

132 BGH NJW 2013, 291 para 28; Brinkmann (n 126) para 17; Wolfgang Wurmnest, ´§ 307 Inhaltskontrolle´ in Franz Jürgen Säcker, Roland Rixecker, Hartmut Oetker (eds), Münchener Kommentar zum BGB (9th edn, C.H. Beck 2022) para 71.

133 Taeger (n 50) DS-GVO Art. 7 para 44.

134 Kühling, Buchner (n 76) Art. 7 para 51.

135 Alexander Golland, ´Das Kopplungsverbot in der Datenschutz-Grundverordnung´ [2018] MMR, 130 (132).

136 Kühling, Buchner (n 76) Art. 7 para 51 also assume this development.

137 Also: Alexander Golland, ´Das Kopplungsverbot in der Datenschutz-Grundverordnung´ [2018] MMR 130

138 EDPB (n 128) para 37.

value of the data with monetary means. In addition to these basic explanations, it should be noted that a disproportionately high price can again call the voluntary nature into question.[139]

V. Informed consent

53 Pursuant to Article 4 No. 11 GDPR, consent must be given in an informed manner to be effective. Once again, the aim is to ensure that the data subject can assess the impact of giving consent and that the data subject can clearly and unambiguously understand the circumstances of the data processing and the scope of their consent.[140] The GDPR itself does not exhaustively specify the minimum content that should be provided by the processor; a guiding framework, however, can be found in Articles 13 and 14 GDPR, which has been further specified by the EDPB to the effect that the following minimum information should be included: the identity of the controller, the purpose of each processing act, the type of data collected, the possibility of withdrawal, if applicable, information on the use of the data for automated decision-making according to Article 22 (2) lit. c GDPR and a notice on possible processing risks in the case of third country transfers pursuant to Article 49 GDPR.[141] In addition, the CJEU recently ruled that it is also necessary to provide information on whether third parties have access to the information and on the duration of cookies.[142] The latter seems particularly important regarding *persistent cookies*, which can—in contrast to *session cookies*—remain in place for years. It is important to emphasize that the provisions of Articles 13 and 14 GDPR are not conditions for the legal effectiveness of consent[143]; the enacting terms of the GDPR merely state that consent must be given in an informed manner (cf. Article 4 No 11). Articles 13 and 14 GDPR provide a framework for this, but the absence of certain information listed in these provisions does not result in the consent being legally ineffective.[144] This is supported not only by the fact that these standards are not in the enacting terms of the GDPR but also by the considerations in Recital 42, according to which informed consent is given if the data subject at least knows the identity of the controller and the purposes of the processing for which the personal data are intended.[145] However, the information specified by the EDPB and the CJEU should be provided in any case, because otherwise, it seems—especially regarding Recital 42—questionable whether the user can form a comprehensive understanding of the scope of his or her declaration.

54 Also, concerning the "how" of providing information, the GDPR does not make entirely clear statements. However, Recital 42 states that pre-formulated declarations (such as those in cookie banners) must be provided in an understandable and easily accessible form in clear and simple language, which is supplemented by Recital 32 with the requirement that, in addition to a clear and concise form, there should also be no unnecessary interruptions to the service. Consequently, the declaration of consent should be kept as short and precise as possible[146] and it must be written in a language that the data subject can understand, meaning that the common national language has to be chosen. Besides, the use of unnecessary technical vocabulary should also be avoided.[147] The complexity of the declaration by oversized, overlong banners or cookie banners and new information appearing in a variety of new tabs should be avoided.[148] Of course, the declaration as a

139 With regard to the appropriate price, no general statements can be made; this depends on various circumstances such as the scope, type and exclusivity of the "lost" data, in detail to different criteria: Golland, (n 135) 130 (134 f.).

140 Heckmann, Paschke (n 89) Art. 7 para 57; Kühling, Buchner (n 76) Art. 7 para 59; Arning, Rothkegel (n 15) DS-GVO Art. 4 para 277; Veil (n 94) 3339.

141 EDPB (n 92) para 72; A slightly smaller circle is drawn by: Flemming Moos, Tobias Rothkegel, ´Anm. Zu EuGH, Setzen von Cookies erfordert aktive Einwilligung des Internetnutzers – Planet49´ [2019] MMR 732 (739) who usually consider it sufficient to provide information about the controller, the purposes of the processing and the revocability but not about the data types.

142 Case C-673/17 *Planet49* [2019] ECLI:EU:C:2019:801 paras 75 f.

143 EDPB (n 92) para 72; Philipp Albrecht, Florian Jotzo, *Das neue Datenschutzrecht der EU* (Nomos 2017) Part 3 para 41; Schulz (n 49) DS-GVO Art. 7 para 36; Arning, Rothkegel (n 15) DS-GVO Art. 4 para 278; Stemmer (n 76) para 99

144 Schulz (n 49) DS-GVO Art. 7 para 36; Arning, Rothkegel (n 15) para 278; Philipp Albrecht, Florian Jotzo, *Das neue Datenschutzrecht der EU* (Nomos 2017)Part 3 para 41, Part 4 para 8; Kühling, Buchner (n 76) Art. 7 para 59.

145 Also of this opinion: Moos, Rothkegel (n 141) 739.

146 Heckmann, Paschke (n 89) Art. 7 para 42; Ingold (n 87) Art. 7 para 36.

147 Kühling, Buchner (n 76) Art. 7 para 60; Ernst (n 15) Art. 4 para 83; Stemmer (n 76) DS-GVO Art. 7 para 66.

148 Ernst (n 15) Art. 4 para 79 f.; Kühling, Buchner (n 76) Art. 7 para 60; Heinrich Amadeus Wolff, in Peter Schantz, Heinrich Amadeus Wolff (eds), *Das neue Datenschutzrecht* (1st edn, Nomos 2017) para 524.

whole must be legible[149]; it would not be sufficient to write the decisive information in minuscule font size.

55 The requirement to provide sufficient information is closely linked to the transparency requirement arising from Article 7 (2) GDPR: all decisive information should be disclosed to the data subject in a reasonable manner. To meet the need for completeness and transparency on the one hand and simplicity and conciseness on the other, a multi-layer system seems appropriate.[150] On the first level, the minimum content described above should be presented in a concise form, and on another level, the remaining information pursuant to Articles 13 and 14 GDPR, as well as more detailed explanations, if necessary, should be provided.[151] If the decision is made to present more than the required minimum information on the first layer, the minimum content should be highlighted by size, shape, or colour to enable quick and complete comprehension of the most important information.[152] Neither the CJEU nor the German Federal Court have commented precisely on this, but at least in their view, a multi-level system does not seem to be inadmissible per se.[153] Furthermore, it should be noted that pursuant to recital 42 pre-formulated declarations of consent are subject to the control of general terms and conditions according to Directive 93/13/EEC. As a result, pre-formulated declarations of consent may be void, if, for instance, unfair clauses are used.

VI. Excursus: information obligations for consent-free cookies

56 Articles 13 and 14 GDPR set out extensive information obligations that the respective controller must fulfill when collecting personal data. From Article 13 GDPR (in case of direct collection) and Article 14 GDPR (in case of third party collection) respectively, arises an information obligation that the controller has to fulfill towards the data subject when collecting personal data.[154] The information obligation exists regardless of the legitimacy of the processing according to Articles 6 or 9 GDPR, even if the processing is carried out lawfully, the data subject has a right to know whether and which personal data are being collected, since only then the data subject's rights pursuant to Article 15ff. GDPR can be exercised adequately.[155] Furthermore, according to Recital 60 of the GDPR, the principle of fair and transparent processing requires that the data subject is always informed about the existence of the processing operation and its purpose. This means that, unless one of the exceptions listed in Articles 13 (4) and 14 (5) GDPR applies, the obligation exists and is abstract from other information obligations, in particular from the requirement of informed consent pursuant to Article 4 No. 11 GDPR. It is important to emphasize that the provisions of Articles 13 and 14 GDPR are not conditions for the legal effectiveness of consent; the enacting terms of the GDPR merely state that consent must be given in an informed manner (cf. Article 4 No 11 GDPR). Articles 13 and 14 GDPR provide a framework for this, but the absence of certain information listed in these provisions does not result in the consent being legally ineffective. Thus, a breach of the information requirements under Article 13f. GDPR can result in a fine under Article 83 (5) lit b GDPR, but does not affect the lawfulness of the processing; a lack of informed consent "only" results in the unlawfulness of the processing.

57 This means that if only consent-free cookies are set, solely the information requirements of Article 12ff. GDPR apply. The GDPR itself does not define the format or the specific way in which the information set out in Articles 13 and 14 GDPR must be provided. However, it follows from Article 12 (1) GDPR that

149 Kühling, Buchner (n 76) Art. 7 para 60; also in this direction Heinrich Amadeus Wolff, in Peter Schantz, Heinrich Amadeus Wolff (eds), *Das neue Datenschutzrecht* (1st edn, Nomos 2017) para 524; Different opinion Stefan Ernst, ´Die Einwilligung nach der Datenschutzgrundverordnung´ [2017] ZD 110 (113).

150 EDPB (n 92) para 69; Kühling, Buchner (n 76) Art. 7 para 59; Schulz (n 49) DS-GVO Art. 7 para 47; Stemmer (n 76)Art. 7 para 57; Klement (n 93) Art. 7 para 74.

151 Also in this direction: Schulz (n 49) DS-GVO Art. 7 para 47.

152 EDPB (n 92) para 71; Heckmann, Paschke (n 89) Art. 7 para 42; Also to distinguish from other declarations Schmitz (n 30) para 275.

153 This rather unsatisfactory result for the practice is also reached by: Böhm, Halim (n 38) 655; different view Maren Pollmann, Dennis-Kenji Kipker, ´Informierte Einwilligung in der Online Welt´ [2016] DuD 378 (379).

154 Alexandra Mester, 'Art. 13, 14 DS-GVO' in Jürgen Taeger, Detlev Gabel (eds), *DSGVO – BDSG – TTDSG* (R&V, 4th edn 2022) Art. 13 para 4, Art. 14 para 5; Matthias Bäcker, 'Art. 13, 14', in Jürgen Kühling, Benedikt Buchner (eds), *Datenschutz-Grundverordnung BDSG Kommentar* (3rd edn, C.H. Beck 2020) Art. 13 para 12; Art. 14 para 9.

155 Rainer Knyrim, 'Art. 13'13 f.', in Eugen Ehmann, Martin Selmayr (eds), *Datenschutz-Grundverordnung Kommentar* (2nd edn, C.H. Beck 2018) Art. 13 para 1, Art. 14 para 1; Mester (n 154) Art. 13 para 1, Art. 14 para 2.

the controller has to take appropriate measures to provide the information to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language. According to Article 12 (7) GDPR the information may be provided in combination with standardized icons to give in an easily visible, intelligible, and clearly legible manner a meaningful overview of the intended processing. Although Article 12 ff GDPR do not prescribe a specific form, the Article 29 Working Party is of the opinion that the controller has to take into account all the circumstances of the data collection and processing when deciding on the appropriate manner and form of provision.[156] Furthermore:

> *"In particular, appropriate measures will need to be assessed in light of the product/service user experience. This means taking account of the device used (if applicable), the nature of the user interfaces/ interactions with the data controller (the user "journey") and the limitations that those factors entail."*[157]

58 Nevertheless, the data controllers are not completely free as to the choice of medium; in particular in the online context, a "*media discontinuity*"[158] would generally be inadmissible.[159] The required information should be available on the website of the data controller.[160] Since no concrete specifications are made, the design as a separate part of a website on which the information can be viewed in bundled form—i.e., the "*classic*" data privacy statement—is possible.[161] However, the controller must actively inform the data subjects and ensure that they can receive the information in a timely manner; this follows from the wording of Articles 13 (1) and 14 (1) GDPR, according to which the relevant information must be "*provided*".[162] It is not sufficient for the data controllers to make certain information available for retrieval only, for example in a general privacy statement on their website.[163] The user of the website should therefore be referred to the necessary information directly when visiting the website; this can be done, for example, by placing an HTML element with a forwarding link.[164]

59 Although the timing of the presentation of information is not explicitly defined in Article 12 ff GDPR, the wording "at the time of data collection" in Article 12 (1) GDPR does not indicate whether the information must be shown during or before the data collection. It follows, at least from the purpose of the information obligations, that they must be fulfilled immediately before the start of data collection.[165] In the case of third-party collection in the sense of Article 14 GDPR, the responsible party must provide the information within a reasonable period of time after receipt of the data, but no later than one month, Article 14 (3) GDPR.

60 Since the information should be clear and understandable for the reader, the Article 29 Data Protection Working Party also proposes other forms of design than the classic data privacy statement in order to prevent information fatigue. These include, on the one hand, a layered approach and, on the other hand, *push* or *pull* notices. The Article 29 Working Party states that:

> *"In the digital context, in light of the volume of information which is required to be provided to the data subject, a layered approach may be followed by data controllers where they opt to use a combination of methods to ensure transparency. WP29 recommends in particular that layered privacy statements/notices should be used to link to the various categories of information which must be provided to the data subject, rather than displaying all such information in a single notice on the screen, in order to avoid information fatigue. Layered privacy statements/notices can help resolve the tension between completeness and understanding, notably by allowing users to navigate directly to the section of the statement/notice that they wish to read. It should be noted that layered privacy statements/notices are not merely nested pages that require several clicks to get to the relevant information. The design and layout of the first layer of the privacy statement/notice should be such that the data subject has a clear overview of the information available to them on the processing of their personal data and where/how they can find that detailed information within the layers of the privacy statement/notice."*[166]

156 Article 29 Working Party, 'Guidelines on transparency under Regulation 2016/679 last revised and adopted on 11th of April 2018', para 24.

157 Article 29 Working Party (n 156) para 24.

158 when the information is not provided in the form that is also used for data collection (e.g. electronically).

159 Mester (n 154) Art. 13 para 36.

160 Article 29 Working Party (n 156) para 17, 40.

161 Article 29 Working Party (n 156) para 24; Oliver Daum, ´Pflichtangaben auf Webseiten´ [2020] MMR 643 (645); critical in this regard Joerg Heidrich, Michael Koch, ´Die Nutzer im Netz zwischen Einfluss und Ohnmacht´ [2020] MMR 581 who see this as "*information overkill*".

162 Article 29 Working Party (n 156) para 33; Mester (n 154) Art. 13 para 36.

163 Bäcker (n 155) Art. 14 para 41; Bernd Lorenz, ´Datenschutzrechtliche Informationspflichten´ [2019] VuR 213 (220).

164 Article 29 Working Party (n 156) para 33.

165 Bäcker (n 155) Art. 13 para 56; detailed Article 29 Working Party (n 156) para 26.

166 Article 29 Working Party (n 156) para 35.

61 The Article 29 Working Party also presents a proposal on what information should be displayed and at what level:

> *"As regards the content of the first modality used by a controller to inform data subjects in a layered approach (in other words the primary way in which the controller first engages with a data subject), or the content of the first layer of a layered privacy statement/notice, WP29 recommends that the first layer/modality should include the details of the purposes of processing, the identity of controller and a description of the data subject's rights. (Furthermore this information should be directly brought to the attention of a data subject at the time of collection of the personal data e.g. displayed as a data subject fills in an online form.) The importance of providing this information upfront arises in particular from Recital 39.34 While controllers must be able to demonstrate accountability as to what further information they decide to prioritise, WP29's position is that, in line with the fairness principle, in addition to the information detailed above in this paragraph, the first layer/modality should also contain information on the processing which has the most impact on the data subject and processing which could surprise them. Therefore, the data subject should be able to understand from information contained in the first layer/ modality what the consequences of the processing in question will be for the data subject (see also above at paragraph 10)."*[167]

62 Instead of the multi-level approach, the Article 29 Working Party believes that the form of push or pull notices can also be useful. Push notices involve the provision of information "just-in-time"[168], while pull notices command access to information via tools such as a privacy dashboard.[169] None of these procedures are legally required, but to fulfil the information obligation from Article 13 or 14 GDPR, providers must always check whether the form they have chosen creates the necessary transparency, or whether it is more likely that a large part of the information will go unnoticed.[170]

63 Overall, the GDPR leaves a great degree of discretion to the controller with regard to the presentation of the information. However, this does not mean that it is sufficient to make all the information available for retrieval in an unstructured manner. It is the responsibility of the controller to take appropriate measures to ensure that the information is presented in a concise, transparent, intelligible, and easily accessible form. The controller must therefore always examine carefully whether the concretely chosen form of information provision does not contradict this objective.[171]

VII. Revocability

64 Article 7 (3) GDPR stipulates that consent is freely revocable. The controller must inform the data subject about this possibility and also has to ensure that the data subject can withdraw consent at any time. Withdrawal of consent must be as simple as its original granting. In particular, according to Article 7 (3) S. 4 GDPR the withdrawal of consent can be carried out in the same way as consent was given.

65 The GDPR does not impose any material, formal, or temporal requirements for revocation, in particular, no special form must be followed[172] and the controller must inform the data subject of this. The requirement that the revocation must be as simple as the consent leads to a reciprocal right of revocation. This means that if consent can be given electronically via a cookie banner by mouse click or keystroke, this must also apply to revocation.[173] Thus, consent given via a cookie banner cannot be made dependent on a revocation email or a call to a service centre, for example.[174] This would constitute an unreasonable effort and is not in line with the simplicity requirement.

66 However, it may be rather difficult to set up the appropriate revocation environment if the data subject has not created a user account so that the revocation option can be integrated into the user interface.[175] One possibility would be to set up a pop-up window when the user wants to close the website or app and scrolls with the mouse on the X-button, asking whether the consent should be

167 Article 29 Working Party (n 156) para 36.

168 Article 29 Working Party (n 156) para 39, a just in time notice is described by the Article 29 Working Group as [a] *notice [which] is used to provide specific 'privacy information' in an ad hoc manner, as and when it is most relevant for the data subject to read.*

169 Article 29 Working Party (n 156) para 39.

170 Article 29 Working Party (n 156) para 34.

171 For the question of which information must be provided in accordance with Art. 13 and 14 GDPR, see the overview: Article 29 Working Party (n 156) 35 ff.

172 Heckmann, Paschke (n 89) Art. 7 para 91; Stemmer (n 76) DS-GVO Art. 7 para 95; Kramer (n 126) Art. 7 para 39.

173 EDPB (n 92) para 114Kramer (n 126) Art. 7 para 40; Uwe Schläger, ´Einwilligung´ in Schläger/ Jan Christoph Thode (ed), Handbuch Datenschutz und IT-Sicherheit (1st edn, Erich Schmidt 2018) para 90.

174 LfDI BaWü, 'FAQ Cookies und Tracking durch Betreiber von Webseiten und Hersteller von Smartphone-Apps' (Version 2.0 März 2022) 27.

175 Also remarked by Heckmann, Paschke (n 89) Art. 7 para 91.

revoked and set the corresponding tick boxes there, which the user can simply click on.[176]

F. Design of a Cookie Banner

67 There are several regulations that have to be followed, yet, there is still a spectrum of design options. It should be noted, however, that the design to be chosen on the spectrum should not only be legal but also adequately designed from the perspective of behavioural science. This is because designs that have been proven to lead to users being confused, fatigued, or even deceived and therefore lead to suboptimal behaviour[177] can also call into question the active and informed consent and/or voluntariness of consent from a legal perspective. Manipulative design methods should be refrained from; the choice ends where misbehaviour is deliberately challenged.

I. Placement, Visibility and Accessibility

68 To give the user a sufficient choice to start with, the banner must be presented in a suitable place, at a suitable time, and in a suitable colour.

69 For this purpose, the cookies banner should appear directly when the website or application is opened and not at a later time.[178] This procedure is necessary, on the one hand, to enable actual consent prior to processing. On the other hand, however, it also avoids that the user first contractually commits themselves on the website and then only being shown the consent at the end of an order process.

70 A design in which no cookie banner appears when the website is visited, but only when the user calls up a specific product should be avoided. In this case, the user's propensity to buy is exploited. Behavioural science studies have shown that shoppers are more likely to give their consent when they are already far along in the shopping process, to avoid having to search for alternative products.[179] To enable users to make a truly voluntary decision, they should be given the opportunity to do so before any interaction on the website.

71 In addition, the cookie banner should be placed in a way that it is clearly visible when the page is called up; this can best be achieved with a separate pop-up element, making the cookie banner stand out from the rest of the website. The banner should have colour highlighting at the bottom or top of the website. The consent element should not merge with the page and disappear when scrolling. The user should be given the opportunity to engage with the relevant data protection provisions; this is impaired if the corresponding banner has already disappeared after a single scroll.

72 Furthermore, a colour scheme should be chosen that does not unnecessarily complicate the absorption of information, therefore colours that are comfortable for the eyes should be used.

II. Mandatory information

73 In order to enable the user to give informed consent under the GDPR, the following information must already be included at the first level of the cookie banner:

- the identity of the controller,
- the purpose of each processing act,
- the type of data collected,
- the duration of the data usage
- the possibility of withdrawal,
- if applicable, information on the use of the data for automated decision-making pursuant to Article 22 (2) lit c GDPR, and
- a notice on possible processing risks in the case of third-country transfers pursuant to Article 49 GDPR.

74 To ensure that consumers actually read and process the information completely, a short text with short and easy-to-understand sentences should be chosen. With increasing complexity, which is reinforced by the use of legal language or very technical terms, for example, the level of understanding decreases.[180]

176 Heckmann, Paschke (n 89) Art. 7 para 91 and Georg Schröder, *Datenschutzrecht für die Praxis* (4th edn, dfv 2021) 154 suggests setting a checkbox on the data protection declaration next to the place where consent was given.

177 Detailed on this: CNIL, 'IP Report No 6: Shaping Choices in the Digital World' (2019) 27 <https://linc.cnil.fr/sites/default/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf> accessed 10 December 2022.

178 Also DSK (n 53) 9.

179 Sara Elisa Kettner, Christian Thorun, Max *Vetter*, 'Wege zur besseren Informiertheit: Verhaltenswissenschaftliche Ergebnisse zur Wirksamkeit des One-Pager-Ansatzes und weiterer Lösungsansätze im Datenschutz' (Con Policy, 28.02.2018) <https://www.conpolicy.de/data/user_upload/Studien/Bericht_ConPolicy_2018_02_Wege_zur_besseren_Informiertheit.pdf > accessed 10 December 2022.

180 In detail with further reference: Conpolicy, 'Abschlussbericht: Innovatives Datenschutz-Einwilligungsmanagement' (2020)

Despite the required conciseness, it must immediately be apparent to the user what they are consenting to, overview-like summaries such as "this site uses cookies to enhance your browsing experience" or "advertising analysis and marketing purposes" are not sufficient[181] because it is not clear which data should be processed for which purpose, so the data subject is not sufficiently informed.[182] Each purpose must be explained individually and specifically, if third-party services are integrated, these must be named individually, and the purposes of any partners must also be clearly and unambiguously listed. It is not sufficient to refer to the websites and/or privacy policies of the third parties for details of third-party cookies.[183] In order to achieve a sufficient degree of information, but also not overwhelm the user with information, a mixture of fixed text modules and drop-down elements or sidebar elements should be chosen. The 'fixed' text should explain what the consent is being requested for and how cookies work, as well as how and for what purposes they are used. If third-party providers are involved, they should also be listed directly. Above all, designs that induce the user to give consent as a result of a flood of information and that have pre-clicked purposes and third-party providers—requiring significant effort to deselect—are to be avoided.[184] In these cases, the required level of information is usually already lacking, as the information is prepared in an inappropriately complex manner, and active consent is also absent, as everything has already been pre-clicked. Transparent information should be available before consent is given, i.e., it must be possible to give granular consent already at the first level of the cookie banner and to obtain information about purposes and third-party providers and duration without detours. In particular, the frequently encountered "One-Click-Away" designs, in which only "accept all" "reject all" or "settings" can be selected at the first level and further information—especially on the purposes of processing—is only provided via the Settings selection, are not transparent because not all the necessary information is directly available.[185] However, it is possible to use an "accept all" and "reject all" button if further information and individual options for selecting and deselecting third-party providers are available at the same level.

75 Neither the legal requirements nor the courts and data protection authorities make strict statements on the question of whether all information should already be 'unfolded' on the first level. However, since clarity also plays a major role in the reception of information, the presentation of information about purposes, providers, and duration of use should be logically bundled in a drop-down menu or sidebar on the first level. This should be designed intuitively. The fold-out or expanding menu items should be easily recognizable as such; greying out or similar designs should be avoided, otherwise there is a lack of transparency since the information cannot be found.[186] There shouldn't be an excessive number of levels on which the user has the opportunity to make a decision only at the very last level, since the attention and receptiveness decreases with each level.[187] The user should not be overwhelmed with the necessary information, but it should also not be hidden.

76 According to Recital 32 of the GDPR, clear and simple language should be used for the information (this already applies to the headline of the banner). Which also means that the relevant information must be provided in the official language of the

part 2.1.2.2.1; The EDPB is therefore also against the use of such language: EDPB (n 92) para 67.

181 Also with this opinion: Landesbeauftragter für Datenschutz und Informationsfreiheit (LfDI) BaWü, FAQ Cookies und Tracking durch Betreiber von Webseiten und Hersteller von Smartphone-Apps, Version 2.0 März 2022 p. 19; LfDI Niedersachsen, 'Handreichung: Datenschutzkonforme Einwilligungen auf Webseiten – Anforderungen an Consent Layer' (November 2020) 3; this design was recently classified as Dark Pattern (Left in the Dark Pattern – type: ambiguous wording or information) by the EDPB cf. EDPB, 'Guidelines 3/2022 on Dark Patterns in social media platform interfaces: How to recognize and avoid them' (Version 1.0, 14 March 2022) para 67 f., detailed on more types of Dark patterns and on the term in general see below part F.6.

182 EDPB (n 181) para 68.

183 This design is classified as Dark Pattern by the EDPB (Hindering Pattern – type: Dead End), cf. EDPB (n 181) para 78 f.; already in 2014: Damien Clifford 'EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behaviour' [2014] JIPITEC 194 (199), but on the Data Protection Directive which was applicable until 2018.

184 EDPB (n 181) para 118 f. (Overloading Pattern- type: too many options).

185 The danish data protection authority also recently ruled in this way: Datatilsynet, Vejledning: Behandling af personoplysninger om hjemmesidebesøgende, 02.2022 <https://www.datatilsynet.dk/media/7784/vejledning-om-behandling-af-personoplysninger-om-hjemmesidebesoegende.pdf> accessed 10 December 2022.

186 This design is classified as Dark Pattern by the EDPB (Stirring Pattern – type: Hidden in Plain Sight), cf. EDPB (n 181) para 47 ff.

187 This design is classified as Dark Pattern by the EDPB (Overloading Pattern – type: Privacy Maze), cf. EDPB (n 181) para 47.

country concerned.[188] Despite the simple and clear language, the wording should not be so trivializing that the user is not even aware of what they are agreeing to or that they are giving legally effective consent at all. Formulations such as "A quick cookie and then onwards" should therefore be avoided for the consent button. The consent button should be labelled in a way that reflects its nature, and it should be clear what is meant by the button. A simple "okay, thank you" or "got it" will often not be sufficient, as it won't be clear whether the *okay* should only mean acknowledgement or active consent.

77 The information relevant to consent should be clearly separated from other information, so it should for example not be "buried" in the privacy policy. In addition, the Consent Banner should not be filled with contextless information that distracts from the actual consent process, e.g., cookie recipes or further links to cookies or cookie recipes, as this distracts the users from the actually relevant information and they will be more likely to click an "okay" button as they are not aware that they consent to data processing.[189]

78 To continue, other types of framing, in which the consent is set in a certain framework, can call the informed consent into question. Behavioural science studies have shown that consumers trust the judgment of "experts", so if a button is labelled "proceed with expert settings" or "proceed with recommended settings" instead of 'agree' or 'accept all', the consent rate can be increased[190]; however, these consents are not informed consents in the sense of the GDPR, as no information is provided about which operations and processing purposes are being consented to. Such labelling is therefore not sufficient according to the GDPR.

III. Active participation and defaults

79 As stated above, Recital 43 GDPR provides that consent is only deemed to have been given voluntarily if the data subject has a genuine or free choice and is therefore also able to refuse consent. Cookie banners where there is no choice at all, but only information about the use of cookies, are therefore generally inadmissible.[191]

80 The situation is similar if no rejection option is presented at the first level, but only via a "Learn more" link.[192] A mere notice about the processing, without decision options, is only sufficient if only consent-free cookies are set.

81 With the *Planet49* decision of the CJEU[193] and the subsequent BGH ruling[194], opt-out designs where consent is for all purposes pre-selected, and the user must opt-out are generally impermissible.[195] This was recently confirmed by the EDPB, as the *default effect* is exploited by such a design, which nudges users to keep a pre-selected option, they are unlikely to change this even if given the possibility.[196] The same applies if only some purposes are preselected since in this case there is no active consent on the part of the user. Only the necessary cookies may be permanently preselected as no consent is required for these.

82 The reverse design, on the other hand, in which all cookies and purposes are initially deselected complies with the requirement of voluntariness since the user must become active to consent to the processing. However, the consent process must not be unduly prolonged by requiring the user to review an interminable list of individual cookies and to select or deselect each one individually, without being given the opportunity to provide consent or rejection for all of them at once.[197]

188 LfDI BaWü (n 174) 24; if the information is presented only in another language, this constitutes a dark pattern according the EDPB (Left in the dark Pattern – type: language discontinuity), EDPB (n 181) para 69.

189 This design is classified as Dark Pattern by the EDPB (Skipping Pattern – type: Look over there), cf. EDPB (n 181) para 99 f.

190 Detailed on the *Expert frame* with further references: Conpolicy (n 180) part 2.1.2.2.2.

191 This is also the position of the DSK: DSK (n 53) 10.

192 This has also been confirmed by the CJEU: CJEU Case C-61/19 *Orange Romania* [2020] ECLI:EU:C:2020:901 para 52; and by national courts: Regional Court Cologne GRUR-Prax 2021, 385.

193 CJEU Case C-673/17 *Planet49* [2019] ECLI:EU:C:2019:801.

194 BGH m. Anm. Gierschmann, ´Verwendung personenbezogener Daten - Cookie Einwilligung II´ [2020] MMR 609.

195 in detail on the preceding decisions Agnieszka Jabtonowska and Adrianna Michatowicz, 'Planet49: Pre-Ticked Checkboxes Are Not Sufficient to Convey User's Consent to the Storage of Cookies' [2020] EDPL 137.

196 This design was also classified as Dark Pattern (Skipping Pattern – type: deceiptive snugness), EDPB (n 181) para 127.

197 EDPB (n 181) para 118 f. (Overloading Pattern - type: too many options).

IV. Revocability

83 According to Article 7 (3) GDPR, the revocation must be possible at any time and just as easy to implement as the consent. Thus, it would not be permissible to hide the revocation option somewhere in the privacy policy making it difficult to find. On the other hand, it will probably not be necessary to keep the cookies banner open all the time to allow immediate revocation, this will probably be more of a bother. Instead, the revocation option should be placed in an easy-to-find location, and in particular, it should be designed reciprocally to consent; if this was possible via a click-in-the-cookie banner, the revocation must also be possible via a click.

84 It is also important to ensure that the revocation option remains available and easy to find throughout the entire use of the website or app. According to the *Cookie Banner Task Force* by the EDPB a suitable solution is to implement a shortcut that enables the revocation by simply clicking on it ("small hovering and permanently visible icon").[198] A notice in the cookie banner that a revocation option can be found in the privacy policy or is possible via an email does regularly not meet the requirements of Article 7 (4) GDPR.[199]

V. Cookie-Walls

85 Cookie walls that block access to the site until the user chooses one of the options are not per se permitted under the GDPR. However, designs in which the user can only consent or can choose between general consent and general rejection, are not in line with the principle of voluntariness, as there is no genuine choice here.[200] In addition, the necessary granularity does not exist in the previously mentioned scenarios.

86 These types of cookie walls must be distinguished from the so-called "PUR model", which is very often found in the journalistic context. In this model, users can choose whether they want to access journalistic content without tracking, in which case they must pay a fee to use the service, or whether they consent to data processing and tracking, in which case they can use the site without paying further monetary compensation.[201] This raises the question if the consent is given voluntarily. Several data protection authorities of the Member States and the EDPB have expressed their views on this issue, and most of them have come to the same conclusion: cookie walls with an adequate alternative offer do not per se exclude the voluntary nature of consent.[202] However, this is only the case if the alternative offer is provided by the same party; pleading that (news) offers are available from other providers does not lead to a genuine and

198 EDPB (Cookie Banner Task Force), Report of the work undertaken by the Cookie Banner Taskforce, 17.1.2023, para 32.

199 EDPB (n 181) para 58 ff. (Hindering Pattern – type: Dead End) and para 45 (Hindering Pattern – type: longer than necessary).

200 Further details: Bundesverband Digitale Wirtschaft (BVDW), 'White Paper zum Wege-Modell / PUR-Modell / Cookie-Wall' (18.10.2021) 2, available at: <https://www.bvdw.org/fileadmin/bvdw/upload/dokumente/20211012_BVDW_Mehrwegemodell_PUR_Modell.pdf> accessed 11 December 2022.

201 in detail on issues of contract law, in particular on how a revocation of consent affects the contract: Dominik Nikol, Johannes Rost, ´Pur-Modelle unter dem neuen Digitale-Inhalte-Gesetz´ [2022] NJW 975.

202 EDPB (n 92) para 37 f.; DSK (Germany), decision of 22.3.2023 'Bewertung von Pur-Abo-Modellen auf Websites', available at: <https://www.datenschutzkonferenz-online.de/media/pm/DSK_Beschluss_Bewertung_von_Pur-Abo-Modellen_auf_Websites.pdf> accessed 1.4.2023; Austrian Data Protection Authority, decision of 25.5.2018, available at: <https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20181130_DSB_D122_931_0003_DSB_2018_00/DSBT_20181130_DSB_D122_931_0003_DSB_2018_00.pdf> accessed 11 December 2022; p. 6; Spanish Data Protection Authority, Guide to the use of cookies, point 3.2.10, July 2022, available at:https://www.aepd.es/sites/default/files/2020-07/guia-cookies.pdf <https://www.aepd.es/es/documento/guia-cookies.pdf> accessed 11 December 2022; Italian Data Protection Authorities, Guidelines on the use of cookies and other tracking tools, point 6.1 available at: <https://www.garanteprivacy.it/documents/10160/0/Consultazione+sul"e+"Linee+guida+s'll'utilizzo+di+cookie+e+di+altri+strumenti+di+tracciamen"o "+-+Allegato+1+-+Linee+guida.pdf/72eab081-e4c4-4500-77c3-8b6957f8cd12?version=2.0> accessed 11 December 2022; more reluctant, after the general ban on cookie walls was suspended by the Conseil d'etat (Decision of 6.19.2020 available at: <https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2020-06-19/434684)> accessed 11 December 2022 now the *CNIL*, Délibération n° 2020-091 v. 17.9.2020, available at: <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000038783337> accessed 11 December 2022; Questions-réponses sur les lignes directrices modificatives et ecommendationion « cookies et autres traceurs » de la CNIL, question 27, available at: <https://www.cnil.fr/fr/questions-reponses-lignes-directrices-modificatives-et-recommandation-cookies-traceurs> accessed 11 December 2022; states that cookie walls are only in certain cases contrary to the voluntariness requirement; other opinion is taken by the Dutch Data Protection Authorities, who undifferentiatedly consider cookie walls to be inadmissible, available at: <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/cookies> accessed 11 December 2022.

free choice.[203] Furthermore, the alternative offer must have a reasonable price[204], which depends on the circumstances of the individual case. The limit is usually reached where the price is so high that users are deterred from using the offer, as there is no real choice.[205] The view of the permissibility of the PUR model is also supported by the current draft of the ePrivacy Regulation[206]:

> *In contrast to access to website content provided against monetary payment, where access is provided without direct monetary payment and is made dependent on the consent of the end-user to the storage and reading of cookies for additional purposes, requiring such consent would normally not be considered as depriving the end-user of a genuine choice if the end-user is able to choose between services, on the basis of clear, precise and user-friendly information about the purposes of cookies and similar techniques, between an offer that includes consenting to the use of cookies for additional purposes on the one hand, and an equivalent offer by the same provider that does not involve consenting to data use for additional purposes, on the other hand. Conversely, in some cases, making access to website content dependent on consent to the use of such cookies may be considered, in the presence of a clear imbalance between the end-user and the service provider as depriving the end-user of a genuine choice. (Emphasis added by the author)*

87 Whether this view will prevail remains to be seen[207], since the result will be a digital two-class society despite the formal "freedom" and fair design of the model, since privacy will only be granted to those who can "afford" it. In particular, if this model is no longer used only in journalistic areas, but also by other digital services, it seems questionable whether its permissibility is in line with the values of the GDPR. The protection of personal data should not be made dependent on the solvency of the individual.

VI. Nudging and Dark Patterns

88 Nudging and Dark Pattens describe special methods of influencing behaviour. Dark pattern is a collective term for digital decision environments that are designed to induce users to take actions that could potentially be contrary to their presumed interest, or that they probably would not have taken without being influenced.[208] The EDPB has recently defined Dark Patterns as:

> *[...] interfaces and user experiences [....] that lead users into making unintended, unwilling and potentially harmful decisions in regards of their personal data. Dark patterns aim to influence users' behaviours and can hinder their ability "to effectively protect their personal data and make conscious choices", for example by making them unable "to give an informed and freely given consent".*[209]

89 The distinction between Nudging and Dark Patterns is not always easy to make. Nudging is intended to make it "easier" for the person concerned to make decisions. No option for action is prohibited or excluded from the outset, but the decision is steered in a certain direction through special design.[210] Nudging is generally intended to help the person concerned, whereas Dark Patterns are usually intended to mislead the person into making detrimental decisions. However, the actual interest of the person concerned can vary, so that nudging is not per se useful or in line with interests.

203 EDPB (n 92) para 38; Spanish Data Protection Authorities, Guidance on the use of cookies, July 2020, point 3.2.10, available at: < https://www.aepd.es/es/documento/guia-cookies.pdf > accessed 11 December 2022; Italian Data Protection Authorities, Guidelines on the use of cookies and other tracking tools, point 6.1 available at: <https://www.garanteprivacy.it/documents/10160/0/Consultazione+sul"e+"Linee+guida+s'll'utilizzo+di+cookie+e+di+altri+strumenti+di+tracciamento "+-+Allegato+1+-+Linee+guida.pdf/72eab081-e4c4-4500-77c3-8b6957f8cd12?version=2.0> accessed 11 December 2022; Austrian Data Protection Authority, decision of 25.5.2018, available at: <https://www.ris.bka.gv.at/Dokumente/Dsk/DSBT_20181130_DSB_D122_931_0003_DSB_2018_00/DSBT_20181130_DSB_D122_931_0003_DSB_2018_00.pdf>, p. 6 accessed 11 December 2022.

204 DSK (n 202) 1.

205 Nikol, Rost (n 201) 976.

206 Cf. recital 20aaaa ePrivacy Regulation Draft, available at: <https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf> accessed 11 December 2022.

207 The CNIL also appears to be very sceptical in this regard, making its comments on these designs on"y " conditional on the legality of this practies" CNIL, Deliberation No. 2020-091, 17.9.2020, para 19 available at: <https://www.cnil.fr/sites/default/files/atoms/files/lignes_directrices_de_la_cnil_sur_les_cookies_et_autres_traceurs.pdf> accessed 11 December 2022

208 Carolin Loy, Ulrich Baumgartner, ´Consent-Banner und Nudging´ [2021] ZD 404 (404); Mario Martini, Christian Drews, Paul Seeliger, Quirin Weinzierl, ´Dark Patterns´ [2021] ZfDR 47 (49).

209 EDPB (n 181) para 3.

210 Loy, Baumgartner (n 208) 404.

90 Neither the ePrivacy Directive, the GDPR, nor the TTDPA explicitly address these phenomena. Thus, there are no binding legal provisions for a permissible design. Hence, it is always necessary to consider each case based on the guidelines outlined above regarding voluntariness and informed consent as well as the new Dark Patterns Guidelines by the EDPB and the findings by the Cookie Banner Task Force[211] (although the specifications are explicitly not conclusive[212]). In addition, recourse can also be made to the recommendations of some Data Protection Authorities, which have recently made initial recommendations on nudging.[213]

91 The behaviour of a user of a website or an app can be influenced by colour design and the size and placement of the choices. Not every colour highlighting leads to the exclusion of voluntariness. On the contrary, the colour highlighting of the options can even be useful for the person concerned and can prevent a long search. Nevertheless, those designs are to be omitted in which the consent to the processing is highlighted in colour, while the rejection option is greyed out or barely visible[214], as this seriously calls into question the voluntary nature of the consenting process. This could lead the person concerned to the erroneous assumption that there is only the possibility of consenting, leaving them with the wrong assumption not having a real choice.

92 To avoid confusion, especially on the first level, not only the consent button should be highlighted in colour, especially not in a colour that the (regular computer) user associates with something positive. In *Windows,* in particular, the buttons that can be clicked or are to be clicked are highlighted in blue, for example, in installations. If now on the first level the "accept all" button is highlighted blue, one tends to click this button from routine, our learned behaviour is activated and the probability that the click was preceded actually by a comprehensive information admission sinks.

93 It follows from Recital 32 GDPR that the required information in the case of pre-formulated declarations of consent (as in the case of cookie banners) must be presented in a clear and comprehensible manner. Accordingly, if a cookie banner uses a slider, to select or deselect individual cookies, whose colour design is counterintuitive—for example, if consent leaves the slider in red and rejection leaves the slider in green—there is regularly no informed choice.[215] Green is generally associated with consent, so linking it to the rejection of data processing is misleading. The same applies to the position of the slider. In the digital context, the position of the slider on the right means that an option is turned on, and the position on the left means that the option is turned off. If this is reversed in the cookie banner, especially in combination with misleading colour codes, it is for the average user no longer easy to understand what their action will result in, so that the required information is regularly lacking. If a special colour code is used on the first level (e.g., green is consent and red is rejection), this should be maintained on all levels of the consent banner and not suddenly be swapped. The same applies to the positioning of the buttons, processors should take care that all information, inclusive of control buttons, are displayed consistently.[216] Otherwise, users may become unclear about what their actions mean and lack the necessary information. To definitely exclude nudging in the wrong direction or even misleading, either no button should have a particular colour or both should have the same colour.[217]

94 The uncertainty caused by renewed requests for rejection with the indication that consent is urgently needed or that the existence of the website or the service would be impaired without consent can also seriously call into question the voluntary nature of consent, especially since the GDPR stipulates that rejection should be as simple as consent. A neutral notice before consent in the information text that and for what purpose it is useful will not be objectionable. But the aggravation of the refusal and/or the repeated request[218] paired with an emotional ap-

211 EDPB (Cookie Banner Task Force), Report of the work undertaken by the Cookie Banner Taskforce, 17.1.2023.

212 EDPB (n 181) Annex: List of Dark Patterns Categories and Types, p. 60; EDPB (Cookie Banner Task Force) (n 211) Disclaimer, 1.

213 LfDI Niedersachsen (n 181) 7 ff.

214 EDPB (Cookie Banner Task Force) (n 211) para 18.

215 EDPB (n 181) para 95 (Left in the Dark Pattern – type: conflicting information); LfDI BaWü (n 174) 26.

216 Otherwise this can be classified as a Dark Pattern EDPB (n 181) para 66 (Fickle Pattern – type: Lacking Hierarchy); Loy, Baumgartner (n 208) 407 who classify this design as misdirection pattern; LfDI BaWü (n 174) 26.

217 This view is also supported by the French data protection authority CNIL, Délibération n° 2020-092 du 17 septembre 2020 portant adoption d'une recommandation proposant des modalités pratiques de mise en conformité en cas de recours aux «cookies et autres traceurs», p. 10 No. 34; <https://www.cnil.fr/sites/default/files/atoms/files/recommandation-cookies-et-autres-traceurs.pdf> accessed 11 December 2022; also agreeing LfDI BaWü, FAQ Cookies und Tracking durch Betreiber von Webseiten und Hersteller von Smartphone-Apps, Version 2.0 März 2022 p. 21.

218 In this direction also LfDI Niedersachsen (n 181) 7; EDPB

peal[219] or the indication that the website will only be usable to a very limited extent violates the principle of voluntariness. Consent given for such external considerations is not voluntary.

G. Practical problems with current consent mechanisms

95 The General Data Protection Regulation aims at protecting personal data. One of the cornerstones is consent, which is intended to ensure that processing only takes place if the informed data subject has agreed to it.

96 However, the objectives of the GDPR are currently only moderately achieved due to several reasons. As already explained, the legal situation is extremely complex. Several laws apply to the same processes. This problem has been addressed with the introduction of the TTDPA, among other things, but even with the introduction of the TTDPA, there is only a punctual improvement. It has become clear that the requirements of the GDPR generally also apply to consent for the storage of and access to information in end devices, but open questions in this regard have not been clarified. In particular, it remains questionable which cookies are covered by the exceptions. There are also no requirements for the design of the consent procedure. All in all, there is still uncertainty about which cookies require consent and which cookies are covered by the legal permissions in the GDPR or TTDPA. In addition, there are inconsistent provisions of the data protection authorities of the individual member states.[220] The result is that the data controllers generally ask for consent. In practice, this means that on every website visited and for every application used, data processing must be consented to or rejected in advance, regardless of whether obtaining consent was legally required in the specific case. This leads to a certain consent fatigue: the affected parties simply no longer want to deal with the content of the banner, even if it is prepared in compliance with the GDPR. This leads to the clicking without reading phenomenon, which has also been observed concerning data protection declarations. The EDPB also pointed this out:

> *This may result in a certain degree of click fatigue: when encountered too many times, the actual warning effect of consent mechanisms is diminishing.*[221]

This fatigue makes misleading designs even more effective; informed consent is practically rare.

97 This was also critically considered in the legislative process for the TTDPA, but the proposed Section 24 (3) which specifically aimed at cookie banners was not included in the final act:

> *(3) In the cases referred to in paragraph 1, the consent [...] shall be designed in such a way that the user can declare his consent or opt-out by using buttons legibly labeled with nothing other than the words "consent" and "opt-out." The buttons must be presented on the same level in a graphically equivalent manner. The obligation to provide information in accordance with paragraph 1 and the permissibility of using a further button that enables the user to give itemized and individual consent to the use of individual storage or access as defined in sentence 1 on a graphically separately designed level shall remain unaffected by this.*[222]

98 Given these problems, modern consent solutions have been proposed, which will be outlined in the following.

H. Innovative consent management

I. Browser and Software solution

99 The GDPR itself does not lay down any specific requirements for the design of consent, neither with regard to banner designs nor with regard to other possibilities. However, it also addresses technology. According to Article 25 GDPR, data protection-friendly default settings and data protection requirements are to be technically guaranteed. In this context, so-called Do-Not-Track (DNT) mechanisms are being discussed.[223] These mechanisms intend to enable users to make settings in their browsers that allow or deny the collection of data by tracking

(181) para 110 (Overloading Pattern – type: continuous prompting).

219 EDPB (n 181) para 163 (Stirring Pattern – type: Emotional Steering).

220 Until recently, it was still the case in France that for certain cookies 'informed browsing' should be sufficient to meet the requirements for consent, Art. 2 Délibération n° 2013-378 du 5 décembre 2013 portant adoption d'une recommandation relative aux Cookies et aux autres traceurs visés par l'article 32-II de la loi du 6 janvier 1978, whereas the German authorities consider this to be insufficient EDPB (n 92) paras 79, 86.

221 EDPB (n 92) para 87.

222 Statement of the Bundesrat and counterstatement of the Federal Government, ´Entwurf eines Gesetzes zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien' (BT-Drs. 19/28396, 2021) 3 f.

223 Cf. Specht-Riemschneider (n 37) Sec. 9 para 39.

tools of certain online services. This could restore at least a minimum of informational self-determination, which is currently impaired due to the previously addressed problems of consent fatigue and information overload. The German Federal Council has advocated for a DNT provision in the preparation of the TTDPA, which was not implemented by the legislator.[224] This result is accurate, even if it does not lead to an improvement of the cookie banner problems in the short term. A national DNT provision would be in conflict with the GDPR in terms of content and competence; the GDPR establishes the requirement of granularity, a single consent for any processing of personal data would currently not be data protection compliant. The Article 29 Working Party also expressed its opposition to the GDPR compliance of such a browser solution:

> *However, as general browser settings are not intended to apply to the application of a tracking technology in one individual case, they are unsuitable for providing consent under Article 7 and recital 32 of the GDPR (as the consent is not informed and specific enough).*[225]

100 Moreover, very precise specifications for the implementation of DNT would have to be introduced for browser providers in order to prevent misuse by them.[226] However, the national legislator has no regulatory competence for the design of consent mechanisms in the area of the GDPR.

101 The reduction of cookie banners would, by the current law, not be possible through a DNT function. However, the current draft of the ePrivacy Regulation contains in Article 9 (2) the provision that consent can also be given via suitable technical settings of software that enables access to the Internet, insofar as this is technically possible and feasible. Article 10 of the draft expands this by adding the provision that software placed on the market that permits electronic communication must also provide settings to prevent the storage or processing of information on the user's terminal equipment. In addition, the software must inform the user about the setting options directly during installation and require a decision by the user regarding the cookie setting. In the case of software that has already been installed, these requirements must be met at the latest during the next update. Thus, in future law, DNT settings in software or browsers could actually eliminate the need for individual consent on every website and every application.

102 However, the proposed rules have not been received without criticism. The Article 29 Working Party criticized, among other things, the fact that there are no rules on how to deal with outdated browsers or software that can no longer be updated.[227] In addition, they pointed out that, based on the current regulations, the software doesn't need to be set by default to prevent the storage or processing of information.[228] The Article 29 Working Party also calls for the establishment of uniform DNT standards to ensure that consent given in this manner is always voluntarily informed and granular.[229] Practical concerns were also expressed, partly doubting the technical feasibility of the project.[230] Whether and in what form DNT will be possible under the ePrivacy regulation is still uncertain, as the negotiations have not yet been concluded. For the moment, it, therefore, remains that DNT settings do not currently meet the requirements for effective consent.

II. Button solution

103 It has been suggested that, to ensure that the data subjects are actually informed and to make them aware of the consequences of their actions, the buttons should be specially labelled.[231] This is not a completely new approach to consent, but an increased warning function is to be achieved through appropriate labelling. For cookie walls, in particular, it is proposed to label the button with "*Pay with my data now*" or "*Agree to my surfing behaviour being tracked now*" in order to encourage the user to take a closer look at the consent to data processing.[232] The German Federal Council also proposed a comparable

224 Statement of the Bundesrat and counterstatement of the Federal Government (n 222) 4.

225 Art. 29 Data Protection Working Party, 'Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)' (WP 247, 17/EN) para 24.

226 In detail on the danger of misuse: *Golland*, Statement on the TTDSG draft, pp. 13f. <https://www.bundestag.de/resource/blob/836010/498ffdbeff45200bdc011b13acc38b31/19-9-1054_Stellungnahme_SV_Dr_Golland_PwC_Legal_oeA_TTDSG_21-04-2021-data.pdf> accessed 13 October 2022.

227 Art. 29 Data Protection Working Party (n 225) para 49.

228 Art. 29 Data Protection Working Party (n 225) para 19.

229 Art. 29 Data Protection Working Party (n 225) paras 24, 48.

230 The Commission nationale informatique & libertés (CNIL) does not consider the current state of technology to be so advanced that effective consent can be given via corresponding settings in the browser: recommendation *CNIL* „cookies and other trackers", paras 71 – 73.

231 Andreas Sesing, `Cookie-Banner-Hilfe, das Internet ist kaputt' [2021] MMR 544 (547).

232 Sesing (n 231) 547.

provision in its opinion on the draft TTDPA, which however was not included in the final Act.[233]

104 This minor modification will not be sufficient to address the problems outlined above; a more comprehensive solution for consent management is needed. Since the labelling of the buttons cannot compensate for an otherwise cumbersome or difficult-to-understand consent banner. Nevertheless, the uniform and warning labelling of the button could be added as a complementary step. However, in this respect, the national legislator should refrain from imposing fixed labelling requirements, as otherwise the spectrum enabled by the GDPR would be unlawfully restricted, which would lead to the corresponding national requirements being unlawful under EU law.[234]

III. PIMS

105 Another approach, which has been under discussion for some years, could be to provide data subjects with more centralized information and consent tools (so-called Personal Information Management Systems (PIMS)), which would allow them to manage consent in a particularly user-friendly way. The user should be able to make all the desired and required privacy settings via a central dashboard, which must be accepted by the respective service providers. To link the respective settings to the data usage requests, a service is intermediated: a data fiduciary. This trustee takes over the administration without earning any money from the use of the data. The advantage of this approach is that the number of consents could be significantly reduced, and simple acceptance and rejection is made possible. The user also always has an overview and persistent cookies, which remain even after the website has been closed, are not lost sight of. Furthermore, it is always possible to revoke them.

106 A distinction must be made to PIMS that are designed for data sharing intermediation[235] (to simplify the intended exchange of data between the data subject and the controller) and PIMS designed to ensure a secure and simple exchange of data in the B2B area. In this case, the management system primarily serves to promote data trade; Article 10ff. Data Governance Act (DGA)[236] is aimed at these systems. Among other things Article 12 DGA stipulates that:

107 The provision of data-sharing services referred to in Article 10 shall be subject to the following conditions:

> (a) the data intermediation services provider shall not use the data for which it provides data intermediation services for purposes other than to put them at the disposal of data users and shall provide data intermediation services through a separate legal person;
>
> (b) the commercial terms, including pricing, for the provision of data intermediation services to a data holder or data user shall not be dependent upon whether the data holder or data user uses other services provided by the same data intermediation services provider or by a related entity, and if so to what degree the data holder or data user uses such other services;
>
> (c) the data collected with respect to any activity of a natural or legal person for the purpose of the provision of the data intermediation service, including the date, time and geolocation data, duration of activity and connections to other natural or legal persons established by the person who uses the data intermediation service, shall be used only for the development of that data intermediation service, which may entail the use of data for the detection of fraud or cybersecurity, and shall be made available to the data holders upon request;
>
> (d) the data intermediation services provider shall facilitate the exchange of the data in the format in which it receives it from a data subject or a data holder, shall convert the data into specific formats only to enhance interoperability within and across sectors or if requested by the data user or where mandated by Union law or to ensure harmonisation with international or European data standards and shall offer an opt-out possibility regarding those conversions to data subjects or data holders, unless the conversion is mandated by Union law;
>
> (e) data intermediation services may include offering additional specific tools and services to data holders or data subjects for the specific purpose of facilitating the exchange of data, such as temporary storage, curation, conversion, anonymisation and pseudonymisation, such tools being used only at the explicit request or approval of the data holder or data subject and third-party tools offered in that context not being used for other purposes;

233 Statement of the Bundesrat and counterstatement of the Federal Government (n 222) 4.

234 Based on this reasoning, the corresponding provision in the TTDPA proposed by the Federal Council was rejected by the Federal Government Statement of the Bundesrat and counterstatement of the Federal Government (n 222) 4.

235 Detailed information on all types of PIMS: *Blankertz et al.*, Datentreuhandmodelle – Themenpapier, April 2020, pp. 3 ff. <https://pure.mpg.de/rest/items/item_3222478_2/component/file_3222479/content> accessed 11 December 2022.

236 Regulation of the European Parliament and of the Council of 30 May 2022 on European data governance 2022/868 (Data Governance Act) (EU) 2022/868, OJ L 151, 1.

108 It is evident that the regulations are specifically intended to govern data trading via a central system and not primarily to simplify consent. PIMS, which are only intended to serve as a "consent assistant", have not yet been subject to any concrete legal regulation at European level.

109 A provision in this regard has now been introduced on the national level by the TTDPA. Section 26 (1) TTDPA cumulatively requires that consent management services have user-friendly and competitive procedures and applications for obtaining and managing consent, have no economic self-interest in consent and managed data, do not process information about consent decisions for other purposes and, finally, present a security concept that demonstrates compliance with data protection and data security requirements. If these requirements are met, these services can be recognized by a body that is yet to be determined. The actual rules have not yet been established by Section 26 (1) TTDPA, since Section 26 (2) TTDPA stipulates that the German Federal Government shall regulate the content of Section 26 (1) No. 1 - 4 TTDPA by statutory order. So far, however, it is not yet foreseeable when such an ordinance will come into force.[237] According to the German Federal Government, an expert opinion has already been requested.[238] This opinion was completed in December 2021.[239] The finalization of the ordinance based on this expert opinion is planned for the end of 2022. Then it is to be submitted to the European Commission for notification. If the proposal will be accepted, the regulation could be promulgated. However, the provisions can be blocked by the Commission for 12–18 months if a harmonization in the same area is (to be) carried out by the EU. Such harmonizing provisions may lie in the DGA, which also contains provisions for data-sharing services as shown above, so a temporary blocking of the regulations by the Federal Government is indeed possible.[240]

110 Apart from the lack of a concretizing regulation, there are several other problems. The prototype of a PIMS that serves as a consent assistant could function as follows: the trustee manages the data of the data subject, i.e. they grant or deny consent on behalf of the data subjects according to their specific preferences (these can be defined in the trust agreement). Although such systems are included in the TTDPA the legally compliant design of a PIMS is problematic, even if civil law questions of data trust[241] are ignored. Actions by and with those systems must always be measured against the GDPR. If PIMS are to function as a kind of consent assistant, several data protection questions arise.

1. Data protection issues

111 Initially, it should be noted that there are several (processing) acts that need to be distinguished from one another, and each needs to be evaluated and, if necessary, justified separately according to the GDPR standards. The evaluation depends on the exact design of the PIMS, but for simplicity, the following explanations are based on the prototype of the consent assistant described above[242]:

112 The information sent by the user to the data trustee will usually be stored or at least temporarily stored; this (temporary) storage already constitutes the first relevant processing act under Article 4 GDPR. The same applies to the forwarding or making available of the relevant information to or for the third party so that the latter can adjust the use of its cookies accordingly. Besides consent according to Article 6 (1) lit. a GDPR, the fulfilment of a contract pursuant to Article 6 (1) lit. b GDPR could be considered as a justification for these processing operations since the

237 The *Bitcom* has completely advocated against the introduction of national PIMS provisions because of the pending Data Governance Act; in their view, only a uniform European regulation makes sense: *Bitcom*, Statement on the TTDSG draft, pp. 13f.: <https://www.bmwi.de/Redaktion/DE/Downloads/Stellungnahmen/Stellungnahmen-TTDSG/bitkom.pdf?__blob=publicationFile&v=4> accessed 11 December 2022:, p. 3; Other view: Rolf Schwartmann/Kristin Benedikt/ Yvette Reif, ´Entwurf zum TTDSG: Für einen zeitgemäßen Online-Datenschutz´ [2021] MMR 99 (101) who think that Germany should take on its role as a driving force.

238 *Bender*, Federal ministry of economics and energy, speech at the conference: Das TTDSG und neue Wege zur Einwilligungsverwaltung, 3.11.2021 <https://stiftungdatenschutz.org/veranstaltungen/unsere-veranstaltungen-detailansicht/ttdsg-einwilligungsverwaltung-234#lg=1&slide=12> accessed 11 December 2022.

239 Oliver *Stiemerling/ Steffen Weiß/ Christiane Wendehorst*, Forschungsgutachten zum Einwilligungsmanagement, 16.12.2021, available via: <https://www.ecambria-experts.de/it-sachverstaendiger/wp-content/uploads/2022/01/211216-Gutachten_fuer_Bundesministerium_fuer_Wirtschaft_und_Energie_pos37621.pdf> accessed 11 December 2022.

240 Also of this opinion: Alexander Golland, Anne Riechert, in Anne Riechert, Thomas Wilmer (eds), *TTDSG* (Erich Schmidt Verlag, 1st edn 2022) § 26 para 3.

241 Detailed on this: Louisa *Specht-Riemenschneider, Aline Blankertz, Pascal Sierek, Ruben Schneider, Jakop Knapp, Theresa Henne, `Die Datentreuhand* -Beil. 25 (33ff).

242 for further scenarios and the legal implications, see Jens Nebel, Einwilligungsverwaltungsdienste nach dem TTDSG´ [2022] CR 18 (19 ff.).

performance of these actions will regularly be governed by the trust agreement. However, this justification does not apply to sensitive data within the meaning of Article 9 GDPR. The evaluation and the storage of the data by the responsible website operator and controller must of course also be justified. Depending on the future legal regulation on PIMS—to be discussed below—these processing acts could be permitted by Article 6 (1) lit. c GDPR.

113 Another central question for these types of management systems is whether consent by a third party is possible at all. Representation concerning consent is generally rejected by a certain number of authors.[243] This is partly based on the fact that consent is not a declaration of intent, but a reason of justification.[244] Some authors focus on the existence of the representation rules regarding data subjects' rights in Article 80 GDPR and conclude *e contrario* that no representation is possible with regard to other acts such as consent.[245] Neither the ECJ nor international or national data protection authorities have explicitly commented on the issue, although the EDPS' opinion 9/2016 on Personal Information Management Systems[246] strongly suggests that representation is principally possible, since otherwise the user-friendly system the EDPS described[247] would hardly be feasible. Without the possibility of representation, the fiduciary would only be a mostly useless third party who does not contribute to an improvement of consent management. A significant part of the literature favours, however, the possibility of representation with regard to consent.[248] On the one hand, this is because representation is not fundamentally unknown in EU law, even if it has not been explicitly anchored in the GDPR, and on the other hand, because the GDPR primarily serves to protect the right of informational self-determination, and the decision to use a representative is ultimately also an expression of this right.[249] However, to ensure a high level of data protection, it is necessary to apply the same requirements to the proxy as to the consent itself.[250] Depending on the specific design and configuration of the system, the trustee may also be merely a messenger, which should legally be even more possible according to the view advocated here.

114 A crucial factor for the success of PIMS will be whether a legal obligation for data controllers to take account of the forwarded decisions (consent/no consent) is introduced. If the controllers are not obliged to take into account the decisions made by the data subjects within the PIMS, they can continue using their own consent tools, which aggravates the actual problem[251] as data subjects will then regularly have to make multiple decisions for the same process. This will significantly reduce trust in PIMS and hinder their success.

115 A further problem is that, in principle, users would have to decide for each individual processing operation, i.e., for each individual website, whether they want to consent or refuse to data processing—even if they use a PIMS—to ensure that there is no violation of the principle of granularity and certainty. However, this would just result in moving the aforementioned problems to a different setting. The user would no longer have to consent to the websites rather than in their PIMS, and the number of consents would not be reduced so that consent fatigue would also quickly develop in this scenario. It is argued that the principle of certainty should be interpreted according to the situation and that the spe-

243 Stefan Ernst, 'Die Einwilligung nach der Datenschutzgrundverordnung´ [2017] ZD 110 (111); Helferich, 'Einführung und Grundbegriffe des Datenschutzes' (56th ed. May 2021), Part. 16.1 para 51; Taeger (n 50) Art. 7 para 10; Schulz (n 49) DS-GVO Art. 7 para 8 f.

244 Ulrich Freiherr von Ulmenstrein, `Datensouveränität durch repräsentative Rechtswahrnehmung´ [2020] DuD 528 (534) Schulz (n 49) DS-GVO Art. 7 para 8, who, however, classifies consent as a "real act".

245 Michael Funke, 'Die Vereinbarkeit von Data Trusts mit der Datenschutzgrundverordnung (DSGVO)' (Algorithm Watch, December 2020) 15, <https://algorithmwatch.org/de/wp-content/uploads/2020/11/Die-Vereinbarkeit-von-Data-Trusts-mit-der-DSGVO-Michael-Funke-AlgorithmWatch-2020-1.pdf> accessed 13 October 2022 who leaves the question unanswered.

246 EDPS, 'Opinion 9/2016 on Personal Information Management Systems' (20.10.2016) 8 <https://edps.europa.eu/sites/default/files/publication/16-10-20_pims_opinion_en.pdf> accessed 13 October 2022.

247 EDPS, ´Opinion on Personal Information Management Systems´ (n 246) 8.

248 Birgit Hoffmann, ´Einwilligung der betroffenen Person als Legitimationsgrundlage eines datenverarbeitenden Vorgangs im Sozialrecht nach dem Inkrafttreten der DSGVO` [2017] NZS 807 (808); Thomas Janicki, `Die Einwilligungsfähigkeit zwischen Digitalisierung und demographischem Wandel´ [2019] DSRITB 313 (323); Ingold (n 87) Art. 7 para 19; Specht-Riemenschneider, Blankertz, Sierek, Schneider, Knapp, Henne (n 241) 25 (41).

249 Jürgen Kühling, ´Der datenschutzrechtliche Rahmen für Datentreuhänder´ [2021] ZfDR 1 (8); Funke (n 245) 15.

250 So correctly: Specht-Riemenschneider, Blankertz, Sierek, Schneider, Knapp, Henne (n 241) 41; Jürgen Kühling, ´Der datenschutzrechtliche Rahmen für Datentreuhänder´ [2021] ZfDR 1 (8).

251 This is also expected by: *Golland*, NJW 2021, 2238 (2241).

cific circumstances of the situation may lead to a broad interpretation.[252] The background and purpose of the use of PIMS are precisely to give and manage a *typified* consent that is merely *generic*—this must be considered so that the requirement for certainty should already be fulfilled if only objective foreseeability regarding the processing operations is given.[253] However, this is not officially or judicially confirmed, and to avoid legal uncertainty there is a need for legislative action with regard to the possibility of "broad consent".[254] This has already been discussed for medical research[255] and seems very beneficial for PIMS. In its opinion on PIMS, the EDPS already encouraged that the conditions under which this type of broad consent shall be permitted should be examined.[256] The user should be able to give or refuse consent for specific purposes in a bundled way. Of course, there should still be the possibility to decide granularly if this is desired. In the case of broad consent, it must always be ensured that the data subjects are aware that they are practically giving multiple consents and that they are accurately informed about the purposes for which they are giving this multiple consent; comprehensive information for the user is essential. Since the "relaxation" of the strict granularity in Recital 33 explicitly refers only to scientific research and also the opening clause in Article 9 (2) lit. j GDPR has only a very narrow scope of application, a regulatory act with regard to PIMS is mandatory. There has to be a balance between the necessity of informing and educating the user and keeping the system simple and practicable.

2. Technical implementation

116 In addition to the legislative issues, designing a user-friendly, legally compliant, and efficient system is also a technical challenge. So far, there are only a few providers that have already presented widely developed (test) systems, such as *NetID* or *NOYB*. The functioning of NOYBs system "Advanced Data Protection Control" (ADPC) is an extension of the simple DNT-browser setting: web pages can send their privacy requests in a machine-readable way, and ADPC allows the response to be transmitted using special header signals or via Java Script. Similar to a "camera release"-request, users can release their data via a uniform pop-up in the browser. Furthermore, intelligent settings should also be possible, allowing users to choose to receive only certain requests—a function similar to a spam filter.[257] In contrast, NetID's system does not focus on browser signals, but on log-in solutions: users have to register once and can manage their consents and other privacy settings in the NetID portal. When data subjects visit a website, they can use the NetID log-in and the privacy settings are applied directly to the website without the user having to make any additional decisions.[258]

3. Certification procedure

117 It is of utmost importance that the reliability of the data trustees is ensured. Article 26 (1) TTDPA already provides for a certification procedure. In order to assure a high level of data protection, it is essential to ensure that only reliable independent companies receive such certification and not obvious stakeholders. The *Data Ethics Commission* has also warned that if PIMS are designed incorrectly, there is a risk that instead of enabling genuine self-determination, affected persons will be led down a path of unconscious or careless external determination and that the operators of the PIMS can exploit their full decision-making power in a way that is not in line with the users' interests.[259] A strict certification procedure must be in place to ensure that this kind of abuse will not occur. For instance, criticism was voiced against NetID questioning its data-protecting intent, as it was founded by *Mediengruppe RTL Deutschland*, *ProSiebenSat.1* and

252 Nebel (n 242) 21.

253 Nebel (n 242) 21.

254 Specht-Riemenschneider, Blankertz, Sierek, Schneider, Knapp, Henne (n 241) 41.

255 On this matter: Stefanie Hänold, `Die Zulässigkeit eines„broad consent" in der medizinischen Forschung - a never ending story?` [2020] ZD-Aktuell 06954; Thanos Rammos, `Die datenschutzrechtliche Zulässigkeit von Broad Consent für Forschungszwecke nach der DSGVO´ [2017] DSRITB 359;; Carina Dorneck/Ulrich M Gasser/Jens Kersten/Josef Franz Lindner/Kim Philip Linoh/Katja Nebe/Henning Rosenau/Birgit Schmidt am Busch,´Contextual Consent` [2019] MedR 431.

256 EDPS, ´Opinion on Personal Information Management Systems´ (n 246) 8.

257 Cf. <https://noyb.eu/de/neues-browser-signal-koennte-cookie-banner-ueberfluessig-machen> (accessed on 15th November 2021) accessed 11 December 2022.

258 Cf. <https://image.netid.de/cd/netid/netid_spot_30.mp4> and <https://image.netid.de/cd/netid/netid_spot2_30.mp4> accessed 11 December 2022.

259 Gutachten der Datenethikkommission, 23.10.2019, Sec. 4.3.2 <https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf;jsessionid=98CEBC17A4DF3180E939F10819AC4129.2_cid295?__blob=publicationFile&v=6> accessed 11 December 2022.

United Internet.[260] According to some critics, the fact that such media and Internet giants do not primarily have the interests of the data subjects in mind becomes particularly evident as NetID uses dark patterns.[261] These are intended to ensure that as much data as possible can be collected.[262] Such circumstances should be taken into account in the certification process; on the other hand, not only strict consumer protection organizations should be certified, since PIMS should not be designed to reject all queries in general. They should be auxiliary tools that allow the users to exercise their decision-making authority and do not deprive them of this authority in one direction or the other.

118 Overall, PIMS have great potential to minimize the above-mentioned problems[263], but their success depends on the legislative requirements for their design and in particular, on whether they are technically feasible.

I. Conclusion

119 In conclusion, it can be stated that despite sector-specific regulations, the requirements of the GDPR are central and form the benchmark for the analysis of consent tools, primarily because the ePrivacy Directive, the TTDPA, and the draft of the ePrivacy Regulation refer to its regulatory regime. This means that for the storage and access or other processing of personal and non-personal data, it is generally necessary to obtain a clear, informed, voluntary, and granular consent.

120 Even if no explicit specifications are made for the design, it follows from these requirements that the cookie banner must be clearly visible and contain all the necessary information in clear and simple language; care must be taken to ensure that this information is arranged in a reasonable manner and, if necessary, can be accessed via easy-to-find dropdown menus or sidebars. The data subject must be given the opportunity to give his or her consent or refusal granularly for each processing purpose, the listing of the purposes, and, if applicable, third-party providers must also be done in a transparent manner, and a simple, if possible bundled, selection and deselection option must be provided. The information should already be available on the first level and not be hidden behind links or in the data protection declaration. In addition, the labelling and design of the buttons must be as neutral and comprehensible as possible, and misleading colour choices or designations must be avoided. Other forms of negative nudging or dark patterns must also be averted, even if the applicable standards do not advocate any explicit prohibitions in this regard, a design that is intended to cause behavioural anomalies for the user regularly violates the principle of voluntariness and the transparency respectively information obligation.

121 Even cookie banners that meet these requirements and are therefore formally legally compliant cannot completely prevent practical problems such as consent fatigue. It is therefore important to examine new forms of consent management that allow users to manage their consent centrally in order to avoid constant consent queries. However, these PIMS must also enable a voluntary, informed and, in principle, granular decision; it remains to be seen to what extent this will be implemented by the expected ePrivacy Regulation. Until then, it remains that users must be able to give their consent on websites they visit or apps they use according to the picture drawn here.

260 Florian Meier,´Datenkrake im Schafspelz: netID´ (2019) flomei-online <https://www.flomei.de/blog/2019/12/15/datenkrake-im-schafspelz-netid/> accessed 11 December 2022.

261 In detail: Torsten *Kleinz*, ´NetID: LogIn-Allianz startet mit 60 Partnerseiten´ (2018) heise-online <https://www.heise.de/newsticker/meldung/NetID-LogIn-Allianz-startet-mit-60-Partnerseiten-4216340.html> accessed 11 December 2022.

262 Meier (n 260).

263 Cf. Part H.3.

Home is where the heart is

The household exemption in the 21st century

by **Bart van de Sloot***

Abstract: The household exemption provides that the data protection regime does not apply when a natural person processes personal data for purely personal or household activities. The exemption was inserted because personal and household activities were considered to fall under the right to privacy and because it was deemed unlikely that such activities would cause significant harm. Ever since its introduction, but especially due to its interpretation by the Court of Justice and the partial revision under the GDPR, ambiguity and uncertainty have plagued the exemption. Moreover, because of the increased access of citizens to data processing technologies and the ease with which large amounts of (sensitive) data can be made public, the question is whether the initial rationale for the household exemption is still valid and whether it should be revised or even omitted from the data protection regime.

Keywords: household exemption; GDPR; Lindqvist; Rynes; Jehovan todistajat

Recommended citation: Bart van de Sloot, Home is where the heart is: the household exemption in the 21st century, 14 (2023) JIPITEC 34 para 1.

A. Introduction

1 The first data protection instrument that contained a household exception was the European Union (EU) 1995 Data Protection Directive (DPD). Previous national regimes[1] and the Council of Europe (CoE) Resolutions from 1973[2] and 1974[3] and its Convention108[4] from 1981 did not. The reason for its introduction was that automated processing techniques until the 1990's had by and large been in the hands of a few larger corporations and governmental agencies. Consequently, the earliest legal frameworks focussed primarily or even exclusively on the small number of parties that had the capacity to maintain and utilize them. The EU legislator was mindful that at the end of the 1980's, citizens were also gaining access to automated data processing techniques, such as through a personal computer, and digital forms of communication, such as e-mail. Although the consensus was that citizens who process personal data about others should in principle fall under the data protection regime and respect the rights and obligations contained therein, the thought was also that some small-scale processing of personal data by citizens in the privacy of their homes might be excluded.

* Associate professor, Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University, Netherlands.

1 U. Dammann, O. Mallmann & S. Simitis (eds.), 'Data protection legislation: an international documentation', 1977.

2 Resolution (73) 22 on the protection of the privacy of individuals vis-a-vis electronic data banks in the private sector (26 September 1973).

3 Resolution (74) 29 on the protection of the privacy of individuals vis-a-vis electronic data banks in the public sector (20 September 1974).

4 Convention for the protection of individuals with regard to automatic processing of personal data, 1981.

2 During the legislative process of the DPD, many views on the precise wording, scope and fields of application arose , without the parties suggesting these sometimes-conflicting views clearly entering a dialogue with one another. Consequently, the reasons behind the final wording of the relevant recital and article are unclear and difficult to grasp. The European Court of Justice (CJEU) subsequently interpreted the household exemption in a very narrow manner, while the Working Party 29 (WP29), and its successor, the European Data Protection Board (EDPB), have actively tried to nuance the rulings by the Court.

3 This article will provide a discussion of the household exemption. It will focus primarily on the legislative processes of the DPD and GDPR, CJEU judgements and opinions by the WP29, the EDPB and the European Data Protection Supervisor (EDPS). Literature on the point of the household exemption will not be discussed. The approach this article will adopt is a mainly textual analysis, assessing in detail specific sentences, phrases and words and their potential meaning. Doing so, critical thoughts and questions about potential unclarities will be highlighted throughout the article. The driving questions for this research are: What is the rationale behind the household exemption? What is its scope? And are the rationale and scope still viable in the 21st century?

4 To answer this question, section B will delve into the legislative process of the Data Protection Directive, the relevant opinions by the EDPS and the WP29 and the judgements of the CJEU. This will result in a thorough understanding as to why the household exemption was introduced and how it has been (re)interpreted since. Section C will assess the legislative process of the GDPR and its subsequent implementation in the legal regimes of Member States. This will result in an understanding as to which changes were and which changes were not made in the GDPR and how the household exemption under the GDPR has been interpreted. Section D will provide an analysis, also assessing potential arguments in favour and against omitting the household exemption from the data protection framework and assess how, should that option be chosen, the household exemption could be revised and reformulated.

B. Data Protection Directive

I. Legislative history

5 Right from the initial proposal for a DPD by the Commission, the household exemption was included in the text. Throughout the legislative process, the provision underwent several small, but important changes. From the legislative history, no unified approach can be discovered with respect to the meaning, interpretation, rationale and scope of application of the exemption. Rather, it seems that while sometimes explicitly substituting its own wording for that of another party to the legislative process, most revisions are not the result of a critical dialogue, but rather of ad hoc and standalone suggestions and variations on a theme. Some of the most important aspects of the household exemption in the legislative process of the DPD will be discussed below to understand the ambiguity that later plagued its interpretation and meaning in jurisprudence and opinions. The text that was finally adopted in the Directive is:

Recital 12	Whereas the protection principles must apply to all processing of personal data by any person whose activities are governed by Community law; whereas there should be excluded the processing of data carried out by a natural person in the exercise of activities which are exclusively personal or domestic, such as correspondence and the holding of records of addresses;
Article 2	2. This Directive shall not apply to the processing of personal data: - by a natural person in the course of a purely personal or household activity.

6 **Examples**: Both in the legislative history and in the relevant recital, several closely related, but distinct examples of when the household exemption would apply have been provided. The example given by the Commission in its initial proposal was that of keeping a personal electronic diary.[5] A diary is highly personal, and something normally not shared with third parties. It contains subjective interpretations and private emotions as well as objective facts, such as what a person did or whom they spoke to on a certain day. A diary may contain data about a person themself, but often also discusses the lives and behaviour of loved ones, friends, and family. It may also include statements or observations about public events and figures or personal effusions like 'I'm in love with my boss' or 'I think the prime minster is a total creep'. A second example is that of a personal address file.[6] An address file is distinctly different

5 COM(90) 314 final ~.sYN 287 and 288 Brussels, 13 September 1990.

6 I CC)M(90) 0314 — C3-0323/90 SYN 287.

from a personal diary. It contains far less information and in principle no sensitive data (though of course an example might be construed where a person lives in a brothel or similarly sensitive location). These addresses are usually already in the public domain; addresses, names and telephone numbers were traditionally made available through a phone book or similar catalogues. Normally, a person only holds an address book with people whom they are in contact with or plan to be; importantly, a person may keep an address book for both personal and professional reasons (especially as some colleagues may be friends). A third and final example, which was incorporated in the recital only late in the process, was that of correspondence.[7] Obviously, this example is directly related to keeping an address file. Still, it is distinct in that it entails acting on the data, engaging with persons outside the home or family sphere and that personal data of third parties may be disclosed. An e-mail addressed to a friend may, for example, concern the awkward behaviour of a mutual colleague, a friend, or the prime minister. This example, as well as the second example, is directly linked to Article 8 of the European Convention on Human Rights (ECHR), the right to correspondence, while the first example, that of keeping a diary, may be seen as linked to the right to private life. The first example was not, the latter two examples were incorporated in the recital of the DPD.

7 **Rationale:** The Commission favoured a household exemption because an "invasion of privacy was unlikely to occur" when data are used for private purposes only,[8] thus focussing on the potential impact of the data processing.[9] A second rationale was that household activities themselves were deemed to fall under the right to private life (Article 8 ECHR).[10] Because the data protection framework was set out to enhance the privacy of citizens, it should not intrude on the private sphere of individuals.

8 **Scope:** The standard approach to the household exemption is that if it applies, then the data protection framework is inapplicable. Another approach was suggested by the Economic and Social Committee (ESC), which stressed that it supported the household exemption, but that "the general principles of Convention108 should continue to apply to such processing to guard against improper use."[11] The DPD, which is meant to provide for more and stricter rules than Convention108, cannot lead to a lower level of protection than provided by Convention108, which does not contain a household exemption.

9 **Private/personal/household/domestic:** The initial proposal for the Article did not refer to the household, but spoke of "private and personal", while the initial recital referred to the exercise of a natural person's right to privacy. This was changed only quite late in the legislative process, when it was suggested that the recital speak of "personal or domestic" and the article of "personal or household".[12] No explanation was given for this amendment. It might be suggested that the revised wording makes clear that the private domain in which the processing takes place should be a central element, thereby excluding private activities that take place outside the home. But, if this were the correct interpretation, this raises a question concerning the relationship between private and personal and between personal and domestic. Why the recital speaks of domestic and the article of household was left unexplained.

10 **And, or:** The revision had another important effect, namely that it changed "and" for "or" [i.e. "personal or household" instead of "personal and household"]. With respect to "and", it could be wondered whether it was meant as an exclusive or an inclusive term. Was it used in the sense of "I like to go on vacation to Paris and New York" or in the sense of "I like to go on vacation to a place warm and sunny"? This is important, because though "private" is replaced by the more specific and potentially more restrictive "domestic" and "household", the term "personal" has a broad connotation and personal activities could extend far beyond the private sphere. The legislator seems to have made an end to this discussion by using the term "or" instead. Yet, the term "or" raises similar questions, as it can be used in an inclusive way, "I like to go on vacation to France or Spain", or in an exclusive way, "I like to go on vacation to a place that's very warm or ice-cold".

11 **Purposes/activities:** The initial proposal spoke of private and personal *purposes.* Consequently, it was the goal or the reason for which personal data were processed that was determinative for the question of whether processing of personal data fell under the household exemption. Parliament suggested to change that to *activities*, without providing explanation. Perhaps it is because activities can

7 92 /C 311 / 04 COM (92) 422 final — SYN 287.

8 Supra (5).

9 It is good to note that the harm is linked to the right to privacy and not to the right to data protection.

10 Supra (5).

11 91/C 159/14 Opinion on: the proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data.

12 95/C 93/01 Common position (EC) No 1 /95 on 20 February 1995 adopted by the Council,.

be objectively assessed, while purposes are purely subjective. Although there is something to be said for this interpretation, and this line of is at times adopted by the CJEU, it would still be remarkable because the purpose for processing personal data is arguably the central element in the data protection framework.

12 **Exclusivity:** The Commission's proposal referred to "solely", both in the recital and in the article. Later, this was changed so that the recital speaks of "exclusively" and the article of "purely". All words seem to mean more or less the same, and no discussion or explanation exists of why these words have been changed. Consequently, it might be suggested that they could be treated as interchangeable synonyms. At the same time, if these words mean the same, the question is why they are changed, and different wording is used for the recital and the article. An additional question that might be posed is whether the exclusivity clause only refers to "personal" and not to "household" activities ("exclusively personal" and "household", instead of "exclusively personal" and "exclusively household" or "exclusively personal or household"), but from the changing of the order of the terms, it seems clear that this is not the case.[13]

13 **Files/personal data:** The initial proposal by the Commission referred to files held by an individual solely for private and personal purposes. The notion of data file, instead of personal data, was central throughout the initial proposal for the Directive by the Commission. This was changed on the suggestion of the ESC because the concept of data files seemed too narrow: "personal data can nowadays be processed in an expert system without necessarily having to be structured (integrated data-bases). Moreover, it is the "purpose" of the processing that is crucial in data protection and that establishes whether or not the collection of data is legitimate. Accordingly, the Committee feels that the concept "processing of personal data", rather than the "file", should be used to define the scope of the Directive. The term "processing" should therefore replace the term "file" in Articles 3, 4, 5, 7, 8(l)(c), 8(2) and 11."[14]

14 **Embedding:** The initial proposal referred not only to the matters falling outside community law, but also, in paragraph 2 of Article 3, both to the household exemption and to non-for-profit-organisations holding files on its members, who have consented to their personal data being processed, where those data are relevant for the interests of these organisations and where the data are not transferred to third parties. Examples that were given related to political organisations, sport organisations, trade unions, religious organisations and, more generally, cultural, philosophical, and even leisure organisations. The reason to treat this exemption in the same paragraph as the household exemption was that in both situations, harm was thought to be unlikely.[15] This suggestion did however not make it to the final text.[16]

II. EDPS and Working Party 29

15 The EDPS has only in a small number of opinions referred to the household exemption, the WP29 in a substantial number of opinions. Several points stand out from their reflections.

16 **Controllership:** The WP29 treats the household exemption, in quite a number of instances in the context of controllership, as if the household exemption was an exemption to the notion of controllership instead of the data protection framework as a whole.[17] For example, it stressed that a citizen needs not assume the role of the data controller when using Social Network Sites (SNS),[18] when they can rely on the household exemption,[19] an approach which was repeated in its opinions on the concepts of data controller and processor,[20] search engines[21] and when assessing the quality of Quebec's data protection legislation.[22] If a citizen relies successfully on the household exemption, and

13 As was later confirmed by the AG in Rynes.

14 Supra (11).

15 Supra (5).

16 Parliament also unsuccessfully suggested to extend the list to (1) data held by journalists and journalistic media; (2) data held under an obligation laid down by statute on condition that the personal data are not communicated to third parties; (3) held in archives either for purposes of re-construction or for use as evidence; (4) held in compliance with a legal obligations; (5) from sources or registers whose object is to ensure publicity for such data; and (6) held for payroll, pensions and accounts purposes.

17 5035/01/EN/Final WP 56.

18 The question is here how much a SNS resembles a household. The focus of the WP29 on SNS seems to signify a shift from the focus on the protection of privacy/private sphere to a focus on harm, as the key determinant becomes the number of people to which data are disclosed.

19 01189/09/EN WP 163.

20 00264/10/EN WP 169.

21 0737/EN WP 148.

22 14/EN WP 219.

would have been the only controller, the question is what should be the legal status of the processor, which has to process data at the instruction of the data controller and, inter alia, has to report on potential leaks.

17 **Joint controllership:** By far most references by the WP29 and the EDPS in respect of the household exemption is to cases in which, would the household exemption not apply, there would be joint controllership**.** Such is the case with SNS, IoT devices and other products or services that a citizen may use for personal activities. Interestingly, both advisory bodies are often ambivalent as to whether the household exemption applies.[23] When the user can rely on the household exemption, both advisory bodies point out, such does not have an effect on the legal status of the joint controller (e.g. the SNS or the party to which the data of IoT devices are sent). This is understandable, because these parties process the data for their own interests, be it commercial, be it otherwise. Yet, it does raise the question where the boundary should be drawn. For example, suppose a non-for-profit-foundation was set up with the sole purpose of the processing personal data for personal activities by citizens, would such processing also not fall under the household exemption? In addition: to what extent can the joint controller (e.g. the social media platform) be held accountable for the activities of citizens relying on the household exemption?

18 **Purposes:** Contrary to the legislative choice, the WP29 generally focusses on purposes rather than activities when determining whether the household exemption applies. What is more, it has referred not only to personal purposes, but also to family affairs and recreational purposes.[24] This raises complex issues, because when assessing SNS sites, the WP29 stressed that if citizens use the sites not so much for fun, but for productivity, to advance commercial, political or charitable goals, the household exemption would not apply.[25] This yet again brings the question to the fore where the boundary is drawn. Is saying on Facebook "I really like Emmanuel Macron's plans" personal or political and what about "Emmanuel Macron is sexy and hot" or "I think Emmanuel Macron has leadership skills"? All concern processing personal data of Emmanuel Macron, but the purpose behind the statement is not always clearcut. At least two rationales have played a role in the legislative process of the DPD (minimal harm for the "data subject" and the private sphere of the "data controller", both between brackets because the data protection regime does not apply when the household exemption applies). Suppose A places a photo on a social network where a person's child can be seen in an embarrassing situation and B states on a blog "I think we should vote for Emmanuel Macron". If the rationale behind the household exemption should be understood as that no harm is typically done by private processing activities, then A's expression seems potentially more harmful than B's, but if it concerns activities that normally fall under the right to private life, it is A's expression that could fall under the household exemption, while B's would normally not. Interesting in this respect is the discussion of the WP29 on IoT devices, and the fact that it does not answer questions such as:[26] is a smart refrigerator that automatically orders a bottle of milk considered a (exclusively) household activity or a (partially) commercial activity?

19 **Sphere:** The WP29 does not exclude that when data are made available in open access databases for re-use, individuals that harvest that data for personal activities could rely on the exemption.[27] This is remarkable, because the CJEU has stressed that gathering personal data from the public domain does not fall under the household exemption (next sub-section). A bit puzzling as well is the remark by the WP29 on video surveillance. It points out that premises other than those related to one's household—such as hotel rooms, offices, restrooms, cloakrooms, in-house phone booths, etc.—are to be regarded as private premises. It is unclear how this remark should be interpreted, whether it means, for example, that there are limits to putting camera surveillance in hotel rooms by hotel owners, or the other way around, that citizens monitoring a hotel room for private purposes (e.g. to protect their private property) fall under the household exemption.[28] If the latter, the question is how the situation in which a cleaning person might enter the room should be assessed.[29]

23 <https://edps.europa.eu/sites/default/files/publication/10-03-19_trust_information_society_en.pdf>.

24 11580/03/EN WP 82.

25 01189/09/EN WP 163.

26 14/EN WP 223.

27 1806/16/EN WP 239.

28 11750/02/EN WP 67.

29 Additionally, the WP29 suggests that if multiple houses share one common entrance, the household exemption would not apply to cameras monitoring that entrance. This means, apparently, that monitoring closed and private spheres that are co-shared by people from different households, will not fall under the household exemption. The WP29 has also stressed that the household exemption could apply to cars, as long as no personal data of third parties are processed. 17/EN WP 252.

20 **Other legal regimes:** Time and again, the WP29 makes clear that even if the household exemption applies, **other legal regimes** will still need to be respected, such as "the general (civil law) provisions safeguarding personal rights, image, family life and the private sphere – one need only think, for instance, of the visual angle of a camera installed outside the door of a flat, which may allow systematically recording the clients of a medical clinic and/or law firm located on the same floor and thereby cause undue interference with professional secrecy."[30] Although this seems obvious, at the same time, it echoes the statement by the ESC during the legislative process of the Directive. If interpreted strictly, the relevance of the household exemption might be significantly reduced as Article 8 ECHR would still be applicable as well as the tort law regime. For example, the WP29 stressed that if the household exemption does not apply to citizens that use SNS, the freedom of speech exemption in the data protection framework might. This could mean that legality of processing would be treated as a potential conflict between Article 8 ECHR and 10 ECHR.[31]

III. CJEU

21 The CJEU has issued several rulings important to understanding the household exemption.

1. Österreichischer Rundfunk

22 The case of *Österreichischer Rundfunk* was one of the first cases on the interpretation of the data protection framework. The question was posed how that framework should be understood. Is it to be regarded primarily as a framework that aims at providing protection to human rights and the interests of citizens, or is it primarily aimed at facilitating the free movement of data by removing the differences between national legal regimes in place before the Directive took effect? One of the common interpretations is that the DPD had its legal basis in the EU's competence to adopt rules to further the four freedoms (freedom of goods, capital, services, and people). One of the arguments discussed by the Court was whether the Directive could apply to situations that do not have a sufficient relationship to either one of these four freedoms. It did apply to those cases, the Court affirmed, the primarily argument being that of legal certainty; it would be difficult to assess per case which data processing operation was intended to further either one of these freedoms and how direct the link should be to be deemed sufficiently strong. But it went on to stress that moreover, the applicability of the DPD to situations where there is no direct link with the exercise of the four freedoms is confirmed by the wording of Article 3; "Those exceptions would not, at the very least, be worded in that way if the directive were applicable exclusively to situations where there is a sufficient link with the exercise of freedoms of movement."[32]

2. Bodil Lindqvist

23 The classic case concerning the household exemption is the *Lindqvist* case, where a person posted information about others on a public website. Again, the argument was furthered that the data protection framework only applied to the processing of personal data for economic purposes. Interestingly, this argument was not only introduced by the defendant, but also accepted by the respondent state, Sweden. Although stressing that the publication of data on the internet would not fall under the household exemption strictly speaking, it found "that loading personal data on a home page set up by a natural person exercising that person's own freedom of expression and having no connection with any professional or commercial activity does not fall within the scope of Community law."[33] Similarly, the Advocate General found that the processing by Mrs Lindqvist went beyond her personal and domestic circle, but he also agreed "with Mrs Lindqvist that the processing in question was carried out 'in the course of an activity which falls outside the scope of Community law'. In that connection, I note that in fact the home page in question was set up by Mrs Lindqvist without any intention of economic gain, solely as an ancillary activity to her voluntary work as a catechist in the parish community and outside the remit of any employment relationship. [I]t seems to me to be abundantly clear that Article 3(2) of the Directive would be completely meaningless if all activities, even non-economic activities, for which people used telecommunications or other services were to be regarded as falling within the scope of Community law."[34]

24 The Court, however, rejected that approach, essentially repeating its findings from *Österreichischer Rundfunk*. It also found that it was clear that the household exemption could not apply in this case, for which it gave no arguments, but only a staccato

30 11750/02/EN WP 67.

31 01189/09/EN WP 163.

32 ECLI:EU:C:2003:294.

33 ECLI:EU:C:2002:513.

34 ECLI:EU:C:2002:513.

statement: "Charitable or religious activities such as those carried out by Mrs Lindqvist cannot be considered equivalent to the activities listed in the first indent of Article 3(2) of Directive 95/46 and are thus not covered by that exception. [...] That exception must therefore be interpreted as relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people."[35] What makes the argument complex is that what is understood by the CJEU as activities carried out in the course of private life of individuals is very narrow and in sharp contrast with that the European Court of Human Rights (ECtHR), which has left the interpretation of the right to privacy as a negative right decades ago. The ECtHR has found that communicating with loved ones and expressing oneself in public and in work, among many other things, is part and parcel of a person's private life.

3. Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy

25 In *Tietosuojavaltuutettu*, the CJEU stressed that the household exemption "must be interpreted as relating only to activities which are carried out in the course of private or family life of individuals. That clearly does not apply to the activities of Markkinapörssi and Satamedia, the purpose of which is to make the data collected accessible to an unrestricted number of people."[36] Thus, the Court referred to family life, and not only private life, as a relevant determinant. While in the *Lindqvist* case, the CJEU referred to the household exemption not being applicable because the data were disclosed to an "indefinite number of people", here it spoke of "an unrestricted number of people".[37] The Working Party 29 has used an even broader term, namely a "high number of contacts".[38]

26 It is not only remarkable that the distinct change in scope of the household exemption is explicitly mentioned in the DPD as an example of an activity where the household exemption applies but also that the example of communication of data through correspondence is provided. It could be argued that disclosing something on a publicly accessible internet page is something qualitatively different than normal correspondence, because such is traditionally addressed at a specific audience. But if a person sends an e-mail to 1000 of her friends in BCC, would that still fall under the household exemption? Or suppose that at a party of 500 guests, an electronic message board provides the marital status of the participants, at the volition of all of them, would such processing be considered falling inside the data protection directive? What if the party is open to anyone, i.e. not on invitation?[39]

4. Rynes

27 Together with *Lindqvist*, the case of *Rynes* has had the biggest impact on the interpretation of the household exemption. It concerned a private person that made recordings of his home and the immediate surroundings after he had experienced a long period of aggression from unidentified individuals. The records indeed helped to identify the perpetrators.[40]

28 The AG found that the exemption must be narrowly construed and that personal activities are activities that are closely and objectively linked to the private

35 ECLI:EU:C:2003:596.

36 ECLI:EU:C:2008:727.

37 This may be a matter of translation. The French text speaks of indefinite. The authoritative version of the judgement is Finish and speaks of 'määrittelemättömän', meaning unspecified, indefinite, indeterminate or undefined.

38 01189/09/EN WP 163.

39 In the Google Spain case, the AG seemed to go one step further and suggested that when reading a newspaper on a tablet, the data protection framework applied, unless the reading of the news is exercised by a natural person in the course of a purely personal or household activity. This would mean that if a person reads a newspaper on her tablet at home in the course of a professional activity, for example because the financial news is relevant for her job as accountant, the data protection framework would apply in full. Opinion of Advocate General Jääskinen delivered on 25 June 2013. Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. Request for a preliminary ruling from the Audiencia Nacional. ECLI:EU:C:2013:424.

40 When assessing the applicability of the household exemption, the Czech, Italian, Polish and UK Governments felt that the exemption did and the Office, the Austrian, Portuguese and Spanish governments as well as the Commission argued that the exemption did not apply. The AG stressed with regard to the purpose of the processing that 'the scope of an EU legal instrument cannot depend on the subjective purpose of the interested party — in this case, the data controller — since that purpose is neither objectively verifiable by reference to external factors nor relevant with respect to the data subjects whose rights and interests are affected by the activity in question.' ECLI:EU:C:2014:2072. This seems to confirm the most plausible explanation for the explicit change made on this point in the text of the Directive.

life of an individual and which do not significantly impinge upon the personal sphere of others, although he agreed that these activities may take place outside the home: "'Household' activities are linked to family life and normally take place at a person's home or in other places shared with family members, such as second homes, hotel rooms or private cars." Interestingly, he marked a difference between the two activities when he noted "that the video surveillance of others, that is to say, the systematic surveillance of places by means of a device which produces a video signal which is recorded for the purposes of identifying individuals, even inside a house, cannot be regarded as *purely personal*, but that does not mean that it could not fall within the definition of household activity. Nevertheless, in my opinion, video surveillance which covers a public space cannot be considered to be a *purely household* activity, because it covers persons who have no connection with the family in question and who wish to remain anonymous."[41] What is striking is yet again how narrow the interpretation of "personal" by the AG is. Personal activities apparently do not involve relational activities and engaging with other persons. A purely personal activity apparently is something done alone.[42]

29 The Court stressed that the household exemption must be seen in light of the Charter of Fundamental Rights (CFREU), especially Article 7 and 8, and that it followed from jurisprudence that the data protection framework must be interpreted as setting out a high level of protection of citizens. Consequently, the household exemption must be interpreted "only in so far as is strictly necessary". This is an important shift vis-à-vis the *Lindqvist* case, which also dealt with the tension between the two goals of the data protection framework: the protection of individuals and facilitating the free flow of information. While in that case, there were serious pleas to keep all non-economic processing of personal data outside the scope of the data protection framework as a whole, and thus interpret the household exemption in a very wide manner, a few years later the Court takes a position on the other end of the spectrum, emphasizing only the goal of the protection of the rights and freedoms of data subjects, without mentioning the rationale of facilitating the free flow of information.

41 Opinion of Advocate General Jääskinen delivered on 25 June 2013. ECLI:EU:C:2014:2072.

42 It seems as though the AG's interpretation, in line with jurisprudence of the CJEU and the WP29's opinions, tilts towards an inclusive 'and' instead of an exclusive 'and' (even if the text mentions 'or'), meaning that in order to fall under the household exemption, it must concern both a personal and a household activity, just like for person B to enjoy her vacation, it must be both sunny and warm.

30 Interestingly, the CJEU admitted that correspondence and keeping of address books constitute a "purely personal or household activity" even if they incidentally concern the private life of other persons. The notion of "incidentally" is curiously left unexplained, but played a role later, both under the GDPR's legislative process and its implementation. In a brief statement, the Court yet again rejected the applicability of the household exemption: writing instead, "To the extent that video surveillance such as that at issue in the main proceedings covers, even partially, a public space and is accordingly directed outwards from the private setting of the person processing the data in that manner, it cannot be regarded as an activity which is a purely 'personal or household' activity for the purposes of the second indent of Article 3(2) of Directive 95/46."[43] This is a peculiar finding, because it does not put emphasis on the purposes for processing, or the type of activities, but on the sphere from which data are gathered. It thus seems to introduce a third approach to the household exemption. Also, like the AG, it seems to find that personal activities by necessity may only take place in non-public settings. How this interpretation relates to the matters of correspondence and the keeping of an address book and the fact that correspondence will often include personal data about third parties or observations about facts taken from public sphere is unclear. Why is it that when a person accidentally films her neighbour passing by her house on her way to work, this does not fall under the household exemption, but when that person describes in detail in an e-mail to a friend how she saw her neighbour limp by after a very intense medical operation, such is included under the household exemption? Or should the judgement of the Court be interpreted as meaning that such processing also cannot fall under the household exemption because it entails gathering personal data about third parties from the public sphere and automated processing of the data?[44] That would essentially make the household exemption redundant.

5. Jehovan todistajat

31 The case of *Jehovan todistajat* revolved around door-to-door preaching. Interestingly, the defendants tried to use the emphasis on the spheres instead of the type of activities, adopted in the *Rynes* case, in their favour. They argued that door-to-door preaching concerns processing of personal data in the domestic sphere, namely of the person who is visited. This argument, perhaps unsurprisingly, was rejected: "The words 'personal or household', within

43 ECLI:EU:C:2014:2428.

44 ECLI:EU:C:2014:2428.

the meaning of that provision, refer to the activity of the person processing the personal data and not to the person whose data are processed."[45] Yet this line of argumentation might complicate matters even further. Suppose person A stays over at friend B and writes an e-mail to person C, describing what a mess it is at B's home, would such not fall under the household exemption because A stays at B's home and processes personal data about B? Why would this be different, as surely, the household sphere is also meant to have friends over? Or would the Court in such a case place emphasis on the activity again, instead of the physical sphere where the activity takes place, or on the type of relationship between A, B, and C?

32 The AG found that the household exemption could not apply in *Jehovan todistajat*. Like the WP29, who had suggested to treat online expression cases as a conflict between Article 8 and 10 ECHR, the AG suggests that this case should be interpreted as a conflict between the right to privacy and data protection on the one hand and the freedom of religion on the other.[46] It found that the limitations posed on the freedom of religion in light of the data protection framework, were set out by law, served an important interest and could be deemed necessary in a democratic society: "Therefore, the protection afforded by Article 10(1) of the Charter cannot call into question the finding that the doorstep proselytising of members of the religious community is not a purely personal or household activity for the purposes of the second indent of Article 3(2) of Directive 95/46."[47] The Court, in fewer words, stressed that door-to-door-preaching may be covered by the freedom of religion, but should not be understood as a purely personal or household activity.

33 Though arguably, preaching and expressing one's faith to others is, at least to the persons concerned, a very personal activity, sharing their deepest convictions with specific others, the Court rejected this interpretation. Instead, it made a very explicit connection between the personal or household *activity* and the *purpose* of the processing as opposed to the *activity* of the processing and between the *sphere* from which data were gathered and in which it is disclosed, finding that "an activity cannot be regarded as being purely personal or domestic where its purpose is to make the data collected accessible to an unrestricted number of people or where that activity extends, even partially, to a public space and is accordingly directed outwards from the private setting of the person processing the data in that manner."[48]

34 The CJEU emphasised that the preaching was directed at people that do not share the faith of the preachers, meaning that they did not form a religious community, and that data were collected of people that had indicated they did not want to receive a visit anymore (though again it should be stressed that the preaching was intended to precisely form that sort of community). The Court made a remarkable reference to the fact that the data were also disclosed to an unlimited number of persons, which "is also clear from the order for reference that some of the data collected by the members of that community who engage in preaching are sent by them to the congregations of that community which compile lists from that data of persons who no longer wish to receive visits from those members. Thus, in the course of their preaching, those members make at least some of the data collected accessible to a potentially unlimited number of persons."[49] Is the argument here that potentially everyone could become a Jehovah's Witness and thus have access to the list of people that do not want to receive house visits, meaning that the data are disclosed to a potentially unlimited number of people?[50] That would seem a far stretch.

C. GDPR

I. Impact assessment and WP29

35 Before turning to the concrete analysis of the legislative process of the GDPR, it is important to recount two detailed assessments of the household exemption that provided the basis of the discussion, namely the Impact Assessment and an opinion by the WP29.

45 ECLI:EU:C:2018:551.

46 ECLI:EU:C:2018:57.

47 ECLI:EU:C:2018:57.

48 ECLI:EU:C:2018:551.

49 ECLI:EU:C:2018:551.

50 In the *Buivids* case, finally, the Court reaffirmed its previous position by stressing that Article 3 of Directive 95/46 must be interpreted as meaning that the recording of a video of police officers in a police station, while a statement is being made, and the publication of that video on a website, on which users can send, watch and share videos, are matters which come within the scope of that Directive. This, it found, was the case both because the video was disclosed to an unlimited number of people and because the data were gathered in a non-private setting. It used the terminology applied in the Lindqvist case, namely referencing 'an indefinite number of people' and not the wording used in Tietosuojavaltuutettu, namely 'an unrestricted number of people'. ECLI:EU:C:2019:122

36 The Impact Assessment distinguished between three core problems with the data protection framework, one of which were the difficulties for individuals in exercising their data protection rights effectively. One of the solutions it offered was to introduce legislative amendments to reinforce responsibility of data controllers, which could be done, inter alia, by clarifying the household exemption: "In this case, when the processing has no gainful interest and concerns a 'definite' number of individuals they would be totally exempted from data protection rules."[51] One of the main challenges identified was the unclarity of the legal status of citizens using SNS and their obligations within the data protection framework. It was recounted that the yardstick used by the CJEU, whether the data were disclosed to an indefinite number of people, meant that the data protection framework would apply in full, "even if the processing relates to purely non-economic, charitable and religious purposes." In practice, it found, Member States (MSs) limited the obligations of the users or even simply ignored their obligations when processing personal data on SNS, instead focusing on the responsibilities of the SNs. This meant that although there was a formal rule following from the CJEU judgement, in practice, it was not or only marginally enforced.

37 The WP29 devoted no less than 10 pages explaining why it thought the household exemption should be revised. It focussed on the relation of the household exemption vis-à-vis the rules regarding the freedom of expression and stressed that although historically, both exemptions had their clearly defined and demarcated scope, this was no longer the case: "Rather than relating to individuals' correspondence or their holding of records of addresses, for example, the queries and complaints DPAs receive increasingly concern individuals' *publication* of personal data, either about themselves or about other individuals. It would be wrong to say that all of an individual's personal online activity is being done for the purposes of journalism or artistic or literary expression. However, the advent of 'citizen' bloggers and the use of social networking sites to carry out different forms of public expression, mean that the two exemptions have become conflated."[52]

38 It stressed the variations in the implementation of the DPD by MSs, inter alia highlighting that some laws exempted personal processing from the data protection principles but not from the Data Protection Authority (DPA)'s powers of investigation. But, in par with the impact assessment, it noted that DPAs had focused their attention almost exclusively on processing done by corporate entities or by natural persons acting in a professional capacity—for example, financial advisors or doctors. It also questioned whether the rationales for introducing the household exemption were still applicable. It stressed that since the adoption of the Directive, citizens' access to information technology had expanded enormously. Consequently, while the processing of personal data by citizens used to be very limited both in terms of the amount of data, the sensitivity of the data and the potential impact of the data processing, this had radically changed, if only because data that are processed and kept privately can be instantaneously spread to an indefinite number of people with the click of a button.

39 Consequently, it suggested to revise the household exemption. One approach is to let all personal data processing fall under the scope of the data protection regime, or to have a specific set of requirements be applicable when citizens process personal data about other citizens, such as implementing light security measures, respecting some of the data subject rights, the data quality principle, the requirement of having a legal basis, and the transparency requirement. Although it saw merits in these more clear-cut approaches, it also acknowledged that it might put too high a burden on citizens, it may be undesirable for citizens to have a public authority scrutinize their dealings in private settings (one of the two original rationales for introducing the household exemption) and it might be difficult to envisage how DPAs could police individuals' affairs as the logistical and practical issues might be insurmountable.

40 That is why it favoured leaving the household exemption intact but granting DPAs the authority to assess whether it applied in specific cases. The WP29, consisting of representatives of all national DPAs, thus suggested to enlarge the powers of the DPAs. The DPAs should perform that assessment on the basis of a list of criteria, none of which were to be understood as determinative in and of themselves: (1) Are the personal data disseminated to an indefinite number of persons, rather than to a limited group of friends, family members or acquaintances?[53] (2) Are the personal data about individuals who have no personal or household relationship with the person posting it?[54] (3) Does the scale and frequency of the processing of personal data suggest professional or full-time activity?[55] (4) Is there evidence

51 Brussels, 25.1.2012 SEC(2012) 72 final.

52 <https://ec.europa.eu/justice/article-29/documentation/other-document/files/2013/20130227_statement_dp_annex2_en.pdf>.

53 Apparently, disclosing personal data to a limited group of strangers is a borderline case.

54 Note the focus on the type of relationship between the discloser and the receivers.

55 The focus on "full-time" seems peculiar, as it seems

of a number of individuals acting together in a collective and organised manner?[56] (5) Is there potential adverse impact on individuals, including intrusion into their privacy?

II. Legislative process

	Recital	Article
Directive	whereas there should be excluded the processing of data carried out by a natural person in the exercise of activities which are exclusively personal or domestic, such as correspondence and the holding of records of addresses;	by a natural person in the course of a purely personal or household activity.
Regulation	This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities.	by a natural person in the course of a purely personal or household activity.

41 The legislative process of the GDPR is relevant because, although only the relevant recital has been revised, the household exemption was one of the main battlegrounds when drafting the Regulation. Discussions under the DPD were revived and new ones introduced.[57]

42 **Gainful interest:** The initial proposal of the Commission both in the relevant recital and in the article suggested that the household exemption to apply, the activity in question should be both for exclusively personal or household activities *and* be without gainful interest. This would introduce a new criterium (the interest), seemingly very closely aligned to the purposes for which data are processed, a commercial purpose generally meaning the pursuit of a gainful interest. This suggestion, however, received quite some criticism, both from the WP29 and from Parliament. The latter, for example, made clear that there may be gainful interests involved with the processing of personal data, such as when selling private belongings to another person.[58] The examples given by the WP29 are especially illustrative, such as "where an individual sells their unwanted birthday presents on an e-commerce site is an obvious example of 'personal' gainful interest. Another example might be where a child uses the internet to raise sponsorship money for a charity run".[59] These examples seem to run counter to the CJEU judgements. When a person sells a book of Dan Brown through a website, she will process the personal data of Dan Brown and make those data available to an unlimited number of people.

43 **Professional or commercial activity:** The recital of the Commission's proposal after its reference to the gainful interest included the text, "and thus without any connection with a professional or commercial activity". Again, it met resistance and again the WP29 provided an example of why this clause should be omitted, which undermined the CJEU's jurisprudence, namely when "an individual blogs about his day to day experience of working in a floristry shop, perhaps talking about customers and other staff members. WP29 does not accept that the

to exclude the possibility of a person being full-time responsible for household activities and structurally using data processing operations to assist in that respect.

56 The question that has remain unresolved is whether this would include family members acting together.

57 As a small textual change, under the Directive, the article spoke of household activities, while the recital spoke of domestic activities. Though this had never led to confusion or debate, and although during most of the legislative process of the GDPR, this duality was not challenged, the Council suggested to speak of household activities in the recital as well. Brussels, 8 April 2016 (OR. en) 5419/1/16 REV 1. There was a suggestion by Parliament members to change 'personal' to 'private' again, just like it had originally been proposed under the Directive, in the article (remarkably, not the recital), but this amendment was not adopted. Amendment 369+677.

58 2012/0011(COD) 16.1.2013.

59 <https://ec.europa.eu/justice/article-29/documentation/other-document/files/2013/20130227_statement_dp_annex2_en.pdf>.

processing of personal data done for a purpose such as this should necessarily fall outside the exemption, simply because any internet user can read the blog. It might be better to amend the wording to say 'in pursuit of a professional or commercial objective', rather than 'in connection' with it. Thought should also be given as to whether non-commercial, non-personal activity – such as running a political campaign – also needs to be addressed. We also need to consider whether a natural person's keeping of professional contacts – ones that will not be shared or used by anyone else – is an activity that should fall outside the exemption."[60]

44 Although the introduction of the gainful interest was rejected from the final text of both the recital and the provision, the reference to "no connection to a professional or commercial activity" was retained in the recital. This is remarkable because it seems redundant. If an activity is to be for *purely* personal or household activities, it cannot also be, even partially, for professional or commercial activities. An activity can logically speaking not be fully and only A but also B, if B is not a subset of A. The new clause could perhaps have made sense when different wording was chosen; for example, the Committee on Civil Liberties, Justice and Home Affairs (CCLJHA) had suggested to refer to a professional or commercial *objective.* Then, it would mean that purely personal or household activities which have a professional commercial objective fall outside the household exemption. But the final recital uses "activity" with respect to both personal and household and with respect to professional and commercial. Perhaps the added value of the clause lies in the "connection", as some activities could in and by themselves be understood to be purely personal or household activities, but still have a connection to a professional or commercial activity. But what example the drafters of the GDPR had in mind remains unclear.[61]

45 **Examples:** The CCLJHA suggested to refer to, besides keeping an address file and correspondence, "the personal use of certain electronic services", without explaining which electronic services. Parliament members suggested, inter alia, to provide, after the example of "correspondence'", "independently by the medium used",[62] perhaps thinking of personal correspondence through SNS. A suggestion was to speak of "purely personal or family matters",[63] another amendment spoke of "exclusively personal, family-related, or domestic"[64] and a final text made mention of both family related activities and private sale.[65] All of these were rejected, which is remarkable in the case of reference to "family", because it played an important role in the interpretation of the DPD by both the WP29 and the CJEU.

46 The final version of the recital provides, besides a reference to correspondence and keeping an address book, "or social networking and online activity undertaken within the context of such activities."[66] This addition again seems to be confusing rather than clarifying. Apparently, there is a difference between correspondence and holding addresses on the one hand and social networking and online activities on the other, and apparently, the two mutually exclude each other signified by the "or". "Fishing or sporting activities" implicitly means that fishing is not a sporting activity, while e-mailing, just to provide a basic example, seems a matter of both correspondence and an online activity. What is additionally confusing is that the social networking

60 <https://ec.europa.eu/justice/article-29/documentation/other-document/files/2013/20130227_statement_dp_annex2_en.pdf>.

61 With respect to both elements, that of a gainful interest and that of professional and commercial activities, many amendments were suggested by Parliament members. One suggestion was to include as examples of exclusive processing for personal or domestic activities not only correspondence and the holding of addresses, but also private sale. Another was to fully revise the household exemption to hold 'by a natural person for a purpose which cannot be attributed either to his trade or to his self-employed professional activity'. A third suggestion was to have a separate indent in the article providing that the Regulation did not apply when personal data were processed 'by small enterprises in the course of its own exclusively activity and strict and exclusively internal use' and a recital providing 'This Regulation should not apply to processing personal data by small enterprises which are using personal data exclusively for its own business such as offers and invoices. If there is no risk for the processed personal data that no one else than the enterprise itself is handling the data, there is no need for an additional protection than securing the data for access. This exemption should not apply for Articles 15, 16 and 17.' Finally, there were proposals to add to the list of exemptions references to the processing of personal data by micro companies when in the course of their own activity and strictly for internal use, by the employer as part of the treatment of employee personal data in the employment context, by sport organisations for the purposes of prevention, detection and investigation of any violations of sports integrity linked with match fixing and doping (amendment 688), and by churches and religious associations or communities.

62 See e.g. Amendment 368.

63 Amendment 369.

64 A7-0402/2013 21.11.2013.

65 P7_TA(2014)0212.

66 Recital 18 GDPR.

and online activities can be performed "in the context" of the personal and household activities, perhaps similar to when a professional karate sportsman is sent on a Siberian fishing expedition by his trainer to practice endurance and patience. The fishing activity is not performed for its own sake, but is an ancillary activity, performed in the context of a karate training. Perhaps chatting with family members is a household activity and social networks can be used in the context of that activity.

47 **Indefinite number of people:** The unofficial leaked version of the GDPR codified the CJEU's *Lindqvist* doctrine by including a reference to the dissemination of data to an indefinite number of people. The first official draft, however, did not. Parliament members made many attempts to reintroduce this clause, in various wordings, and the CCLJHA suggested to provide in the article: "This exemption also shall apply to a publication of personal data where it can be reasonably expected that it will be only accessed by a limited number of persons".[67] These suggestions were all rejected, perhaps again due to the strong intervention by the WP29, who found it "difficult to accept that the fact that an individual makes his blog or her social networking profile available to the world at large is – in itself – a factor that means that any processing of personal data done in connection with necessarily falls outside the scope of personal or household processing."[68] The fact that indeed, no reference is made to this factor in either the recital or the article arguably means that the GDPR overrules the CJEU judgements on this point. At the same time, it is important to note that the WP29 did suggest including a reference to this element, for example in the recital, along with the other factors it had indicated as relevant but not determinative when assessing whether the exemption applies.[69]

48 **Data gathering:** It is remarkable that there was considerable discussion on the potential codification of the *Lindqvist* doctrine, but virtually none concerning the *Rynes* doctrine. There was one unsuccessful suggestion by a member of Parliament making an indirect reference to the question where data are gathered, suggesting to make reference in the recital to "purely personal or family matters that have been disclosed to them by the data subject himself or that they have received in a lawful manner."[70] It seems to imply that when data are gathered lawfully in the public domain, that is on the basis of consent or one of the other legitimate grounds for processing, such could fall under the household exemption. This would create a difficult loop, because in order to assess whether the gathering of data was legitimate, the requirements from the data protection framework would have to be assessed, and when these are met, the consequence would be that the data protection framework would not apply. Perhaps unsurprisingly, the proposal was rejected.

49 **Third parties:** The WP29 had underlined time and again that the fact that a citizen may lawfully invoke the household exemption should not have implications for third parties. This led to the inclusion in the recital of the following phrase: "However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities." Though the reason for adopting this clause seems to be to regulate situations in which, would the household exemption not apply, there would be two or more joint controllers, such as with SNS, the recital also mentions processors. Such could be relevant, for example, when a cloud provider merely stores data on behalf of a citizen, who pursues a household activity. This would mean that there would be no controller, but a processor, who has to abide by the GDPR. This complicates matters, because most obligations in the GDPR are directed at the data controller. Also, data subject rights can be invoked vis-à-vis the data controller and some of the obligations directly applicable to processors indirectly concern the data controller, such as that when a data breach has occurred, the processor must notify the data controller.[71] The recital does not provide any further clarification on this point, neither does it explain the extent to which the joint data controller can be held accountable for the actions of the natural person that can invoke the household exemption.[72]

67 A7-0402/2013 21.11.2013.

68 <https://ec.europa.eu/justice/article-29/documentation/other-document/files/2013/20130227_statement_dp_annex2_en.pdf>.

69 An approach that was also suggested by some of the members of Parliament (amendment 368).

70 Amendment 369.

71 Article 33(2) GDPR.

72 A related point is that there were suggestions to provide that even if the household exemption would apply, certain minimum data protection standards should be adhered to. <https://ec.europa.eu/justice/article-29/documentation/other-document/files/2013/20130227_statement_dp_annex2_en.pdf>. Later, members from Parliament suggested to adopt a similar clause, amendment 677. The WP29 made an interesting remark about the proposed e-Privacy Regulation, when it said that it 'should be made possible to process electronic communications data for the purposes of providing services explicitly requested by an end-user, such as search or keyword indexing functionality, virtual assis-

III. Interpretation and implementation

50 The implementation laws in the MSs mostly either adopt the wording of the GDPR or simply refer to the GDPR when it comes to the scope and limitations of the data protection regime. Inter alia dealing with the implications of the *Rynes* case, a number of countries have implemented special rules in their implementation laws concerning video surveillance or have adopted official guidelines on video surveillance. Some of these have chosen to follow the *Rynes* judgements, others seem to nuance the outcomes of that case.

51 In the first group, Austrian and Croatian data protection law deserve mention. Austria provides special rules for recording images, meaning observing occurrences in public or non-public space for private purposes, using technical devices for the processing of images. It provides that recording images is permitted if: (1) it is necessary in the vital interest of a person, (2) the data subject has consented to the processing of the data subject's personal data, (3) it is ordered or permitted by special statutory provisions, or (4) there are overriding legitimate interests of the controller or a third party in a particular case. In the latter case, relevant factors to determine the legitimacy are: (a) whether it serves the protection of persons and property, whether the recordings focus on privately owned land "except when it includes public traffic areas, which may be unavoidable to fulfil the purpose of the image recording", or (b), perhaps thinking of drones used to make landscape recordings, whether it serves a private documentary interest and does not aim to record uninvolved persons to identify or to record them, in a targeted manner, or (c), directly referring to the *Rynes* judgement, when "it is required for the precautionary protection of persons or items in publicly accessible places that are subject to the controller's right to undisturbed possession because that right has already been infringed or because the place, by its nature, has a special risk potential".[73]

52 Croatian law provides that the processing of personal data through video surveillance may be carried out only for the purpose necessary and justified for the protection of persons and property, if the interests of respondents who are in conflict with the processing of data through video surveillance do not prevail. Video surveillance may include premises, parts of premises, external surface of a building, as well as internal space in public transport.[74] Both the Croatian and the Austrian law follow the GDPR and the *Rynes* doctrine in the sense that these types of video surveillance in the public domain are said to fall under the scope of the data protection regime but can still be deemed legitimate when certain criteria are met.

53 A different approach is taken by the Latvian legislator, providing that the data protection regime shall not apply to data processing that natural persons conduct by using automated data recording facilities in road traffic, for personal or household purposes. It does clarify, nevertheless, that it shall be prohibited to disclose the records obtained in road traffic to other persons and institutions, except for the cases when any of the grounds for data processing specified in the data protection legislation are present. Secondly, it provides that the data protection regime shall not apply to data processing which natural persons conduct by using automated video surveillance facilities for personal or household purposes: however, "Surveillance of public space on a large scale or cases when technical aids are used for structuring of information shall not be considered as data processing for personal or household purposes."[75] The latter negation seems to imply, a-contrario, that when the public domain is not monitored on a large scale or when no technical aids are used for structuring the data, the data protection regime would not apply. A similar approach seems to be taken in the official guidelines on camera surveillance in the Netherlands: "A person that wants to attach a camera to his jacket (a so-called 'bodycam') and use it to film the environment for himself when he is walking on the street. Other people will also be portrayed on these images. This is for personal or household use only, because this person does not pass on the camera images to third parties. The provisions of the [Dutch Data Protection Framework] therefore do not apply."[76]

54 In an opinion, the EDPB reaffirmed all of the relevant factors set out by the WP29. It also gave illustrative examples: "A tourist is recording videos both through his mobile phone and through a camcorder to document his holidays. He shows the footage to

tants, text-to-speech engines and translation services. This requires the introduction of an exemption for the analysis of such data for purely individual (household) usage, as well as for individual work related usage.' 17/EN WP 247. Thus, it seemed to advocate for a broader scope of the household exemption, at least for the e-Privacy regime, also covering work related usage.

73 <https://www.jusline.at/gesetz/dsg/paragraf/artikel2zu13>.

74 <https://narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html>.

75 <https://likumi.lv/ta/en/en/id/300099-personal-data-processing-law>.

76 Cameratoezicht Beleidsregels voor de toepassing van bepalingen uit de Wet bescherming persoonsgegevens en de Wet politiegegevens.

friends and family but does not make it accessible for an indefinite number of people. This would fall under the household exemption. Example: A downhill mountainbiker wants to record her descent with an actioncam. She is riding in a remote area and only plans to use the recordings for her personal entertainment at home. This would fall under the household exemption. Example: Somebody is monitoring and recording his own garden. The property is fenced and only the controller himself and his family are entering the garden on a regular basis. This would fall under the household exemption, provided that the video surveillance does not extend even partially to a public space or neighboring property."[77] It seems that the EDPB, like the WP29, tries to nuance the *Rynes* judgement by suggesting that when personal data are gathered from the public domain, but not made accessible to an indefinite number of people, such could still fall under the household exemption.[78]

55 Finally, there was a petition for information from the Commission on the household exemption. The petitioner argued in favour of broadening the scope of application of activities of a purely personal or domestic nature so as to include all acts carried out by natural persons that by their nature do not intend to violate the rights of a data subject without a valid reason and to allow data processing by natural persons in all cases as required for the purpose of reasonably reporting breaches or offences under the laws of MS. Remarkably, the Commission again focussed on the notion of controllership and linked this to commercial and professional activities: "Situations in which natural persons could act as controllers are when they process personal data in connection with their professional or commercial activities. Examples would be a medical doctor in private practice documenting treatment administered, or a sole trader processing personal data as part of delivering the services they offer."[79] Thus, while the CJEU in *Österreichischer Rundfunk* and *Bodil Lindqvist*, found that the data protection also applied to situations in which personal data are processed for non-commercial or non-economic activities, now, at least with respect to data controllers that are natural persons, the Commission seems to find exactly that. It does not adopt the wording of the GDPR, namely that the household exemption does not apply in case data processing has a connection to a commercial or a professional activity, but stresses that a natural person can only be a data controller when they process personal data in connection with their professional or commercial activities.

D. Analysis

56 It is clear from the previous two sections that the household exemption could merit either an authoritative explanation or a textual revision. There are three paths forward. One is leaving the current formulation of the household exemption intact, a second is deleting the household exemption altogether, and a third is maintaining a household exemption, but under a revised form. The first option, as explained in this article, does not seem to be preferable. The recital and provision in the GDPR are plagued by ambiguity, incoherence, and legal ambivalence.

57 The second option is one that should be considered. The ease with which data can be transferred from the private domain to the public domain and from one person having access to the data of millions are factors that support the deletion of the household exemption. This possibility was not foreseen when introducing the household exemption under the DPD. More generally, the classic idea of separate spheres of life has lost part of its appeal because the reality is no longer that private and personal matters only take place at home and the public sphere is exclusively utilised for professional and public activities. In addition, citizens now often possess very sensitive data about others, while in the situation in the 1990s, the envisioned data consisted mostly of address books or personal diary notes. Hence, both rationales (that of the right to

77 <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf>.

78 In addition, it seemed to accept that cameras that monitor places that family members pass by regularly, could also fall under the scope of the exemption; whether this implicitly means that this is also the case when third parties do so irregularly was left open. This point was later extended when it discussed processing of personal data by 'smart' cars, which will typically also be used to transport third parties, but still could be considered to fall under the household exemption. <https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202001_connectedvehicles.pdf>. How this relates to taxi drivers was left open. The example also raises the question whether, when a person is using spyproducts in her home, the household exemption would apply when a friend comes over. Although some of the CJEU's statements would suggest that 'personal' is per definition 'alone' and 'household' is per definition restricted to 'family members', the WP29 and the EDBP seem to adopt a broader approach. Some DPAs have taken a strict approach to the household exemption. See e.g.: <https://gdprhub.eu/index.php?title=Pers%C3%B3nuvernd_(Iceland)_-_2021010073&mtc=today>. <https://edpb.europa.eu/sites/default/files/article-60-final-decisions/es_2010_10_right_to_erasure_transparency_and_information_decisionpublic_redacted.pdf>.

79 <https://www.europarl.europa.eu/doceo/document/PETI-CM-719902_EN.pdf>.

privacy and the minimal harm) for introducing the exemption are not as forceful now as they used to be.

58 In addition, it might be wondered whether with the introduction of new processing techniques, there is a case to be made for more regulation in the private sphere. Suppose a person stores private photographs of his ex-girlfriend on his computer, with which he then produces a deepfake video in which she performs all kinds of perverse sexual acts. He tells his friends about it, who also communicate this to her. This is just one of the many possible examples of deepfake applications that cannot be addressed under the GDPR. The production of compromising material and the possession of it are not covered by the GDPR. Once the material is on the internet or distributed to large groups of friends it is, but by then it is too late. The damage has already been done; compromising videos can attract thousands or millions (in the case of celebrities) of viewers within hours. It may often be impossible to take that video down permanently, because of the ease with which a copy of the video can be produced. Consequently, it could be considered to limit the household exemption, both because such behaviour is deemed intrinsically immoral and because it might prevent damage from materialising and allow DPAs to address potentially harmful material at the source.

59 On the other hand, however, it is questionable how realistic it is to ask of DPAs to monitor the private sphere of citizens, as they already suffer from a lack of manpower and resources. Omitting the household exemption might lead to an even bigger enforcement gap, as DPAs will generally choose not to monitor the private lives of citizens in detail. If they would in fact monitor the private lives of citizens, the cure might be worse than the disease, as the government would start monitoring in detail the behaviour of its citizens. Finally, as to the harm, it might be argued that there is no harm done with processing of personal data, as long as the data stay in the private sphere and limited to a limited number of people. Creating a deepfake porn of someone else, for example, might be likened to a person fantasizing about another or making an explicit drawing of her.

60 A third option would be revising the household exemption. This option could again be subdivided in three potential strategies.

1. Focussing on likely harm and potentially requiring a pre-DPIA;

2. Focussing on one of the five factors distinguished or using a combination between two or more of those factors;

3. Making a list of relevant but non-decisive factors that should be taken into account when assessing whether the household exemption applies.

61 A rudimentary formulation of these alternatives could take the following form (see table next page):

	Recital	**Article**
GDPR	This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities.	by a natural person in the course of a purely personal or household activity
Alternative 1	-	-
Alternative 2a	This Regulation does not apply to the processing of personal data by a natural person when such is unlikely to cause harm. The natural person shall make an assessment of the likely harm before commencing the data processing personal data.	by a natural person when such is unlikely to cause any harm;
Alternative 2b	This Regulation does not apply to the processing of personal data by a natural person or SME when such is unlikely to cause harm. The natural person or SME shall make an assessment of the likely harm before processing personal data.	by a natural person or SME when such is unlikely to cause any harm;
Alternative 3a	This Regulation does not apply to the processing of personal data by a natural person for personal purposes.	by a natural person for personal purposes;
Alternative 3b	This Regulation does not apply to the processing of personal data by a natural person for personal activities.	by a natural person in the course of personal activities;
Alternative 3c	This Regulation does not apply to the processing of personal data by a natural person in her private sphere.	by a natural person in her private sphere;
Alternative 3d	This Regulation does not apply to the processing of personal data when such data are gathered from and processed in her private sphere.	by a natural person when such data are gathered from her private sphere and processed in that sphere;
Alternative 3e	This Regulation does not apply to the processing of personal data when such data are not disseminated to a large group or unlimited number of people.	by a natural person when such data are not disseminated to a large group or unlimited number of people;
Alternative 3f	*A combination between two or more of the alternatives 3a-3e*	*A combination between two or more of the alternatives 3a-3e*

Alternative 4	This Regulation does not apply to the processing of personal data when personal data are processed by a natural person for a personal activity. In order to determine whether this exemption applies, the following elements should be taken into account: 1. The harm likely done by the data processing operation; 2. The sphere from which the data are gathered; 3. The sphere to which the data are disseminated; 4. Whether the activities for which the data are processed are typically considered personal activities.	by a natural person for a personal activity;

62 A final assessment of the desirability of these alternatives should be made by the EU legislator. However, from the arguments and examples that have been discussed in this article, the following tentative conclusions can be drawn:

1. Data controller and processor: Maintaining the reference to the applicability of the data protection regime does not seem preferable, inter alia, because in the case of a processor that processes personal data for a citizen that can invoke the household exemption, the processor would have duties vis-à-vis a non-existent controller.

2. Purely: There are few activities/purposes that are "purely" household or personal; mostly, they are an amalgam of various types of activities and/or purposes. Consequently, it could be considered to omit this element from the final wording of the revised household exemption.

3. In the course of: The formulation in the GDPR speaks of data processing "in the course of" personal or household activities. It is unclear what this term means precisely, how direct the link should be between the activity and the processing of personal data and whether processing data should be necessary for that activity. That is why it may be better to opt for a clearer formulation, such as "for".

4. Personal, household and family: The GDPR speaks of personal or household activities. In addition, the CJEU and WP29 have made reference to the family sphere/activities. It has never been clear what precisely the difference is between personal and household activities. It seems as though personal activities would include household activities, if the broader interpretation of the ECtHR is followed. In addition, it appears the very term and concept of "household" is too archaic to serve as an important legal concept. Consequently, in light of legal clarity and textual efficiency, it should be considered to only speak of personal and make clear in a recital, an explanatory memorandum or opinion what activities/purposes are regarded to be "personal".

5. Harm: The approach focussing on harm seems difficult to uphold for at least two reasons. First, one of the original rationales for introducing the household exemption was the minimal harm that processing of personal data in the private sphere did, while this rationale has moved more and more to the background, inter alia, given the technological tools that are now in the hands of ordinary citizens. Second, it would require of citizens an assessment of the likely harm entailed with their data processing operation, perhaps a pre-DPIA. It is questionable whether citizens would do such an assessment; an additional element that would need to be determined is whether such a pre-DPIA should be formalised and put on paper. If not, it is likely that citizens will use post-hoc explanations for their decisions. In addition, this alternative would require a more precise indication of what harm is. Is psychological harm enough and who decides whether such harm has been inflicted, on the basis of which criteria? What is the threshold for harm in light of the household exemption? Finally, focussing on the harm to determine the applicability of the data protection regime runs counter to the foundation of the data protection framework. Though over time, the ECtHR has expanded the scope of the right to privacy in order to include many modern-day data processing operations, the material scope of the right to privacy (Article 8 ECHR) is still different from that of data protection law. The data protection regime has a wider scope of application, for at least two reasons. First, the material scope is dependent on the definition of "personal data" which is particularly wide; though the term "private life", contained in Article 8 ECHR is also wide, the scopes of the two notions do not always overlap.

That is: not all processing of personal data will be considered affecting a person's "private life". Second, in human rights framework, a claim is assessed on both the *ratione materiae* (does the matter complained of fall under the material scope of the article invoked?) and the *ratione personae* principle (can the applicant claim to be a victim?). With respect to that second question, there is a significant threshold, as applicants must be able to show that they have suffered from direct, individualizable, and substantial harm. Under the data protection framework, both principles are merged. This means that any processing of personal data, however mundane and small, even writing in a blog post "Emmanuel Macron has blue eyes", is considered processing personal data, to which the GDPR applies. Thus, using harm as an element for determining the applicability of the data protection regime would undermine one of the core differences separating the right to data protection (Article 8 CFREU) from the right to privacy (Article 7 CFEU).

6. Focussing on the sphere from which data are gathered/in which data are processed: Only allowing the household exemption to apply when data are gathered from/processed in the private sphere of a person herself, as was suggested by the CJEU, would run counter to the very idea behind the household exemption, as it would disallow for many forms of private correspondence and writing a personal diary, namely when such is done in the private sphere of others or when such regards data taken from the private sphere of others.

7. Focussing on the sphere from which the data are gathered: Disallowing the household exemption to apply when data are gathered from the public sphere again seems to run counter to the very idea of the household exemption, as it would disallow writing observations in a diary about public events or the behaviour of people in public. Both the WP29 and MS have tried to nuance the outcome of the *Rynes* decision.

8. Relevant but non determinative factors: Alternative 4 may seem appealing at first sight, but may result in legal uncertainty and unclarity, as a significant risk may be that various national courts and DPAs may further their own interpretation.

9. Multiple determinative factors: The same applies, though to a lesser extent, to Alternative 3f.

10. SMEs: Although it is true that the inclusion of certain organisations under the household exemption was discussed both when the DPD and the GDPR, it seems to be a better option to leave the household exemption for private individuals and instead extent the exemptions for SMEs or micro-organisations form the obligations of the GDPR when deemed necessary.

63 Given these considerations, four options seem worth contemplating are:

1. Alternative 1: Deleting the household exemption. If this alternative is adopted, there should be additional provisions that relieve data controllers from obligations if they process a minimal amount of non-sensitive data. This could be done through extending the rules for SMEs already in the GDPR and by applying them to natural persons.

2. Alternative 3a (This Regulation does not apply to the processing of personal data by a natural person for personal purposes): Focussing on the type of activities. If this alternative is adopted, a list should be adopted, either by the Commission, by the EDPB or by the EU-legislator, indicating the type of activities that are typically considered personal.

3. Alternative 3b (This Regulation does not apply to the processing of personal data by a natural person for personal activities): Focussing on the purpose for processing. Again, if this alternative is adopted, a list should be adopted, either by the Commission, by the EDPB or by the EU-legislator, indicating the type of purposes that are typically considered personal.

4. Alternative 3c (This Regulation does not apply to the processing of personal data by a natural person in her private sphere): Of the alternatives 3a, 3b and 3c, perhaps 3c would be the most elegant. The only question would be whether the data are processed in the private sphere of any natural person and stay there. This would align with the two new rationales for the household exemption, namely that DPAs do not have the capacity to enforce the GDPR in the private sphere of all citizens and that even if they would, such would be undesirable. In addition, it aligns with the first rationale for introducing the household exemption, namely the protection of privacy. Finally, it may be argued that if data are indeed only processed in the private sphere, the harm is usually only minimal. If harm arises nevertheless, other legal regimes, such as tort law and criminal law would apply. Still, choosing for this alternative would defy the fact that the public and the private sphere are no longer strictly separable. Indeed, many public activities are taking place at home and that data

can be transferred from the private domain to a worldwide audience with the click of a button.

Shaping the field of EU Data Law

by **Nine Riis***

Abstract: The lawmakers in Brussels have worked relentlessly in recent years on enacting legislation targeting data. Yet, data legislation and the associated research have so far been conducted through the lenses of traditional fields of law, such as copyright law and fundamental rights law. While some authors do use the term "EU data law", almost no works exist that elaborate on the term and set out the value in conceptually working with an independent field of EU data law. To bridge this gap, the article demonstrates how EU data law can be classified as an autonomous legal field pursuant to the theory of factual classification. Furthermore, it shows how EU data law diverges from adjacent legal fields by striving to safeguard five distinct objectives stemming from data's particular characteristics. The objectives can be summarised as protection of the following: (i) a competitive market, (ii) fundamental rights, (iii) consumers, (iv) trustworthiness and (v) Open Data. The article argues that to effectively create, interpret and enforce data legislation, it is necessary for the EU lawmaker to take into account all of these objectives, thus making classification an essential tool for ensuring a coherent body of data legislation. Moreover, the article advances that there is a dichotomy within EU data law between economic goals and fundamental rights. While such a dichotomy is not an issue in itself, it is problematic if it is not taken adequately into account by the legislator when proposing and enacting data legislation. The article concludes that the EU legislator must actively acknowledge the effects of the dichotomy in order to ensure a coherent data legislation capable of sustaining a digital European society.

Keywords: data; data law; classification; economic goals; fundamental rights

Recommended citation: Nine Riis, Shaping the field of EU Data Law, 14 (2023) JIPITEC 54 para 1.

A. Introduction

1 The EU legislator has developed an avid interest in regulating data. The lawmakers in Brussels spare no time and they propose and enact new legislation targeting data at an unprecedented speed. Since 2018, the GDPR,[1] NPDR,[2] P2B Regulation,[3] Open Data Directive,[4] Data Governance Act[5] and Digital Markets Act[6] have

* PhD Fellow at the Centre for Private Governance at the Faculty of Law, University of Copenhagen (nineriis@jur.ku.dk). I thank Associate Professor Sylvie Cécile Cavaleri for helpful feedback. Any errors are my own.

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2018] OJ L 119/1 (GDPR).

2 Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union [2018] OJ L303/59 (NPDR).

3 Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services [2019] OJ L186/57 (P2B Regulation).

4 Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information [2019] OJ L172/56 (Open Data Directive).

5 Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) [2022] OJ L 152/1 (Data Governance Act).

6 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 and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022]

entered into force. Moreover, proposals for the Data Act[7] and the AI Act[8] are in progress and closely followed by scores of stakeholders both inside and outside the EU.

2 Despite the flurry of regulatory activity, data legislation and the resulting extensive research on data-related issues have mainly been conducted through the lenses of the traditional legal fields.[9] The most extensive activities have been undertaken within copyright law,[10] consumer protection law,[11] competition law,[12] data protection law,[13] and fundamental rights law.[14] This is a logical development as the increased use of data impacts many different parts of our society. Yet, the approach is problematic, because each legal field has its own set of objectives and criteria for balancing such objectives against each other. When EU data regulation uncritically incorporates core elements from different legal fields, it creates an inherent tension in the legislation.[15] The tension is caused by the (often) contradictory objectives of the fields the legislator uses as steppingstones for the new legislation. Further, the approach results in a fragmented regulatory framework that governs unrelated legal issues within the same Directive or Regulation. On the whole, this obfuscates legal certainty.

3 Against this backdrop, the present article argues that EU data law is an autonomous legal field. The argument for a field of EU data law has been advanced before[16] and several authors use the term as an established concept.[17] In spite of this, there is almost no literature on the theoretical way of classifying the field and why it is valuable to treat data-related legal issues within EU data law. The present article fills this gap by using theories of classification to delimit EU data law and demonstrate that EU data law has its own objectives that diverge from those of adjacent fields of law. Further, it argues that insufficient awareness of EU data law as an independent field of law is an obstacle on the road to a coherent body of EU data legislation that can stand the test of time in the coming digital decades.

OJ L265/1 (Digital Markets Act).

7 Commission 'Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)' COM/2022/68 final (proposal for the Data Act).

8 Commission 'Proposal for a Regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts' (proposal for the AI Act).

9 Thomas Streinz, 'The Evolution of European Data Law' in Paul Craig and Gráinne de Búrca (eds), *The Evolution of EU Data Law* (Oxford University Press USA 2021) 903.

10 Directive 96/9/EC of 11 March 1996 on the legal protection of databases [1995] OJ L77/20 (Database Directive) (currently under revision see <https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-review-of-the-database-directive>accessed 20 December 2022) and proposal for the Data Act art. 35.

11 Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC [2019] OJ L136/28 (Sale of Goods Directive) and Directive (EU) 2019/770 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 [2019] OJ L136/1 (Digital Content Directive).

12 Digital Markets Act, NPDR, Open Data Directive, Data Governance Act and proposal for the Data Act (in particular, chapters 2-4).

13 GDPR.

14 Commission 'Proposal for a European Declaration on Digital Rights and Principles for the Digital Decade' COM (2022) 28 final.

15 Streinz (n 9) 903; Joan Lopez Solano and others, 'Governing Data and Artificial Intelligence for All: Models for Sustainable and Just Data Governance.' (European Parliamentary Research Service 2022) 1.

16 The following works touch upon the topic: Christian Berger, 'Property Rights to Personal Data? – An Exploration of Commercial Data Law' (2017) 9 Zeitschrift für geistiges Eigentum (ZGE) 340; Björn Steinrötter, 'The (Envisaged) Legal Framework for Commercialisation of Digital Data within the EU' in Martin Ebers and Susana Navas (eds), *Algorithms and Law* (Cambridge University Press 2020); Streinz (n 9) Streinz is the most thorough work on the topic to date. Streinz' work has a broader scope than the present article by focusing on the evolution of EU data law and on its intersection with the general regulation in the EU.

17 See, for example, the abstract of Linda Kuschel and Jasmin Dolling, 'Access to Research Data and EU Copyright Law' (2022) 13 JIPITEC; Clarissa Valli Buttow and Sophie Weerts, 'Public Sector Information in the European Union Policy: The Misbalance between Economy and Individuals' (2022) 9 Big Data & Society 2 (who defines the term in a footnote as a body of legislating in EU regulating data as an object); Neil Cohen and Christiane Wendehorst, 'ALI-ELI Principles for a Data Economy' 19.

B. Classification of the law

4 On the one hand, it can be argued that classification of the law is an irrelevant and theoretical task. Classification does not normally influence the substantive legal analysis,[18] on the contrary, legal analysis is rarely bothered by a sharp division between different fields of law. If a lawyer is tasked with drafting a contract for IT services, they need to pay heed to contract law and implications from tax, competition, data protection and intellectual property law. This arguably makes classification appear a superfluous and formalistic task.

5 On the other hand, we operate with classification almost constantly when working as both practitioners and researchers. Many law firms and research institutions are organised in departments or working groups according to specialty. Further, few lawyers see themselves as generalists but rather specialise in one or several legal fields. This has, firstly, a practical purpose. The law and the number of legal sources is virtually unlimited and without any form of system, it is nearly impossible to know where to start when encountering a legal problem.[19] In the absence of classification, it would be an insurmountable task for a lawyer to master the law[20] and for law students to effectively embark upon their studies.[21] Secondly, classification allows for the identification of the distinct objectives of a legal field.[22] The objectives of a legal field are the values and interests the field persistently strives to safeguard. It is only with awareness of these objectives that legislators, practitioners and judges know how to create, interpret and enforce the law coherently.[23] This is, in particular, relevant for EU law as the Court of Justice of the EU (CJEU) often uses a teleological method of interpretation in the case of inconsistent provisions in EU legislation.[24] Consequently, classification is crucial in the quest for legal certainty.

6 Yet, an important note in this regard is that classification is not an end in itself.[25] Rather, classification is a tool to effectively create, interpret and enforce the law. Accordingly, there is no universally correct form of classification and any attempt to identify one would be in vain. Instead, efforts should be made to argue why a specific form of classification is the most useful for creating a coherent field of law. The present article does not argue that the traditional fields of law within which data-related legal issues have so far been handled are irrelevant or obsolete. It argues that for the purpose of creating and enforcing data legislation, it is important to work within the field of EU data law to ensure that all relevant objectives are taken into account.

7 In the case of EU data law this article argues for internal factual classification based on the subject matter *data*. The classification is *internal,* because it only identifies the field of EU data law as opposed to classifying the whole of the law into different fields; the latter would take the form of *external* classification.[26] Factual classification is one of the most favoured classification forms.[27] Factual classification divides the law based on the part of social or economic life the relevant legal rules are most naturally associated with.[28] A particular relevant parameter in this regard is the subject

18 Roscoe Pound, 'Classification of Law' (1924) 37 Harvard Law Review 933, 939.

19 Alf Ross, *On Law and Justice* (Jakob vH Holtermann ed, Uta Bindreiter tr, Oxford University Press 2019) 242; Pound (n 18) 943f.

20 Ross (n 19) 242.

21 See also Pound (n 18) 944.

22 Ross (n 19) 242f Ross does not use the term objectives, but refers to the '[...] principles and ideas which express the prevailing values within the legal area [...]'.

23 See also Pound (n 18) 944 who states: 'Legal precepts are classified in order to make the materials of the legal system effective for the ends of law'.

24 Koen Lenaerts and Jose A Gutierrez-Fons, 'To Say What the Law of the EU Is: Methods of Interpretation and the European Court of Justice' (2013) 20 Columbia Journal of European Law 3, 31.

25 Pound (n 18) 944.

26 Albert Kocourek, 'Classification of Law' (1933) 11 New York University Law Quarterly Review 319, 322.

27 Authors arguing for factual classification are, for example, JA Jolowicz, 'Fact Based Classification of the Law' in JA Jolowicz (ed), *The division and classification of the law* (Butterworths 1970) 7; WL Twinning, K O'Donovan and A Paliwala, 'Ernie and the Centipede' in JA Jolowicz (ed), *Division and classification of the law* (Butterworths 1970) 29; Peter Seipel, *Computing Law - Perspectives on a New Legal Discipline* (LiberTryck 1977) 201 (naming it 'functional' classification). Please note that Seipel also reference both of the before mentioned works.

28 Note that the criteria used for factual classification vary. Jolowicz (n 27); Twinning, O'Donovan and Paliwala (n 27) 20 and; Seipel (n 27) 199f. focus more on the subject matter, for example, 'contracts' or 'computers' to which the legal rules apply, whereas Ross (n 19) 264 adopts a broader view of '[...] typical areas of life'.

matter to which the legal rules apply.[29] For example, the field of construction law is commonly delimited based on the subject matter of construction agreements. Factual classification is in contrast[30] to conceptual classification, where the latter delimits the law according to the specific characteristics of the legal norms and their underlying concepts.[31] Pursuant to conceptual classification, it could, for example, be argued that public law consists solely of rules in the form competence norms.[32] Factual classification is likely favoured due to the ease of understanding the classification for persons outside the legal field.[33] Conceptual and factual classification are not the only forms of classification but the most common ones.[34]

8 However, there is an inherent risk in using factual classification. If the law is classified according to subject matter, an unlimited number of legal fields are identifiable at the risk of rendering classification meaningless: a danger that Easterbrook warns against in his infamous article "Cyberspace and the Law of the Horse".[35] Easterbrook's main argument is that even though horses are without a doubt a particular species, cases concerning horses do not give rise to any distinct legal issues. Tort or contract law cases on horses do not examine problems different from those within general tort and contract law.[36] Consequently, such a legal field "[...] is doomed to be shallow and miss unifying principles".[37] In order to avert the danger highlighted by Easterbrook, factual classification must be supplemented by something more than subject matter. "Something more" is difficult to qualify. Assistance is offered by theorists of comparative law who have struggled with similar issues when classifying legal systems. Zweigert and Kötz argue that a specific legal system is distinguished by its *style*.[38] Zweigert and Kötz define style as, *inter alia*, the "[...] predominant and characteristic mode of thought in legal matters"[39] setting a legal field[40] apart from adjacent legal fields.[41] Arguably, the predominant and characteristic mode of thought is crystallized into the objectives of a legal field. By focusing on style, the obstacle of one-dimensional classification based only on one single criteria[42] (such as subject matter) is overcome. Accordingly, the danger of "the law of the horse" is averted.

9 Consequently, the field of EU data law is delimited based on subject matter—data—and the distinct objectives it persistently strives to safeguard. These objectives are identifiable in the data legislation proposed and enacted by the EU legislator as well as its accompanying policy documents. The objectives differ from those characterising traditional fields of law and stem from the issues created by data's particular characteristics. Data's particular characteristics and the corresponding objectives are more closely examined in the following section.

C. Delimiting the field of EU data law

I. The characteristics of data and the objectives of EU data law

10 For the purposes of this article, data is defined as "any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audiovisual recording".[43] The definition is found in several pieces of (proposed) EU legislation and is in alignment with the definitions advanced by

29 Jolowicz (n 27); Twinning, O'Donovan and Paliwala (n 27) 20 and; Seipel (n 27) 199f.

30 Note that some authors argue for an integrated form of classification that incorporate elements from both factual and conceptual classification, see Ross (n 19) 264 and to a certain extent; Seipel (n 27) 199.

31 Ross (n 19) 243; Seipel (n 27) 198.

32 Ross (n 19) 245.

33 Though Streinz does not explicitly address forms of classification, he seems to use the rationale of factual classification as well cf. Streinz (n 9) 902.

34 Ross (n 19) 243; Twinning, O'Donovan and Paliwala (n 27) 20; Seipel (n 27) 198; Note that the authors use slightly diverging terminology for the types of classification; factual classification is, for example, also known as functional classification, see, inter alia, ibid 201.

35 Frank H Easterbrook, 'Cyberspace and the Law of the Horse' [1996] University of Chicago Legal Forum 207.

36 ibid 207f.

37 ibid 207.

38 Hein Kötz and Konrad Zweigert, *An Introduction to Comparative Law* (3rd edn, 1998) 67.

39 ibid 68.

40 "Legal field" in the case of this article. Kötz and Zweigert examine "legal families".

41 Kötz and Zweigert (n 38) 68.

42 ibid 67.

43 Defined in the Digital Markets Act art. 2(19), Data Governance Act art. 2(1), and proposal for the Data Act art. 2(1). In alignment is also para. 30 of the Open Data Directive.

scholars.[44] The definition is useful and workable due to its broadness. Data can take many different forms and too narrow a definition risks inadvertently excluding some forms. Moreover, the definition emphasises that data must be *digital*, which is essential as data's value creation is intrinsically connected with digital technologies.[45] It is seldom that data in itself (and thereby the mere possession of data) generates value.[46] Generally, data's economic potential must be realised through different methods[47] where the most common is data analysis.[48] By analysing data, it is possible to derive insights with the potential of enabling better decision-making.[49] Such analysis becomes even more valuable when the analysis and the ensuing decision-making are automated as is the case with machine learning algorithms and artificial intelligence.[50] These technologies also create value as they autonomously improve themselves.[51] The value extraction from data analysis can impact both businesses, NGOs and public entities[52] and is thus extremely valuable for the EU economy. Data is therefore essential as an input to the operation and development of data analysis technologies.

11 Data differs from most other commodities in four main ways.[53] Firstly, data is *inexhaustible* meaning that it can be copied an endless number of times without being exhausted nor compromised in terms of quality.[54] It should be noted that such copying can be done at a very low cost.[55] Secondly, data is *non-rival* and can therefore be managed simultaneously by any number of users and processes.[56] Thirdly, data can be *utilised in different contexts* as the same data can constitute the input for different products and services.[57] Lastly, data-driven business models are often characterised by *network effects*[58] and *economies of scope*.[59] Network effects occur when the value of a

44 Thomas Tombal, *Imposing Data Sharing among Private Actors: A Tale of Evolving Balances* (Wolters Kluwer Law International 2022) 15 also uses the definition stated in the recently enacted and proposed data legislation. Similar definitions are advanced by; Steinrötter (n 16) 272; Thomas Hoeren and Philip Bitter, '(Re)Structuring Data Law: Approaches to Data Property' in Katrin Bergener, Michael Räckers and Armin Stein (eds), *The Art of Structuring: Bridging the Gap Between Information Systems Research and Practice* (Springer International Publishing 2019) 297f.

45 Commission 'Artificial Intelligence for Europe' (Communication) COM (2021) 205 final 2018 10; Jens Prüfer and Christoph Schottmüller, 'Competing with Big Data' (2021) 69 The Journal of Industrial Economics 967, 3; Daniel L Rubinfeld and Michal S Gal, 'Access Barriers to Big Data' (2017) 59 Arizona Law Review 339, 375ff.

46 'Measuring the Economic Value of Data and Cross-Border Data Flows: A Business Perspective', vol 297 (2020) OECD Digital Economy Papers 297 10 <https://www.oecd-ilibrary.org/science-and-technology/measuring-the-economic-value-of-data-and-cross-border-data-flows_6345995e-en> accessed 20 December 2022; Julia Wdowin and Stephanie Diepeveen, 'The Value of Data - Literature Review' (Bennett Institute for Public Policy 2020) 3 <https://www.bennettinstitute.cam.ac.uk/wp-content/uploads/2020/12/Value_of_data_literature_review_26_February.pdf> accessed 20 December 2022.

47 Wdowin and Diepeveen (n 46) 19.

48 Commission 'Towards a common European data space' (Communication) COM (2018) 232 final 2018 2f.

49 Hai Wang and others, 'Towards Felicitous Decision Making: An Overview on Challenges and Trends of Big Data' (2016) 367–368 Information Sciences 747, 750.

50 Commission 'Artificial Intelligence for Europe' (Communication) COM (2021) 205 final (n 45) 10.

51 ibid.

52 Martin Wiener, Carol Saunders and Marco Marabelli, 'Big-Data Business Models: A Critical Literature Review and Multiperspective Research Framework' (2020) 35 Journal of Information Technology 66, 67; This perspective is also emphasised in Commission 'Staff Working Document: Guidance on sharing private sector data in the European data economy' 1.

53 See also the analysis of data as a commodity in Llewellyn D W. Thomas and Aija Leiponen, 'Big Data Commercialization' (2016) 44 IEEE Engineering Management Review 74, 83.

54 Charles I Jones and Christopher Tonetti, 'Nonrivalry and the Economics of Data' (2020) 110 American Economic Review 2819, 2819 Note that the authors do not distinguish between inexhaustible and non-rival.

55 Cohen and Wendehorst (n 17) 6; Commission 'A European Strategy for Data' (Communication) COM (2020) 66 final 2020 4.

56 Cohen and Wendehorst (n 17) 6; Stefan Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools: Münster Colloquia on EU Law and the Digital Economy III* (Hart/Nomos 2017) 15; Jones and Tonetti (n 54) 2819.

57 Cohen and Wendehorst (n 17) 126; Commission 'Towards a common European data space' (Communication) COM (2018) 232 final (n 48) 10.

58 Rubinfeld and Gal (n 45) 355f; Prüfer and Schottmüller (n 45) 368. Note that these works have also been cited in; Nine Riis, 'The Duty to Supply Data under Art. 102 TFEU', *Konkurrenceretlige emner 2/2020* (Bech-Bruun 2020) 160ff.

59 Nestor Duch-Brown, Bertin Martens and Frank Mueller-

product increases proportionally with the amount of people using the product.[60] A classic example is a search engine algorithm improving in proportion with the number of entered search requests.[61] Economies of scope happen when combined analysis of several datasets yield more efficient insights than analysing each data set separately.[62]

12 The distinct characteristics of data described above create a risk of harm to different values and interests of the EU. The protection of these values and interests can be expressed as the five objectives of EU data law. Consequently, EU data law strives to safeguard (i) a competitive market, (ii) fundamental rights (iii) consumers, (iv) trustworthiness and (v) Open Data. The content of each of the objectives is elaborated on below.

1. A competitive market for data

13 The Commission has repeatedly stated that a competitive market for data must be established and protected.[63] There are many views on what constitutes a "competitive market", however, three main perspectives can be identified in relation to EU data law: (i) establishment of possibilities and incentives to trade data, (ii) removal of barriers to the internal market for data, and (iii) restrictions on large companies' use of data.

a) Establishment of possibilities and incentives to trade data

14 As stated above, data is a crucial input for the operation and development of a vast number of technologies[64] making access to data essential. One of the best ways to gain access to data is through trade, however, data trade has not sufficiently taken off in the EU and is especially lacking in B2B relations.[65] Several explanations for this can be advanced. To start, data's inexhaustible and non-rival nature makes it difficult for a contracting party to control how the data is used once it has been shared. Further, as the same type of data is usable in a variety of contexts pricing data can be complicated[66] due to the fear of losing competitive edge. Both factors minimise companies' incentives to trade data.

15 As a reaction, the Commission has introduced several legislative and non-legislative[67] initiatives. On the side of legislation, the most relevant measures are the introduction of Article 34 of the proposal for the Data Act and Chapter 3 of the Data Governance Act. Article 34 of the proposal for the Data Act stipulates an obligation for the Commission to develop non-binding model contractual terms to support companies when they draft and negotiate agreements on data access and use. The rationale of the provision is to lower transactions costs and thus increase data trade.[68] Chapter 3 of the Data Governance Act adopts a different approach by providing a voluntary scheme for certifying data intermediation services. Data intermediation services are defined as services that aim to establish a commercial relationship between "an undetermined number of data subjects or data holders on one hand and data users on the other"[69] without using the provided data[70] itself nor improving it with the aim of licensing it for profit.[71] Accordingly, certified data intermediation services have a higher level of impartiality.[72] The rationale

Langer, 'The Economics of Ownership, Access and Trade in Digital Data' [2017] European Commission, Joint Research Centre 9.

60 Riis (n 58) 160.

61 An example also mentioned in ibid 161.

62 Duch-Brown, Martens and Mueller-Langer (n 59) 9. Literature on economies of scope is extensive and further elaboration is outside the scope of this article.

63 Commission 'A European Strategy for Data' (Communication) COM (2020) 66 final (n 55) 1; Commission 'Building a European Data Economy' (Communication) COM (2017) 9 final 1; Commission 'Towards a thriving data-driven economy' (Communication) COM (2014) 442 final 2014 2.

64 Commission 'Artificial Intelligence for Europe' (Communication) COM (2021) 205 final (n 45) 10; Rubinfeld and Gal (n 45) 375ff; Tombal (n 44) 88.

65 Commission 'A European Strategy for Data' (Communication) COM (2020) 66 final (n 55) 7.

66 'Measuring the Economic Value of Data and Cross-Border Data Flows: A Business Perspective' (n 46) 32.

67 One of the non-legislative initiatives is for example the establishment of the Support Centre for Data Sharing see <https://eudatasharing.eu/> accessed 20 December 2022.

68 See also paras. 55 and 83 of the proposal for the Data Act.

69 Data Governance Act art. 2(11).

70 Data Governance Act art. 12(a).

71 Data Governance Act art. 2(11)(a).

72 This is also supported by the fact that a data intermediation service provider complying with the requirements set out in articles 11 and 12 of the Data Governance Act is allowed to use the label "*data intermediation provider recognised in*

behind the provisions is that impartiality increases trust in the intermediation services with resulting incentives to trade data through intermediaries.

b) Removal of barriers to the internal market for data

16 The EU was founded with the main aim of establishing an internal market.[73] Accordingly, there should be no barriers to the free movement of data. This is, in particular, ensured by the NPDR explicitly prohibiting data localization requirements.[74] Moreover, the GDPR ensures the free movement of personal data.[75]

c) Restrictions on large companies' use of data

17 Data markets are prone to informational asymmetry,[76] network effects (both direct and indirect)[77] and economies of scope[78] all of which can act as barriers to entry.[79] Accordingly, it is difficult for new entrants to enter and establish themselves on the market. To address the risks stemming from these market characteristics, the proposal for the Data Act and the P2B Regulation impose *ex ante* restrictions on large companies' use of data in order to prevent market foreclosure and abuse of market power.[80]

18 Articles 4 and 5 of the proposal for the Data Act oblige data holders[81] to grant data users[82] access to data generated by the users' use of a product or related service.[83] Similarly, Article 9 of the P2B Regulation sets out information obligations for online intermediation services. The information obligations include a duty to inform the users about the data the intermediation service has access to and how the data is used.

19 Both Regulations employ *ex ante* mechanisms to address barriers to entry and thus prevent strong market actors from further strengthening their position within a specific data market or use their market power to leverage their position into an adjacent market.[84] Such *ex ante* mechanisms are commonly associated with EU competition law[85] and the rationales underlying the Regulations are to a great extent similar to those in competition law. The goals of EU competition law are ambiguous, but it is generally acknowledged that they include, at least, efficiency and consumer welfare.[86] These goals

the Union" and the accompanying logo as stipulated by art. 11(9) of the Act.

73 Consolidated Version of the Treaty on European Union [2016] OJ C202/13 (TEU) art. 3(3).

74 NDPR Art. 4(1).

75 GDPR art. 1(3)

76 Bertin Martens and others, 'Business-to-Business Data Sharing: An Economic and Legal Analysis' (2020) 27.

77 Rubinfeld and Gal (n 45) 355f; Prüfer and Schottmüller (n 45) 368.

78 Rubinfeld and Gal (n 45) 352ff; Martens and others (n 76) 24.

79 Rubinfeld and Gal (n 45) 349ff.

80 See also the analysis conducted by Ondrej Blazo, 'The Digital Markets Acts - Between Market Regulation, Competition Rules and Unfair Trade Practices Rules' [2022] Strani Pravni Zivot (Foreign Legal Life) 117, 131.

81 "Data holder" is defined as: "a legal or natural person who has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation implementing Union law, or in the case of non-personal data and through control of the technical design of the product and related services, the ability, to make available certain data" cf. art. 2(6) of the proposal for the Data Act. Note that SMEs are explicitly excluded from this definition cf. proposal for the Data Act art. 7(1).

82 "User" defined in art. 2(5) of the proposal for the Data Act. Access can also be granted to a third party designated by the user cf. art. 5 of the proposal for the Data Act.

83 See art. 2(2) and 2(3) of the proposal for the Data Act for definitions for "product" and "related service".

84 Luigi Zingales, Fiona Scott Morton and Guy Rolnik, 'Stigler Committee on Digital Platforms' 336, 37.

85 An illustrative example is the electronic communications sector, which has historically been a focus of competition law due to its specific market characteristics. Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code [2018] OJ L321/36 includes *ex ante* obligations similar to those in the P2B Regulation and the proposal for the Data Act, for example, information obligations cf. art. 69 and obligations to grant access cf. art. 61.

86 See the thorough empirical analysis in Konstantinos Stylianou and Marios Iacovides, 'The Goals of EU Competition Law: A Comprehensive Empirical Investigation' [2022] Legal Studies 1, 5ff with references. The goals of EU competition law have been discussed at length, however, the discussion is outside the scope of this article.

are also evident in the Regulations as they seek to increase both efficiency and consumer welfare[87] by facilitating access to data.

2. Protection of fundamental rights

20 The increased use of data and data analysis can collide with fundamental rights, in particular, (i) the right to protection of personal data cf. Article 8 of the EU Charter[88] and (ii) the prohibition against discrimination cf. Article 21 of the EU Charter. Further, there is (iii) a risk of compromising democratic values due to large companies' access to and use of data.

a) The right to protection of personal data

21 Legislation and case-law concerned with the protection of personal data is commonly referred to as *data protection law*.[89] Data protection has historically been one of the main forms of regulation of data in the EU[90] taking off with the enactment of the Personal Data Directive[91] in 1995. The rationale behind the Directive was partly harmonisation[92] and partly that the easiness of processing data digitally made it difficult for data subjects to exercise control over their personal data.[93] In 2018, the Directive was replaced by the GDPR,[94] which ensures the continued protection of personal data[95] based on the same rationale as the Directive.[96] Yet, the GDPR includes additional obligations (and a stricter fine regime) in light of the increased risks from advanced surveillance technologies and tools facilitating unauthorised access to personal data.[97] Though the GDPR is often referred to in its capacity as a fundamental rights instrument, it also pursues an economic goal by ensuring the unrestricted movement of personal data in the EU.[98]

b) The prohibition against discrimination

22 Article 21 of the EU Charter includes a broad prohibition against discrimination applying to the Member States and the EU institutions.[99] Further, prohibitions against general and specific non-discrimination are included in secondary EU legislation[100] applying to the private sector.[101] Accordingly, non-discrimination law in the EU has a broad scope. The specific concern in regard to data is *algorithmic bias*. If the data used as input in machine learning algorithms or artificial intelligence is biased, the output risks being biased as well[102]—often articulated within data science as "Garbage in, garbage out".[103] Moreover, as the output is often used to further improve the algorithm, the bias becomes an inherent part of the design of the particular

87 P2B Regulation paras. 1 and 3 and Explanatory Memorandum to proposal for the Data Act pp. 3 and 12

88 Consolidated version of the Charter of Fundamental Rights of the European Union [2012] OJ 326/391 (EU Charter)

89 Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press 2015) 14; Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, vol 16 (Springer International Publishing 2014) 4.

90 Together with the Database Directive.

91 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 (Personal Data Directive).

92 Personal Data Directive paras. 5-7

93 Personal Data Directive para. 4. See also Lynskey (n 89) 3.

94 GDPR art. 94(1).

95 GDPR art. 1(1), 1(2), and para. 1.

96 GDPR para. 9.

97 GDPR para. 6; Commission 'Building a European Data Economy' (Communication) COM (2017) 9 final (n 63) 3.

98 GDPR art. 1(3) and para. 13.

99 Sandra Wachter, Brent Mittelstadt and Chris Russell, 'Why Fairness Cannot Be Automated: Bridging the Gap between EU Non-Discrimination Law and AI' (2021) 41 Computer Law & Security Review 105567, 6.

100 See 'Non-Discrimination' (*Commission*) <https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/know-your-rights/equality/non-discrimination_en> accessed 20 December 2022 (also cited in; Wachter, Mittelstadt and Russell [n 99] 7).

101 Wachter, Mittelstadt and Russell (n 99) 7.

102 Commission 'Building Trust in Human-Centric Artificial Intelligence' (Communication) COM (2019) 168 final 2019 6.

103 See, for example, Bertie Vidgen and Leon Derczynski, 'Directions in Abusive Language Training Data, a Systematic Review: Garbage in, Garbage Out' (2020) 15 PLOS ONE e0243300,

algorithmic model.[104] The risk is further intensified in light of the network effects and economies of scope characterising data business models as these effects tend to exacerbate the bias. Algorithmic bias may be covered by current EU non-discrimination law[105] (though no cases have been tried in front of the CJEU), however, there are still gaps as well as evidence issues particular to cases of algorithmic bias.[106] One of the initiatives to remedy this is Article 10 of the proposal for an AI Act. Article 10(3) explicitly states that training, validation and testing data used in high-risk AI systems shall be, *inter alia*, "representative".

c) Risk of compromising democratic values due to large companies' access to and use of data

23 Large companies' (especially platforms') access to and use of data may compromise democratic values. The risk is different from the competition law concern examined above. The competition law concern is based on an economic theory of harm according to which the consumer risks paying the price for the abusive behaviour of a dominant undertaking. The risks for democratic values are harder to qualify. Recent studies have highlighted that companies with access to large amounts of data can cause non-economic societal harms.[107] With a wide reach and massive data sets large companies can, for instance, provide targeted news able to deliberately influence public opinion[108] or promote specific political agendas[109] jeopardizing the democratic values of the EU.[110] Such behaviour may also infringe fundamental rights, for instance, the right to free elections.[111] The preamble to the Digital Markets Act highlight these concerns by stating that the Act "[...] pursues an objective that is *complementary to, but different from that of protecting undistorted competition on any given market*, as defined in competition-law terms, which is to ensure that markets where gatekeepers are present are and remain contestable and fair, independently from the actual, potential or presumed effects of the conduct of a given gatekeeper covered by this Regulation on competition on a given market. This Regulation therefore aims *to protect a different legal interest from that protected by those rules* and it should apply without prejudice to their application" (author's emphasis).[112] The wording underlines that the conduct of large companies does not purely give rise to economic concerns.[113] The specific provisions of the Digital Markets Act, *inter alia*, prohibits gatekeepers'[114] use of certain categories of data[115] in competition with its business users.[116] Further, it obliges the gatekeeper to provide business users with access to data that has been either provided or generated by the business users through the gatekeeper's services.[117] These obligations are similar to *ex ante* competition law mechanisms and arguably the obligations will also affect the competitive conduct of gatekeepers. However, as stated above, the Digital Markets Act has a broader scope of protection than merely competition on the market.

104 Commission 'Building Trust in Human-Centric Artificial Intelligence' (Communication) COM (2019) 168 final (n 102) 6; Commission 'White Paper on Artificial Intelligence' (White Paper) COM (2020) 65 final 2020 11.

105 Wachter, Mittelstadt and Russell (n 99) 29; Raphaële Xenidis and Linda Senden, 'EU Non-Discrimination Law in the Era of Artificial Intelligence: Mapping the Challenges of Algorithmic Discrimination' (2020) 174.

106 Wachter, Mittelstadt and Russell (n 99) 29; Xenidis and Senden (n 105) 174.

107 See, for example, John W Cioffi, Martin F Kenney and John Zysman, 'Platform Power and Regulatory Politics: Polanyi for the Twenty-First Century' (2022) 27 New Political Economy 820; 4 José van Dijck, David Nieborg and Thomas Poell, 'Reframing Platform Power' (2019) 8 Internet Policy Review; Christoph Busch and others, 'Uncovering Blindspots in the Policy Debate on Platform Power' 20ff.

108 Busch and others (n 107) 20 and 22 state that personal data can be used to provide targeted news and thus work as 'instruments for manipulation'. The quotation is taken from; van Dijck, Nieborg and Poell (n 107) 3.

109 Busch and others (n 107) 22.

110 See the values set out in art. 2 and 3 of the TEU.

111 Art. 3 of the Protocol of the European Convention on Human Rights (ascended by the EU cf. art. 6(2) of the TEU).

112 Digital Markets Act para. 11.

113 Busch and others (n 107) 17 also advance this interpretation.

114 As defined in art. 3 of the Digital Markets Act.

115 Data which has been either generated or provided by business users through their use of the core platform service (or supporting services), including data generated or provided by business users' customers cf. art. 6(2) of the Digital Markets Act.

116 Digital Markets Act art. 6(2).

117 Digital Markets Act art. 6(10).

3. Trustworthiness

24 The concept of *trust* and *trustworthiness* emerged in EU law concurrently with data-driven technologies. The Commission has emphasised that "[a] high level of trust is essential for the data-driven economy"[118] and almost all legislation regulating data put emphasis on the importance of trust.[119] The underlying rationale is that without trust in technology—and in particular trust that technology respects fundamental rights and European values—there will be no uptake in the use of such technology. Consequently, a lack of trust will prevent the effective development of a competitive EU market for data and the ensuing beneficial technologies.

4. Open Data

25 To encourage and ensure Open Data is an aim evident in EU data law. "Open Data" describes data in an open format that can be freely used, re-used and shared for both commercial and non-commercial gains.[120] Open Data has been in focus since the entry into force of the Public Sector Information Directive[121] (now the Open Data Directive) in 2003. Open Data is desirable both from a fundamental rights and a competition law perspective. Open Data can be perceived as an extension of the right to receive and impart information as set out in Article 11(1) of the EU Charter.[122] Yet, Open Data is also advantageous for competition as the sharing and free availability of data grant companies new opportunities to produce and improve products.[123] Open Data also advances the agenda of administrative law as it ensures transparency and accountability when the data relates to the public sector.[124] The two main instruments regulating Open Data is the Open Data Directive and the Data Governance Act. The Directive sets out a general obligation for Member States to ensure that documents held by public authorities[125] are re-usable for commercial and non-commercial purposes cf. Article 3. Similarly, the Data Governance Act includes an obligation for public authorities to make specific categories of data available for reuse under specific conditions cf. Article 5.

a) Consumer protection

26 Consumer protection is anchored in Article 169 TFEU[126] and in Article 38 of the EU Charter. One of the main goals of EU consumer protection law is to provide consumers with rights that enable them to establish a fair foundation for economic transactions.[127] This is, *inter alia*, obtained by granting consumers appropriate and effective remedial rights in contractual relations as protected by the Sale of Goods Directive since 1999. Yet, these rights have been under growing pressure due to the increase in generated data.[128] An example is the surge in business models based on consumers providing data as remuneration for (monetary) free services. A reaction to these business models has been a revision of the Sale of Goods Directive and the introduction of the Digital Content Directive. The Directives introduce contractual rules favourable to consumers procuring digital content, digital services[129] and physical goods interconnected with or incorporating such content or services.[130] The rationales underlying the two directives are twofold. Firstly, the quality of the provided content and services using data improve

118 Commission 'Towards a thriving data-driven economy' (Communication) COM (2014) 442 final (n 63) 3.

119 GDPR para. 7, Data Governance Act para. 23, NPDR, para. 33, P2B Regulation, para. 3, proposal for the Data Act paras. 48 and 78 and proposal for the AI Act paras. 45 and 62 Commission 'Building a European Data Economy' (Communication) COM (2017) 9 final (n 63) 3; Commission 'Towards a common European data space' (Communication) COM (2018) 232 final (n 48) 1; Commission 'A European Strategy for Data' (Communication) COM (2020) 66 final (n 55) 1 and 11; Commission 'White Paper on Artificial Intelligence' (White Paper) COM (2020) 65 final (n 104) 1.

120 Open Data Directive para. 16

121 See paras. 4 – 5 of Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information [2003] OJ L345/90.

122 Open Data Directive para. 5.

123 Open Data Directive paras. 8 – 9.

124 Open Data Directive para. 14.

125 However, several exceptions are set out in art. 1(2).

126 Consolidated Version of the Treaty on the Functioning of European Union [2016] OJ C202/47 (TFEU).

127 Agustin Reyna, Natali Helberger and Frederik Zuiderveen Borgesius, 'The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law' (2017) 54 Common Market Law Review 1427, 1427.

128 Sale of Goods Directive para. 5.

129 Digital Content Directive art. 3(1).

130 Sale of Goods Directive 2(5)(b).

as consumers can exercise remedial rights in case of non-conformity[131] leading to better products on the market. Secondly, the rules encourage consumers' trust in technologies, because consumers know that the companies providing the data-driven services are contractually liable.

D. The inherent dichotomy in EU data law and the way forward

27 By defining the field of EU data law, all the objectives concerning data deemed important by the EU legislator are fleshed out. The objectives stem from the distinct issues created by data's particular characteristics and differ from the objectives characterising traditional fields of law. Consequently, the classification of EU data law contributes to an enhanced understanding of the values and interests that are relevant to take into account when creating, interpreting, and enforcing data legislation. This, in turn, provides for a coherent field of law that ensures legal certainty.

28 When examining the objectives of EU data law, it is clear that there is an inherent dichotomy between economic goals on the one hand and fundamental rights on the other hand.[132] Data has an enormous economic potential exacerbated by its ability to make an economic impact across a vast number of industries.[133] Data-driven technologies have a broad scope; they can provide better and faster medical diagnosis,[134] improve sustainability[135] and innovate an uncountable number of products and services.[136] It is exactly the broadness of data's use that warrants the catchphrase "data is the new oil".[137] Yet, data also has the ability to compromise the democratic values upon which the EU is built and the potential to infringe fundamental rights. The extent of the risks ensuing from algorithmic bias or from large companies' potentially far-reaching power are difficult to fully comprehend as our society may be impacted in ways we cannot yet imagine. The dichotomy is also evident when considering the subjects of protection in current data legislation. Arguably, there is a difference in the approach to regulation depending on if the subject of protection is a consumer assessing a product or the public seeking to navigate in a risk zone for fundamental rights.[138]

29 Both economic goals and protection of fundamental rights are important and the legislator must decide how to balance them against each other, which the EU legislator has not sufficiently done.[139] A relevant example is the continuous distinction between personal and non-personal data in EU legislation.[140] The distinction relies on the assumption that data sets of personal and non-personal data are easily separated and that parallel application of different legal rules is possible. However, this is not necessarily aligned with reality[141] and is problematic because the stricter mandatory requirements for processing of personal data (while justifiable from a fundamental rights perspective) effectively impede data trade. Consequently, there is an ensuing risk that the legal provisions mainly pursuing economic goals cannot efficiently achieve such objective. As an illustration, Article 12 of the Data Governance Act lists the requirements that must be satisfied in order to become a certified data intermediation

131 Digital Content Directive paras. 5 and 8 and Sale of Goods Directive para. 32.

132 See also Streinz (n 9) 934 in agreement.

133 Commission 'Towards a common European data space' (Communication) COM (2018) 232 final (n 48) 2.

134 It can, for example, (earlier and faster) detect skin cancer as well as calculate the chances of relapse for certain medical conditions cf. Jenni AM Sidey-Gibbons and Chris J Sidey-Gibbons, 'Machine Learning in Medicine: A Practical Introduction' (2019) 19 BMC Medical Research Methodology 64, 2.

135 Commission 'Towards a common European data space' (Communication) COM (2018) 232 final (n 48) 2.

136 ibid.

137 'The World's Most Valuable Resource; Regulating the Data Economy' (2017) 423 The Economist.

138 Solano and others (n 15) 53.

139 ibid 1; Streinz (n 9) 903.

140 Something often noted and criticized, see, inter alia, Christiane Wendehorst, 'Of Elephants in the Room and Paper Tigers: How to Reconcile Data Protection and the Data Economy' in Reiner Schulze, Dirk Staudenmayer and Stefan Lohsse (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools: Münster Colloquia on EU Law and the Digital Economy III* (Nomos 2017); Inge Graef, Raphaël Gellert and Martin Husovec, 'Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data Is Counterproductive to Data Innovation.' 44 European Law Review 605; Inge Graef and Raphael Gellert, 'The European Commission's Proposed Data Governance Act: Some Initial Reflections on the Increasingly Complex EU Regulatory Puzzle of Stimulating Data Sharing' [2021] SSRN Electronic Journal 2 <https://www.ssrn.com/abstract=3814721> accessed 3 February 2023.

141 Graef, Gellert and Husovec (n 140) 5.

service provider.[142] Article 12 stipulates different requirements dependent on the provided data being personal or non-personal[143] requiring stricter requirements for processing personal data. However, the provision does not take into account cases of mixed datasets or cases where non-personal data becomes personal due to the dynamic interpretation of what constitutes personal data.[144] The latter situation is likely to arise due to the vast amount of different datasets available in data intermediation services. The sparse guidance in the Data Governance Act in this regard risks limiting the intended effect of Article 12 as providers may have difficulties satisfying the requirements of the provision and thus qualify for the certification.

30 It can be argued that the objective of trustworthiness can, in some cases, solve the dichotomy between economic goals and protection of fundamental rights. In other words, without fundamental rights protection (that is, *trust*) no EU citizen or company will use new technologies.[145] However, the soundness of this rationale should be subject to closer examination. It is a convenient way to solve a complex matter, but when taking into account how all of our lives (and modern comforts) depend on new forms of data-driven technology, the argument seems weak.

31 An inherent dichotomy is not detrimental to a legal field, in fact, it is what characterizes almost all fields of law. However, it is important to acknowledge a field's contrary stances and decide how to balance them against each other. This is, in particular, important when taking into account how speedily the EU legislator is proposing and passing data legislation. If the legislator does not acknowledge the different objectives of EU data law and their inherent tension, the risk is that none of the objectives will be effectively achieved. Further, legal uncertainty is increased as businesses and individuals have considerable difficulties navigating an increasing amount of legislation safeguarding opposing objectives.

32 The aim of EU data law is not to solve the dichotomy between the field's objectives. In the words of Roscoe Pound, "Classification is not an end".[146] Classification is a tool used to construct a solid foundation for creating, interpreting and enforcing the law. By classifying EU data law, the present article brings to light the field's objectives and their inherent tensions. This clarity can assist the EU legislator in making the decisions necessary for creating better and more consistent data legislation to sustain a digital European society in the coming digital decades.

142 The distinction used in art. 12 is also criticized by the European Data Protection Board and the European Data Protection Supervisor in 'EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act) (2021) 28f. Note that some of the criticism issued in the opinion have been mitigated in the final approved text of the Data Governance Act.

143 See, for example, art. 12(j) – (n) operating with the distinction.

144 Wendehorst (n 140) 331; Graef, Gellert and Husovec (n 140) 3f.

145 Commission 'White Paper on Artificial Intelligence' (White Paper) COM (2020) 65 final (n 104) 1; Commission 'A European Strategy for Data' (Communication) COM (2020) 66 final (n 55) 1.

146 Pound (n 18) 944.

The Digital Services Act: transparency as an efficient tool to curb the spread of disinformation on online platforms?

by **Alain Strowel and Jean De Meyere***

Abstract: The Digital Services Act (DSA), which aims at the creation of a safer online environment in Europe, addresses the lack of transparency in content moderation by online platforms. Therefore, the DSA imposes several new due diligence obligations. This article explores the implications of these transparency obligations on the spread of disinformation, in particular on the Very Large Online Platforms (VLOPs) that will be subject to additional scrutiny. The article highlights the potential benefits of the new regulatory framework that enables the access of vetted researchers to platforms' data, empowers users by reducing information asymmetry and mitigates certain risks. However, questions remain regarding the information overload for the regulators and the effectiveness of the future DSA enforcement. In view of the possible enforcement issues, the article proposes to go further, for example by adding a general principle of transparency (beyond the list of due diligences obligations) and by strengthening the co-regulatory and multistakeholder model of regulation (beyond what the DSA helpfully provides).

Keywords: disinformation; DSA (Digital Services Act); online platforms; transparency

Recommended citation: Alain Strowel, Jean De Meyere, The Digital Services Act: transparency as an efficient tool to curb the spread of disinformation on online platforms, 14 (2023) JIPITEC 66 para 1.

A. Introduction

1 Today, the role of platforms has become central in our life: to book a ride or a ticket, to organize travelling and accommodation, to access news or to exchange memories or thoughts, we constantly use online platforms[1]. Yet, they are notoriously opaque, in particular when ranking and propagating content and thus deciding about what we see and read (and buy, book as travel, etc.: the list is long!). While in the US, the Biden administration has announced principles to enhance platform accountability[2], the

* Alain Strowel, Professor, UCLouvain and USL-B, attorney and Jean De Meyere, PhD student, UCLouvain.

1 It is worth noting that, in 2023, the use of the term "platform" to designate, among others, the large social networks (Facebook, Instagram, TikTok, YouTube, Twitter...) is widely accepted, while, around 2015, the existence of those pivotal intermediaries, and the use of the term, were strongly opposed (for ex. by Google) and by certain researchers (see Thierry Pénard et Winston Maxwell, Réguler les plateformes: une fausse bonne idée, in L'Opinion, 23 avril 2015, at <https://www.lopinion.fr/economie/reguler-les-plateformes-une-fausse-bonne-idee>). In this paper, we focus on the very large online platforms (see below) as defined in the 2022 Digital Services Act.

2 On September 8, 2022, the White House released a statement containing some principles on platform accountability aiming, among others, to « increase transparency about platform's algorithms and content moderation decision [...] platforms are failing to provide sufficient transparency to allow the public and researchers to understand how and why such decisions [about content display] are made, their potential effects on users, and the very real dangers these

EU has recently adopted the Digital Services Act ("DSA")[3], an important piece of hard law which, among other things, imposes new transparency obligations on platforms.

2 In this contribution, we examine whether the transparency requirements of the DSA are adequate to fight the spread of online disinformation. We thus question whether the newly adopted rules are able to usefully highlight the platforms' mechanisms and (algorithmic) decisions about content prioritization and propagation, more commonly captured under the notion of 'content moderation'. Making those mechanisms and decisions more intelligible, in particular how the business choices on the platform's design influence information sharing, should facilitate the adoption of measures against some excesses in the spread of disinformation. We conclude that most of the new provisions are geared at reinforcing the 'reporting' requirements, with the risk of 'infobesity' and, in turn, of overwhelming the regulatory authorities. Some new provisions are, however, helpful in that they open the access to the content moderation mechanisms, for example to vetted researchers, but the possibility of online platforms to still hide their decisions, or to minimize their impact, behind the claimed protection of trade secrets or other concerns (as permitted by Article 40(5) DSA[4]) does not bode well for the implementation of the new rules. In the end, the efficiency of the new legal framework will mostly depend on how the enforcement mechanisms, including the Digital Services Coordinators (in particular, in the countries where the large platforms will be located) and the Commission, will put the rules into practice, and whether sufficient resources and skilled staff will be devoted to enforcement at the EU and national levels. This is not yet clear although it will be decisive for the DSA to be able to reach its objectives and to curb disinformation (and other unwanted content and behavior) on platforms.

3 At the same time, beware: the role of public authorities should remain minimal to avoid encroaching on freedom of expression, thus the measures should be the least invasive and strictly necessary to reduce the (proved) harms linked to online disinformation. Therefore, we also plead in the conclusion for the development of 'middleware'[5], i. e. a new layer of software or content-curation services that give users more control over what they see and thus allow them to customize content moderation. To moderate the online conversation so as to improve the quality of exchanges requires all parties, the platforms of course—under the right incentives from the regulators—, but also the online users, whether speakers or receivers, to participate in this joint enterprise. The empowerment of users, through technology and other design measures, is thus a necessary complement to the regulatory measures adopted in the DSA.

4 First, we start this paper with an attempt to delineate which problematic situations are covered under the term "disinformation", and we distinguish this phenomenon from other information disorders (such as misinformation, fake news, malinformation, etc.). Three different criteria, based on their relation to truth, on the intentional element, and on the potential damage, should be used to identify disinformation cases.

5 In the second part, we briefly describe the evolving liability framework for online platforms and highlight some changes brought by the DSA. As a few online platforms concentrate a large number of Internet users, their impact on the online conversation is considerable, they are the source of the problem as well as the possible solution if they are adequately incentivized to take the right (self-regulatory) measures. In relation thereto we look into the EU Code of Practice against Disinformation, a self-regulatory instrument aimed at curbing the spread of online disinformation.

6 In the third part, we focus on the DSA and present the transparency obligations imposed in particular on a new category of online intermediaries, the Very Large Online Platforms ("VLOPs") as they are called under the DSA. (In brief, those are the online platforms having more than 45 million average monthly users in the European Union). We focus on four different types of transparency obligations:

decisions may pose. » (see <https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/08/readout-of-white-house-listening-session-on-tech-platform-accountability/>)

3 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) (Text with EEA relevance) 2022 (OJ L).L277/1

4 This important Article 40, however, constitutes a major improvement over the DSA proposal whose initial Article 31 contained several loopholes.

5 Middleware has been defined in this context as "software and services that would add an editorial layer between the dominant internet platforms and internet users" (see the first Article that refers to this notion: Francis Fukuyama et alii, Middleware for Dominant Digital Platforms: Technological Solution to a Threat to Democracy, Stanford Cyber Policy Center, available, but not dated, at: <https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/cpc-middleware_ff_v2.pdf>, accessed 8 Sept. 2022; see also Daphne Keller, The Future of Platform Power: Making Middleware Work". Journal of Democracy, vol. 32, no. 3, July 2021, pp. 168-72).

transparency information-related obligations, transparency scrutiny-related obligations, reporting obligations and risk-assessment obligations. While reviewing those transparency obligations, we also look into the changes made from the initial DSA proposal of December 2020 to the regulation as adopted in 2022.

7 In the fourth and concluding part, we sketch three different paths to improve the overall framework for regulating harmful yet lawful content online: the implementation of a general transparency principle, the adoption of a co-regulatory model empowering users and third parties, such as vetted researchers and NGOs, and the creation of an independent authority in charge of regulating platforms and the conflicts arising from their use. (Indeed, we consider that the central role left to the Digital Services Coordinators constitutes the "weak link" in the new regulatory framework defined by the DSA; similarly, the role of national data protection authorities under the 2016 General Data Protection Regulation (GDPR) did not facilitate its enforcement.)

B. Disinformation: towards a definition

8 **An ancient issue.** Disinformation is not a new phenomenon. In a time of war, it takes the form of state-sponsored propaganda, as seen since the Ukraine war started[6]. Its usage can be traced as far as the battle of Actium in 31 BCE[7]—even though it is likely that disinformation was used before this. The evolution of disinformation closely follows the evolution of information itself; the more information spread, the more disinformation spread. The invention of the printing press in Europe in the 15th century and the wide development of the press during the industrial revolution allowed for a much larger dissemination of information—and disinformation—worldwide[8]. Of course, the invention of the Internet in the late 20th century caused an ever-growing dissemination of information, a phenomenon that was amplified by the emergence of the first social media platforms[9].

9 **"Fake news": too ambiguous.** The term "fake news" that was widely used by the press and the general public can cover a variety of situations, going from the honest mistake of a journalist to a campaign of invented news orchestrated by a foreign government with the goal of undermining democratic societies. It therefore appears justified to ban this term in scientific studies because it encompasses too many sorts of information disorders and speech acts (such as false statements, misdirection, biased allegations and outright propaganda) and cannot be relied on if one aims at designing effective counter-measures[10]. The weaponization of the term by various politicians, such as former US president Donald J. Trump, in order to discredit news-outlets sharing critical views, renders the term misleading[11].

10 **Constitutive elements of disinformation.** In order to correctly understand disinformation and to attempt to regulate it properly, we need a definition of disinformation. Unlike other nefarious content, such as pedo-pornography or apology for terrorism which are clearly illegal, disinformation involves what can be called "awful yet lawful" content[12]. Regulating this information disorder therefore could be incompatible with the requirements deriving from freedom of expression and of the press. The definition of disinformation at the same time must be comprehensive enough and well delineated in order to distinguish it from other disinformation

6 For a previous analysis of the Russian campaign orchestrating disinformation around the annexion of Crimea in 2014, see Sinan Aral, *The Hype Machine: How Social Media Disrupts Our Elections, Our Economy and Our Health - and How We Must Adapt* (HarperCollins Publishers Ltd 2020).

7 'Perspective | The Long History of Disinformation during War' *Washington Post* <https://www.washingtonpost.com/outlook/2022/04/28/long-history-misinformation-during-war/> accessed 26 July 2022.

8 Julie Posetti and Alice Matthews, 'A Short Guide to the History of 'fake News' and Disinformation' 20.

9 Carol A Watson, 'Information Literacy in a Fake/False News World: An Overview of the Characteristics of Fake News and its Historical Development' (2018) 46 International Journal of Legal Information 93.

10 W Lance Bennett and Steven G Livingston (eds), *The Disinformation Age: Politics, Technology, and Disruptive Communication in the United States* (Cambridge University Press 2021)., p. 193.

11 Content and Technology (European Commission) Directorate-General for Communications Networks, *A Multi-Dimensional Approach to Disinformation: Report of the Independent High Level Group on Fake News and Online Disinformation* (Publications Office of the European Union 2018) <https://data.europa.eu/doi/10.2759/739290> accessed 15 August 2022.

12 Miriam Buiten, 'Combating Disinformation and Ensuring Diversity on Online Platforms: Goals and Limits of EU Platform' (Social Science Research Network 2022) SSRN Scholarly Paper 4009079 <https://papers.ssrn.com/abstract=4009079> accessed 27 April 2022.

disorders and to avoid over-regulation of the information ecosystem.[13]

11 The assessment of disinformation must look at the nature of the content shared, at the intention or state of mind of the person circulating the content and at the effects of spreading it. First, the accuracy of the relevant information must be considered. In order to be defined as disinformation, information should be false, inaccurate or misleading[14]. But not all content lacking accuracy, or being plainly wrong, can be considered as disinformation. Second, it is important to look at the motives behind the production and distribution of the information. As the goal in the regulation of disinformation is to better protect our democracies and the public debate among citizens[15], only content that is intentionally fabricated or spread to undermine democratic values and the possibility of a reasonable debate should be qualified as disinformation. Third, disinformation supposes a will to cause public harm or to gain some advantage.[16] Quite often, the individuals who are propagating wrong information do not aim to induce harm, therefore such propagation does not involve disinformation, those persons just fall in the trap of misinformation (see below). Organizations or state-sponsored entities which disseminate false information for achieving some objectives are more likely to be involved in disinformation.

12 **Disinformation in the EU texts.** There is currently no legal definition of disinformation, and the DSA does not define what it covers—even though some of its recitals address the rise of online disinformation.[17] However, the European Action Plan for Democracy defines disinformation as: "false or misleading content that is spread with an intention to deceive or secure economic or political gain and which may cause public harm".[18] Under this definition, which we rely on in this paper, three conditions must be met for a circulating content to be considered disinformation:

- The information must be inaccurate: the truth condition;
- There must be an intent to gain economic or political gains behind the diffusion of the information: the intentionality condition;
- There must be a potential for the information to cause public harm: the public harm condition.

13 It is important to note that the third condition, the potentiality to cause public harm, is not always explicitly mentioned in the literature defining disinformation.[19] We believe the inclusion of such a condition is important as restricting lawful content without significant negative consequences on the public, for example on the cohesion of our societies, would not be proportional and therefore risks to be an unlawful restriction on freedom of expression and of the press.

14 **Disinformation v. misinformation.** Disinformation is to be distinguished from misinformation, which is defined in the European Democracy Action Plan as: "false or misleading content shared without harmful intent" but whose "effects can be still harmful".[20] With misinformation, the false/misleading content requirement and the public harm condition are met, while the condition of intent is not: the person sharing the information did not share the content with the intention to deceive or to secure economic or political gain. This is the case when a person unknowingly shares false information.

15 The remedies to misinformation partly differ from the responses to disinformation. The European Commission points out that misinformation could be more easily countered than disinformation, mostly through better communication strategies, awareness raising and increased media literacy.[21] Furthermore, overregulating speech which was not shared or produced with a malicious intent might pose an excessive risk to freedom of expression.[22] This justifies a stronger response to disinformation, in particular when orchestrated by powerful (State) actors.

13 'European Democracy Action Plan' (*European Commission - European Commission*) <https://ec.europa.eu/info/strategy/priorities-2019-2024/new-push-european-democracy/european-democracy-action-plan_en> accessed 26 July 2022.

14 Directorate-General for Communications Networks (n 11).

15 'European Democracy Action Plan' (n 13).

16 Directorate-General for Communications Networks (n 11).

17 See DSA recital 2, recital 9, recital 69, etc.

18 'European Democracy Action Plan' (n 13).

19 'Information disorder: Toward an interdisciplinary framework for research and policy making' (*Council of Europe Publishing*) <https://edoc.coe.int/fr/medias/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html> accessed 16 May 2022.

20 'European Democracy Action Plan' (n 13).

21 COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS On the European democracy action plan 2020.

22 Noémi Bontridder and Yves Poullet, 'The Role of Artificial Intelligence in Disinformation' (2021) 3 Data & Policy e32.

16 Disinformation v. parody and satire. Satire or parody, if wrongly perceived and shared, without the necessary second-degree humor and understanding, could create some information disorder. In that case, while the person sharing it does not realize that the shared content—if taken at face value—is false, or at least exaggerated, the information is generally not communicated with a malicious intent nor has the potential to cause public harm.[23] However, there have been cases where parodical or satirical content were not clearly identified as such by its author, causing confusion.[24] Politicians and public figures have also been known for sharing parodical articles from websites such as The Onion or Le Gorafi, well-known parodical websites.[25] Although the line between disinformation and parody/satire is not always clear (at least for the persons ignoring the context), it is important to keep the irreverent expression immune from legal interference, thus regulating disinformation must be adequately finetuned to preserve the room of parodical speech.

17 Disinformation v. malinformation. Malinformation is "genuine information that is shared to cause harm".[26] In that case, the truth condition is respected while the intentionality condition is not. Malinformation is not illegal *per se* but could in some circumstances constitute an illegal behavior such as harassment.[27]

18 Regulations touching upon illicit disinformation. Content that commonly qualifies as disinformation can also fall under the scope of prohibitions, for example misleading advertising.[28] Another example is the negation of the Holocaust, which is illegal under the laws of certain European countries.[29] Prohibition of these forms of disinformation is usually justified because they pose a serious threat to customers or democratic societies. The DSA will help to curb the spread of those *illicit* types of content as the DSA permits a better online enforcement of the laws banning such content.

19 Currently, the day-to-day control of online disinformation remains in the hands of private, profit-oriented actors, i.e. the social media platforms such as Meta and Google.[30] Those platforms have been accused of encouraging, by their design and decisions, the rise of disinformation.[31] In part 2 below, we briefly summarize how their business models favor the rise of disinformation. This is why some specific regulatory measures should target those online platforms with regard to disinformation, and this should be distinguished from the liability rules and processual tools for reducing illicit content online.

C. The new liability framework for platforms and some self-regulatory measures to fight disinformation

20 The conditional exemptions of liability for intermediaries still in place with the DSA. The Internet we know today is much different than that of the (early) 1990s, when the Internet was still made of a large number of small communities, for instance researchers, journalists or professionals, who were accustomed to self-regulating their expression (e.g., due to the ethical rules known and shared by them, while the "netiquette" rules never achieved the same moderating effect on the social networks' most aggressive participants). The Internet was a decentralized network without powerful

23 Christine Sinclair, 'Parody: Fake News, Regeneration and Education' (2020) 2 Postdigital Science and Education 61.

24 'Bye Bye Belgium: en 2006, le docu-fiction de la RTBF créait un électrochoc' (*RTBF*) <https://www.rtbf.be/article/bye-bye-belgium-en-2006-le-docu-fiction-de-la-rtbf-creait-un-electrochoc-9479103> accessed 16 August 2022.

25 'Quand Christine Boutin cite sans sourciller le site parodique Le Gorafi' (*LEFIGARO*, 4 February 2014) <https://www.lefigaro.fr/politique/2014/02/04/01002-20140204ARTFIG00255-quand-christine-boutin-cite-sans-sourciller-le-site-parodique-le-gorafi.php> accessed 16 August 2022.

26 'Information disorder: Toward an interdisciplinary framework for research and policy making' (n 19).

27 ibid.

28 Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') (Text with EEA relevance) 2005.

29 For ex. the Loi n° 90-615 du 13 juillet 1990 tendant à réprimer tout acte raciste, antisémite ou xénophobe.

30 Daphne Keller and Paddy Leerssen, 'Facts and Where to Find Them: Empirical Research on Internet Platforms and Content Moderation' (16 December 2019) <https://papers.ssrn.com/abstract=3504930> accessed 16 August 2022.

31 Christian Stöcker, 'How Facebook and Google Accidentally Created a Perfect Ecosystem for Targeted Disinformation' in Christian Grimme and others (eds), *Disinformation in Open Online Media* (Springer International Publishing 2020).

intermediaries dealing with the content (contrary to intermediaries such as telecom operators dealing with the network infrastructure). "The Web of the 1990s could arguably be thought of as a neutral marketplace of ideas, one in which anyone with a dial-up connection and a bit of training in HTML could write online and potentially find a modest audience".[32] Of course, it does not mean that disinformation was not already present online. But the relatively small audience at the time made online disinformation a marginal issue affecting probably only the people actively looking for this type of content.[33]

21 This situation led regulators, first in the United States and then in Europe, to take measures in order to preserve the neutrality of the Internet. Webhosts could be considered neutral actors in the digital world, as they did not interfere with the content on their networks. In the US, Section 230 of the Communications Decency Act[34] (the "Safe Harbor" clause) made websites non-liable for content posted by their users.[35] Article 14 of the eCommerce Directive contains a similar liability exception.[36] Although the online world has fundamentally changed since the 1990s, this last provision has now been inserted in Article 6 DSA showing that the same regulatory approach remains in place (the other liability exemptions have also been imported in the DSA). Nevertheless the DSA also takes into account new realities and innovates[37]: there is, for instance, a new special rule (Article 6(3)) on the hosting provider liability under consumer law (in particular distance selling); also, the new Good Samaritan provision (Article 7) will clearly encourage platforms to take voluntary measures to tackle illicit content or to comply with EU or national laws (e.g., regarding some type of *illicit* disinformation) by ensuring they can benefit from the liability safe harbors despite becoming active intermediaries; more importantly maybe, the whole chapter III of the DSA creates extensive due diligence obligations, mainly transparency requirements (which we examine in part 3 below). More action from the platforms is thus not only expected, but imposed under the DSA. With the DSA, we move from a liability-focused framework (defined early by the eCommerce directive and interpreted by the CJEU case law) to a due diligence regime; under the DSA, compliance is now key, not liability.[38] This also means that the important role of the judiciary will now be complemented (or superseded potentially) by the role of "agencies/regulators" (i. e., the Digital Services Coordinators, the Board for Digital Services and/or the Commission as the three main enforcers under the DSA).

22 **Platforms and the economy of attention.** The rise of online platforms since the 2000s has radically changed the situation for which the eCommerce framework was designed. Several companies such as Meta and Google follow an advertising-based business model that requires the collection of vast amounts of data from their users to serve targeted ads.[39] The social media companies have developed strategies aiming to maximize the engagement of their users. The more and longer attention they give to the platform, the more advertising revenues the platforms generate.[40] In order to attract visitors, platforms rank and organize the presentation of the content to make it addictive. Whether it is the search results from Google Search or a Facebook newsfeed, algorithms form an essential component of the ranking and moderating mechanisms used by platforms to determine the nature and the order of content shown to a specific user.[41] In addition, studies have shown that disinformation and polarizing content attracts more attention on online

32 Bennett and Livingston (n 10)., p. 159.

33 ibid.

34 United States: Congress: House of Representatives: Office of the Law Revision Counsel, 'Protection for Private Blocking and Screening of Offensive Material. Sec. 230', *TELEGRAPHS, TELEPHONES, AND RADIOTELEGRAPHS. Title 47* (2011th edn, US Government Publishing Office 2011) <https://www.govinfo.gov/app/details/USCODE-2011-title47/USCODE-2011-title47-chap5-subchapII-partI-sec230> accessed 16 August 2022.

35 Bennett and Livingston (n 10).

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

37 Folkert Wilman, Between preservation and clarification, The evolution of the DSA's liability rules in light of the CJEU's case law, 2 Nov. 2022, available at <https://verfassungsblog.de/dsa-preservation-clarification/>).

38 See also Miriam C. Buiten, The Digital Services Act: From Intermediary Liability to Platform Regulation, 12 (2022) JIPITEC p. 361.

39 Yongrui Duan, Yao Ge and Yixuan Feng, 'Pricing and Personal Data Collection Strategies of Online Platforms in the Face of Privacy Concerns' (2022) 22 Electronic Commerce Research 539.

40 Romain Badouard, *Les nouvelles lois du web: modération et censure* (Seuil 2020).

41 Jean-Gabriel Ganascia, *Servitudes virtuelles* (Seuil 2022).

platforms, encouraging the engagement of users and advertising revenues.[42]

23 **Platforms initiatives against disinformation.** In 2018, the revelations of a Canadian whistle-blower uncovered the Cambridge Analytica scandal[43]: this data analysis company had relied on the processing of massive amounts of personal data in order to influence electors during the 2016 US elections in favor of Donald Trump and the UK Brexit referendum.[44] The use of social media platforms by the Russian Internet Research Agency, which was able to disseminate a large amount of disinformation through online platforms during the 2016 elections, also raised suspicion against the platforms' ranking algorithms.[45] Similarly, obscure websites and bloggers are using fakes to develop a narrative above the weakness of the Taiwanese democracy and the alleged desire of Taiwanese people to join China, what might be called "cognitive warfare".[46] The COVID-19 pandemic that started in 2020 and the Russian invasion of Ukraine in 2022 were also accompanied with large campaigns of disinformation[47], putting even more pressure on the social media platforms.

24 Online platforms have responded to those criticisms by putting mechanisms in place to fight disinformation.[48] For example, online platforms work together with journalistic associations to develop fact-checking initiatives[49], but it appears that such attempts to "educate" people are not well-received and could even be counterproductive.[50] We do not review those interesting, although not fully convincing, initiatives here, but it is worth mentioning another self-regulatory scheme that applies in the EU and has been promoted by the European Commission.

25 **The EU Code of Practice on Disinformation.** More serious self-regulation measures have been adopted by platforms, such as Google or Meta, having subscribed to the EU Code of Practice on Disinformation, a strengthened version of which was issued in 2022.[51] The Code contains commitments as well as specific measures, focusing on the following areas:

- Demonetization of purveyors of disinformation;
- Transparency of political advertising;
- Ensuring the integrity of services, notably by preventing the manipulation of services for spreading disinformation;
- Empowering users, researchers and the fact-checking community;
- Strengthening the monitoring, notably by the establishment of a transparency center accessible to citizens.[52]

42 'Misinformation, Disinformation, and Online Propaganda (Chapter 2) - Social Media and Democracy' <https://www.cambridge.org/core/books/social-media-and-democracy/misinformation-disinformation-and-online-propaganda/D14406A631AA181839ED896916598500> accessed 16 August 2022.

43 In the US, this lead to the Dec. 23, 2022 settlement with the FTC, Meta having agreed to pay USD 725 million to settle a longstanding class action lawsuit accusing it of allowing Cambridge Analytica and other third parties to access private user data (see <https://edition.cnn.com/2022/12/23/tech/meta-cambridge-analytica-settlement/index.html>).

44 Christopher Wylie, *Mindf*ck: Cambridge Analytica and the Plot to Break America* (First edition, Random House 2019).

45 Renee DiResta and others, 'The Tactics & Tropes of the Internet Research Agency' [2019] U.S. Senate Documents <https://digitalcommons.unl.edu/senatedocs/2>.

46 See Anne Applebaum, China's War Against Taiwan Has Already Started. How Bejing tries to make a democracy submit without putting up a fight, The Atlantic, Dec. 14, 2022, at <https://www.theatlantic.com/ideas/archive/2022/12/taiwan-china-disinformation-propaganda-russian-influence/672453/>.

47 'Disinformation: Online Platforms Continue the Code of Practice Revision in Light of the War in Ukraine and Report on First 2022 Actions to Fight COVID-19 Disinformation | Shaping Europe's Digital Future' <https://digital-strategy.ec.europa.eu/en/news/disinformation-online-platforms-continue-code-practice-revision-light-war-ukraine-and-report-first> accessed 16 August 2022.

48 Dawn Carla Nunziato, 'Misinformation Mayhem: Social Media Platforms' Efforts to Combat Medical and Political Misinformation' (2020) 19 First Amendment Law Review 32.

49 'L'AFP monte une opération mondiale de vérification des informations' (*L'AFP monte une opération mondiale de vérification des informations*) <https://www.facebook.com/journalismproject/afp-fighting-false-news-facebook?locale=fr_FR> accessed 16 August 2022. For example, platforms put specific stamps on certain content to inform their users that it does not conform to the scientific consensus (for ex. an anti-vaccination content) or that the user who posted it is related to a certain country. See also Government and State-Affiliated Media Account Labels' <https://help.twitter.com/en/rules-and-policies/state-affiliated> accessed 17 May 2022.

50 Wen-Ying Sylvia Chou, Anna Gaysynsky and Robin C Vanderpool, 'The COVID-19 Misinfodemic: Moving Beyond Fact-Checking' (2021) 48 Health Education & Behavior 9.

51 '2022 Strengthened Code of Practice on Disinformation | Shaping Europe's Digital Future' <https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation> accessed 16 August 2022.

52 ibid..

Critics have emerged regarding the Code, for example regarding the lack of details provided by the signatories in the annual reports they have to provide under the Code's commitments.[53] The strengthened version of the Code tries to further detail how platforms should implement the measures it contains. Other critics suggest that, while the Code is an appropriate tool to make online platforms more responsible regarding disinformation, it risks giving them too much power regarding the fine-tuning of the speech controls.[54] In any case, the self-regulatory nature of the Code means that there is a lack of oversight from public authorities as well as no compliance and enforcement mechanisms. Some have suggested to reinforce the Code through co-regulative measures that could allow for a better oversight and enforcement.[55] Despite their lack of teeth, the Code's provisions have become more persuasive in practice as the Commission threatens to adopt mandatory rules of hard law.

26 Lack of transparency of online platforms. Currently, platforms have to play a quasi-regulatory role as they are the one choosing which content will or will not stay on the platform and to whom it will be distributed.[56] Their decisions still lack the required transparency as they do not motivate their decisions, leaving users in the shadow. Even the initiatives proposed by the platforms to solve that issue, such as the creation of an Oversight Board by Facebook[57], raise questions of transparency and legitimacy.

27 The European Union, with the Digital Services Act, aims to better regulate online platforms, notably through the application of several transparency obligations helping regulators and researchers altogether to better understand the architecture of online platforms. We further develop those obligations in the next section.

D. The due diligence and transparency obligations of the DSA

I. Main DSA features and place of disinformation within the DSA

28 Legislative process. The European Commission unveiled the Digital Services Act ("DSA") proposal on 15 December 2020.[58] After a rather swift negotiation period, the final version of the text was voted by the European Parliament on 5 July 2022.[59] The DSA was published on 19 October 2022[60] and shall apply from 17 February 2024.[61]

29 Objective: a safer Internet. The goal of the legislation is to ensure a safe and accountable online environment.[62] The DSA aims to "fully harmonizes the rules applicable to intermediary services in the internal market with the objective to ensure a safe, predictable and trusted online environment, addressing the dissemination of illegal content online and the societal risks that the dissemination of disinformation or other content may generate, where fundamental rights enshrined in the

53 DG for Communications Networks, Content and Technology 'Study for The "Assessment of the Implementation of the Code of Practice on Disinformation" - Final Report' <https://imap-migration.org> accessed 9 January 2023.

54 The Eu Code of Practice on Disinformation and the Risk of the Privatisation of Censorship (Routledge 2020) <https://www.taylorfrancis.com/chapters/oa-edit/10.4324/9781003037385-20/eu-code-practice-disinformation-risk-privatisation-censorship-matteo-monti> accessed 9 January 2023.

55 DG for Communications Networks, Content and Technology (n 53).

56 Rotem Medzini, 'Enhanced Self-Regulation: The Case of Facebook's Content Governance' [2021] New Media & Society 1461444821989352.

57 'Oversight Board' (*Meta*) <https://about.fb.com/news/tag/oversight-board/> accessed 16 August 2022.

58 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 2020.

59 'Digital Services: Landmark Rules Adopted for a Safer, Open Online Environment | News | European Parliament' (5 July 2022) <https://www.europarl.europa.eu/news/en/press-room/20220701IPR34364/digital-services-landmark-rules-adopted-for-a-safer-open-online-environment> accessed 26 July 2022.

60 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) (Text with EEA relevance).

61 DSA, Article 93, 2.

62 'The Digital Services Act: Ensuring a Safe and Accountable Online Environment' (*European Commission - European Commission*) <https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en> accessed 26 July 2022.

Charter are effectively protected and innovation is facilitated".[63]

30 **Tiered structure.** The DSA embraces a tiered structure: the more important the role of an online intermediary is, the more obligations it is subject to.[64] Four classes are defined in the digital services act: providers of online intermediary services[65], providers of hosting services[66], online platforms[67] and very large online platforms (VLOPs).[68] The large social networks on which disinformation circulates with potential systemic effects, such as the erosion of the trust in democracy and in the institutions, are to be considered as VLOPs (see below). With regard to VLOPs (and very large online search engines or VLOSEs[69]), the DSA will enter into force four months after their designation as such by the European Commission. On 25 April 2023, the Commission designated 17 VLOPs and 2 VLOSEs. [70]

31 **Online platforms and VLOPs.** Online platforms are defined as "a provider of a hosting service which, at the request of a recipient of the service, stores and disseminates to the public information"[71], while VLOPs are "online platforms which reach a number of average monthly active recipients of the service in the Union equal to or higher than 45 million".[72] Due to the higher systemic and societal risks VLOPs pose, the DSA imposes higher transparency obligations on VLOPs as well as specific obligations related to risk management.[73]

32 **Illegal content and disinformation under the DSA.** The DSA does not bring any modification to the liability exception granted to online intermediaries by the eCommerce directive[74], but imposes strengthened due diligences obligations on intermediaries and an obligation to delete illegal content when requested by the relevant authorities.[75] Illegal content is now defined as: "any information, which, in itself or in relation to an activity, including the sale of products or the provision of services, is not in compliance with Union law or the law of any Member State, irrespective of the precise subject matter or nature of that law".[76]

33 The DSA provisions on illegal content could directly affect the fight against disinformation if the content shared would be considered illegal speech according to the Member States' legislation. While some disinformation during an election campaign is considered illicit and banned under strict conditions in France[77], most EU Member States have not legislated on this delicate issue. (In principle, free speech is highly protected during an election period, and many excessive and inaccurate allegations made by candidates and their supporters thus pass the proportionality test). Against disinformation which remains licit, despite being wrong, the content removals' obligations of the DSA do not provide for a solution.

34 Disinformation is not completely absent from the DSA. While it lacks a definition of the term, the DSA targets the disinformation phenomenon in several recitals[78] and identifies the fight against the spread

63 DSA, recital 9.

64 Alain Strowel and Laura Somaini, 'Towards a Robust Framework for Algorithmic Transparency to Tackle the Dissemination of Illegal and Harmful Content on Online Platforms' [2021] CRIDES Working Paper <https://cdn.uclouvain.be/groups/cms-editors-crides/droit-intellectuel/CRIDES_WP_2_2021_Alain%20Strowel%20and%20Laura%20Somaini.pdf> accessed 12 April 2022.

65 DSA, Article 2 (g).

66 ibid.

67 ibid., Article 2(i).

68 ibid., Article 33.

69 ibid., Article 33. When dealing with the reinforced transparency provisions, we will refer only to VLOPS, although VLOSES are also concerned – for the present contribution, the very large social platforms (one example of VLOPS) are indeed the main propagators of disinformation (and at least more than the VLOSES).

70 ibid., Article 92, see: <https://ec.europa.eu/commission/presscorner/detail/en/IP_23_2413>.

71 ibid., art 2(i).

72 ibid., art 33.

73 Strowel and Somaini (n 64).

74 Miriam Buiten, 'The Digital Services Act: From Intermediary Liability to Platform Regulation' (Social Science Research Network 2021) SSRN Scholarly Paper 3876328 <https://papers.ssrn.com/abstract=3876328> accessed 25 April 2022.

75 DSA, Article 9.

76 DSA, Article 2 (h).

77 In 2018, one year after the presidential election, France adopted a law regulating online disinformation during elections. The actual effects on this law during the 2022 French presidential campaign are yet to be studied.

78 See DSA Recital 2, Recital 9, Recital 69, etc.: the recitals mostly consider disinformation as one of the societal risk online platforms should be aware of.

of disinformation as an objective of the regulation.[79] Notably, several transparency obligations imposed on online platforms could help understand and correct the design of online platforms in a way that could curb the dissemination of disinformation. For example, the DSA requests VLOPs to "also focus on the information which is not illegal, but contributes to the systemic risks identified in this Regulation. Providers should therefore pay particular attention on how their services are used to disseminate or amplify misleading or deceptive content, including disinformation".[80]

35 We have already established that the problem of online disinformation is reinforced by the importance of online platforms in the public debate. Therefore, we will now concentrate on the transparency obligations which are specific for VLOPs, as their impact on the public conversation is considerable. As VLOPs are also bound to the obligations imposed on other online providers, we will first briefly describe those requirements.

II. Transparency and due diligence requirements applicable to all online providers

36 **Point of contact or legal representative.** Intermediaries will have to designate a single point of contact for communication with users and Member States.[81] Intermediaries not based in the EU also have to appoint a legal representative inside the Union.[82]

37 **Terms and conditions.** Article 14 of the DSA defines specific obligations regarding the terms and conditions of online intermediaries. These should include "information on any policies, procedures, measures and tools used for the purpose of content moderation, including algorithmic decision-making, and human review as well as rules of procedure of their internal complaint handling system".[83] Those should be "set out in clear, plain, intelligible, user friendly and unambiguous language, and shall be publicly available in an easily accessible and machine-readable format".[84] Furthermore, their application should respect fundamental rights of users, including freedom of expression.[85]

38 **Reporting obligations.** Finally, Article 15 of the DSA imposes reporting obligations for intermediary services providers regarding the following information:

- Orders regarding the removal of illegal content based on Article 8 of the DSA[86];
- Information regarding their moderation practices[87], provided that they engage in such activities;
- The number of complaints received through the internal complaint-handling system[88];
- Any use of AI for the purpose of content moderation.[89]

III. Transparency and due diligence requirements applicable to hosting services (including online platforms)

39 **Notice-and-action mechanisms.** Article 16 of the DSA imposes the hosting providers to put in place notice-and-action mechanisms, allowing users to notify host of illegal content. Hosting services have to allow users to easily communicate a series of information about the content, and those notices "shall be considered to give rise to actual knowledge or awareness for the purposes of Article 6 in respect of the specific item of information concerned where they allow a diligent provider of hosting services to identify the illegality of the relevant activity or information without a detailed legal examination".[90] Hosting services also have to inform the person submitting the good reception of the notice[91] and of their decision[92] and specify if this decision was made through the use of AI.[93] Article 15 also requires hosting services to issue information on those notices as part of their reporting obligation. The fact that an obligation specific to hosting services is

79 DSA, Recital 9.

80 DSA, Recital 84.

81 DSA, Article 11 and 12.

82 DSA, Article 13.

83 DSA, Article 14.

84 ibid.

85 ibid.

86 DSA, Article 15 (a).

87 DSA, Article 15 (b).

88 DSA, Article 15 (d).

89 DSA, Article 15 (e).

90 DSA, Article 16, 3.

91 DSA, Article 16, 4.

92 DSA, Article 16, 5.

93 DSA, Article 16, 6.

contained in an article that is normally relevant to all intermediaries is regretful, as including a specific article for reporting obligation specific to hosting services would have improved clarity (see below for the same comment regarding the obligations for trusted flaggers).

40 Statement of reasons. Article 17 requires the hosting services to communicate a statement of reasons to the recipients affected by the measures restricting their usage of the service, whether it is restrictions on the visibility of the content, demonetization or suspension of the services or of the user.[94] This statement of reasons shall include information related to the impact of the decision on the relevant information as well as the facts and circumstances leading to the decision.[95] Such a statement of reasons is not necessary when the removal of content stems from the order of an official authority pursuant to Article 9 of the DSA.[96]

41 Suspicion of criminal offences. Article 18 requires hosting services who are aware of any information related to a criminal offence involving a threat to the life or safety of individuals to notify the appropriate law enforcement or judicial authorities.[97]

IV. Additional transparency and due diligence requirements applicable to online platforms

42 Internal complaint-handling systems. Article 20 requires online platforms to put in place an internal complaint-handling system against the measures taken by the platform to restrict their usage of the service, whether it is restrictions on the visibility of the content, demonetization or suspension of the services or of the user.[98] Furthermore, Article 21 allows online platforms users to rely on out-of-court settlement body which have been certified by the appropriate Digital Services Coordinator.[99]

43 Trusted flaggers. Article 22 introduces the notion of trusted flaggers, a status awarded by a Digital Services Coordinator to individuals with sufficient expertise and independence from online platforms.[100] Notices sent out by those trusted flaggers within their area of expertise should be prioritized by online platforms.[101] Trusted flaggers shall issue specific reports[102], and online platforms have to include information on trusted flaggers as part of their reporting obligation under Article 15 of the DSA.[103]

44 Reporting obligations. Article 24 imposes specific reporting obligation for online platforms. Online platforms have to report on the following information:

- Disputes submitted to out-of-court dispute settlement bodies[104];
- The number of suspension of users pursuant to Article 20 of the DSA, which requires platforms to take measures against the misuse of their services[105];
- Information on the average monthly active recipients of the service in the Union[106]; and
- Decisions and statements of reasons pursuant to Article 17, while preserving their users' privacy.[107]

45 Clear marking of advertising. Article 26 requires online platforms to provide recipients with sufficient information regarding advertising, including the clear marking of commercial communication.[108] To do so, online platforms should provide recipients with the possibility to declare whether the content they provide contains commercial communication or not.[109]

46 Recommender system transparency. Finally, Article 27 requires platforms relying on a recommender system to "set out in their terms and conditions, in plain and intelligible language, the main parameters used in their recommender systems, as well as any options for the recipients of the service to modify or influence those main

94 DSA, Article 17, 1.

95 DSA, Article 17, 2.

96 DSA, Article 17, 5.

97 DSA, Article 18.

98 DSA, Article 20, 1.

99 DSA, Article 21.

100 DSA, Article 22, 2.

101 DSA, Article 22, 1.

102 DSA, Article 22, 3.

103 DSA, Article 15, 2.

104 DSA, Article 24, 1. (a)

105 DSA, Article 24, 1. (b)

106 DSA, Article 24, 2.

107 DSA, Article 24, 5.

108 DSA, Article 26, 1.

109 DSA, Article 26, 2.

parameters".[110] Where several options are available, users should have the ability to modify their preferences at any time.[111]

V. Additional transparency and due diligence requirements applicable to VLOPs

47 **Risk management.** Articles 34 and 35 impose risk management obligations on VLOPs. The DSA, considering the social impact and means of VLOPs, mandates VLOPs to assess, manage and mitigate systemic risks. Those risks stem from the very design of platforms, based on "behavioral insight and advertising-driven business models".[112] Yearly risk assessments should address risks related to online safety, the shaping of public opinion and discourse and online trade. VLOPs should also assess the impact of their content moderation, recommender and advertising systems on systemic risks including "the potentially rapid and wide dissemination of illegal content and of information contrary to their terms and conditions".[113] VLOPs should put mitigating measures in place in order to correct the risks they have assessed and some of these measures, such as discontinuing advertising revenue for specific types of content or enhancing the visibility of authoritative information sources, could benefit the fight against disinformation.[114]

48 The final version of the text further specifies the different risks that need to be considered and adds some categories, such as negative effects related to gender-based violence or the protection of public health and imposes better accountability for risk assessments as they have to be kept by VLOPs for at least 3 years.[115] Risk mitigations measures for some situations that directly relate to information disorders, such as the circulation of deep fakes, have also been included in the regulation.[116] Deepfakes (or "manipulated image, audio or video" falsely appearing authentic or truthful) should be flagged through "prominent markings" on the platforms' interfaces, and recipients should be provided with an easy tool to communicate their inauthentic character. The obligations to adapt the content moderation processes to reduce illegal (hate) speech or cyber violence could as well contribute to reduce some verbal excesses associated with disinformation.[117] These moderation measures against unlawful expressions will prompt a reduction in awful content.

49 The Commission may issue guidelines recommending best practices and possible measures, which could shed further light on the risk assessment process as well as on the mitigating measures that could be taken by platforms.[118]

50 **Crisis response mechanism.** Article 36 of the DSA gives the possibility to the Commission to impose specific measures on VLOPs at a time of crisis.[119] "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 thereof".[120] In this situation VLOPs have to assess how their services can solve the crisis as well as apply specific measures to reduce such impact and to report on those to the Commission.[121]

51 **Independent audits.** Article 37 of the DSA requires platforms to perform independent audits of their services. The audit should give sufficient information and help inform, and, if necessary, suggest improvements, regarding compliance. Audits shall assess compliance with due diligence obligations imposed on the provider as well as the respect of any relevant code of conduct.[122] VLOPs may be forced to adopt mitigating measures in case the audit report is not satisfactory.[123]

52 In the adopted version of the DSA, the transparency obligations related to the audit of VLOPs have been reinforced. Limitations to the audit have been strongly limited: confidentiality should not be an obstacle to the audit itself.[124] Article 28 also details the various circumstances under which the audit

110 DSA, Article 27, 1.

111 DSA, Article 27, 3.

112 Strowel and Somaini (n 64).

113 DSA, Article 34, 2.

114 DSA, Article 35.

115 DSA, Article 34.

116 DSA, Article 35, 1, k.

117 DSA, Article 35, 1, c.

118 DSA, Article 35, 3.

119 DSA, Article 36, 1.

120 DSA, Article 36, 2.

121 DSA, Article 36, 1.

122 DSA, Article 37, 1.

123 DSA, Article 37, 6.

124 DSA, Article 37, 2.

should be performed, and the Commission also receives additional powers to further determine how such an audit should be realized.[125]

53 **Recommender systems.** Article 38 of the DSA reinforces Article 27 in relation to recommender systems.[126] In the original proposal, most of the requirements imposed on online platforms were contained in Article 38 and therefore limited to VLOPs. On top of the requirements set out in Article 27, VLOPs have to allow their users to provide at least one option not based on profiling for their recommender systems.[127]

54 **Additional online advertising transparency.** Article 39 of the DSA reinforces Article 26 on the advertising requirements for online platforms, by requiring VLOPs to put in place a public repository containing information related to the advertisement present on the platforms for at least one year after the last diffusion of the commercial communication.[128]

55 **Data access and scrutiny.** Article 40 imposes data access and scrutiny obligations on VLOPs. It requires platforms to "make data available for regulatory scrutiny and research through access rights".[129] Access to data for externals actors such as the Commission, the Digital Services Coordinators or the vetted researchers allows for a better monitoring of compliance as well as "to assess the risks and possible harms of the platforms' systems".[130] Data related to the risk assessment made by the VLOP may be shared with vetted researchers under certain conditions. The original DSA proposal contained several limitations to the sharing of their data by VLOPs, notably in relation to data privacy and the protection of trade secrets, limiting the efficiency of the scrutiny imposed on platforms—despite the fact that the EU Commission or vetted researchers could be bound by confidentiality agreements.[131]

125 DSA, Article 37, 3. and 7.

126 See supra, chapter 3, section d.

127 DSA, Article 38.

128 DSA, Article 39, 1.

129 Strowel and Somaini (n 64).

130 ibid.

131 ibid; on 25 April 2023, the Commission opened a consultation to obtain additional evidence from interested parties on the framework for vetted researchers's access to data from VLOPs/VLOSEs. see: <https://algorithmic-transparency.ec.europa.eu/news/call-evidence-delegated-regulation-data-access-provided-digital-services-act-2023-04-25_en>.

56 This section was reinforced in the adopted version of the DSA, including with Article 40(3) imposing on VLOPs to "explain the design, logic the functioning and the testing of their algorithmic systems, including their recommender systems"[132] upon request from the Digital Service Coordinator or from the Commission. Access to information for vetted researchers has been broadened, it now covers not only the identification of systemic risks, but also the measures taken to mitigate those risks.[133] VLOPs still have the power to request an amendment of the access requests to the Digital Services Coordinator under article 40(5)—it remains to be seen whether this could undermine the impact of this obligation.[134]

57 **Reporting obligations.** Article 42 imposes specific reporting obligations for VLOPs, in addition to those already contained in Articles 24 and 15. VLOPs will have to issue those reports every 6 months, instead of once year for other intermediaries.[135] Furthermore, VLOPs have to report on the following information:

- Information specific to their human resources involved in moderation, including their qualification and linguistic expertise[136];
- Their number of active users in each Member State[137];
- Information related to the risk assessments and mitigation measures pursuant to Articles 34 and 35[138];
- Information related to the independent audit pursuant to Article 37(4).[139]
- VLOPs have the possibility to publish versions of those reports redacted of certain confidential information. In that case, however, VLOPs have to transmit the complete report to the relevant Digital Services Coordinator and the European Commission.[140]

VI. Enforcement mechanisms in the DSA

58 The enforcement roles in the DSA have been divided between the newly created Digital Services

132 DSA, Article 40, 3.

133 DSA, Article 40.

134 DSA, Article 40, 5.

135 DSA, Article 42, 1.

136 DSA, Article 42, 2.

137 DSA, Article 42, 3.

138 DSA, Article 42, 4.

139 ibid.

140 DSA, Article 42, 5.

Coordinators, the European Board for Digital Services as well as the European Commission.

59 Digital Services Coordinators (or DSCs). Digital Services Coordinators are designed by Member States. Even though more than one authority could be responsible for the enforcement of the Digital Services Act, the DSC should be responsible for ensuring coordination at national level of all authorities in charge of enforcing the DSA.[141] Mechanisms are put in place in order to allow for cooperation between DSCs across borders[142], as well as with the Board and the Commission.[143] DSCs are assigned investigation[144] and enforcement[145] powers, which includes the power to require audits from online platforms, impose fines and require immediate actions or commitments in order to remedy harmful situations.[146]

60 European Board for Digital Services. The European Board for Digital Services is an EU-level independent advisory group whose role is to ensure the consistency of the application of the DSA across Member States and to provide assistance and guidance on relevant emerging issues across the EU and regarding the supervision of VLOPs. It does not have investigating nor enforcement powers towards online platforms.[147]

61 European Commission. The European Commission, while not fully in charge of enforcing the DSA, still has a role to play in its enforcement. Its role is more subsidiary for online platforms under the 45 million users mark where it can assist DSCs in case of inconclusive investigation or repeated infringements. In the context of VLOPs, however, the Commission notably has the authority to launch an investigation[148], to issue fines to non-compliant VLOPs[149], to put interim measures in place in case of urgency[150], to require commitments for platforms to ensure compliance[151] and to effectively take actions to monitor the effective application of the DSA.[152]

62 Limits of enforcement by national authorities. The Member States-centered approach taken by the European legislator with the DSA is similar to the one proposed in the General Data Protection Regulation ("GDPR"), where Member States designate one (or more) Data Protection Authority in charge of data protection. Through a one-stop-shop mechanism, also similar to the one instituted in the GDPR, the DSA aims to better resolve cross-borders conflicts involving platforms.[153] This situation could lead to potential discrepancies between the Member States regarding the DSA, as some have already pointed regarding the GDPR.[154] Lack of uniformity between the means at the disposal of various data protection authorities has been highlighted as an issue regarding GDPR enforcement and the same could be true for the DSA.[155] Finally, the concentration of VLOPs' main establishment in a few Member States, notably Ireland, could put additional workload on specific DSCs as well as political pressure[156] in order not to see VLOPs move their establishment to a Member State which is less strict (or less staffed) in terms of enforcement.[157]

63 The enforcement by the Commission might be more effective. The European Commission has already issued large fines to corporations, such as the $2.4B fine imposed on Google for abusing its dominant position.[158] Letting the Commission enforce the DSA

141 DSA, Article 49.

142 DSA, Article 57.

143 DSA, Article 49, 2.

144 DSA, Article 51, 1.

145 DSA, Article 51, 2.

146 DSA, Article 52.

147 DSA, Article 61.

148 DSA, Article 66.

149 DSA, Article 74.

150 DSA, Article 70.

151 DSA, Article 71.

152 DSA, Article 72.

153 DSA, Article 58.

154 J. Ryan, 'Europe's Governments are failing the GDPR: Brave's 2020 Report on the enforcement capacity of data protection authorities', 2020, <https://brave.com/wp-content/uploads/2020/04/Brave-2020-DPAReport.pdf>.

155 'Has GDPR Delivered on Its Central Promise?' (*Law.com International*) <https://www.law.com/international-edition/2022/01/31/lawyers-say-gdpr-has-failed-to-deliver-on-its-central-promise/> accessed 16 August 2022.

156 See for instance the allegations concerning Facebook's investigations by the Irish Data Protection Authority, B. Goodwin, 'Max Schrems accuses Ireland of 'Kafkaesque' delay in Facebook GDPR investigation', Computer Weekly, 26 May 2020, https://www.computerweekly. com/news/252483668/Schrems-accuses-Ireland-of-Kafkaesque-delay-in-Facebook-GDPR-investigation.

157 Strowel and Somaini (n 64).

158 'Antitrust: Commission fines Google €2.42 billion for abusing

might create some uncertainty in case of a change of the political composition and/or inclination of the Commission (while some of today's Commissioners, for example Thierry Breton, are in favor of robust intervention).

64 **Means in the hands of the EU.** Another issue regarding enforcement that is common to both the DSCs and the EU Commission is the discrepancy between the means at the hands of public powers and the large pockets on which VLOPs can rely on. Effectively regulating platforms will require additional personnel and expertise. New funds should be allocated to this mission. Article 43 of the DSA will allow the Commission to charge VLOPs a supervisory fee that should, in theory, cover the expenses incurred for their supervision.[159]

65 Thierry Breton, in a press release following the final vote on the DSA by the EU parliament, gave a few insights of how the Commission will supervise the enforcement of the DSA for VLOPs. He insists on the cooperation within the Commission itself, but also on a reliance on "a network of trusted flaggers, such as NGOs, hotlines or rightsholders, to ensure that platforms react to the flagged illegal content as a priority".[160] During the same address, he also mentioned the creation of a high-profile European Centre for Algorithmic Transparency (ECAT). The ECAT, hosted by the Joint Research Center of the Commission, has been launched on 18 April 2023, it should closely cooperate with DG CONNECT and with industry representatives, academia and civil society, fostering the multi-stakeholder model of regulation that the DSA aims to promote.[161]

E. Conclusions on the DSA contribution to the fight against disinformation and some possible improvements

66 **A necessary yet only first step.** During the debates preceding the adoption of the DSA, most Members of the European Parliament welcomed the draft legislation. At the same time, they admitted that the DSA is only a first step towards an efficient regulatory framework for online platforms in the EU.[162] When the whole DSA will apply (as of 17 February 2024), we will see how the changes regarding liability for illicit content (see above under C) together with the new diligence obligations (see above under D) and the implementing measures will (or will not) make a difference in practice. The regulators have less than a year to prepare. We have some doubt about whether the new reporting and transparency obligations of the DSA will really make a difference, in particular for reducing online disinformation, but it is also clear that the DSA is part of a European and global trend towards platform regulation (even the US is now clearly considering to introduce such regulatory framework[163]), and the convergent regulatory initiatives might well prompt some platforms to partly revise their (ad-based) business model and their treatment of awful and illicit content.

67 As the DSA alone will thus not be sufficient to curb the spread of disinformation and other nefarious content, we suggest three paths of additional improvements to regulate online disinformation in Europe:

- A broader principle of transparency for online platforms which would provide a positive right for some collectives (such as consumers organizations) to initiate actions;
- A co-regulation model with enhanced involvement of users and third parties in accessing and adjusting the parameters for content recommendation on the platforms; and
- An independent authority to regulate online platforms.

dominance as search engine by giving illegal advantage to own comparison shopping service' (*European Commission - European Commission*) <https://ec.europa.eu/commission/presscorner/detail/es/MEMO_17_1785> accessed 16 August 2022.

159 DSA, Article 43.

160 'Sneak Peek: How the Commission Will Enforce the DSA & DMA' (*European Commission - European Commission*) <https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_22_4327> accessed 16 August 2022.

161 ibid; see: <https://algorithmic-transparency.ec.europa.eu/index_en>.

162 'Sitting of 04-07-2022 | Plenary | European Parliament' <https://www.europarl.europa.eu/plenary/en/vod.html?mode=chapter&vodLanguage=EN&vodId=c53414f9-469d-6196-fa8d-be169c87c94e&date=20220704#> accessed 26 July 2022.

163 See J. Biden op ed in the Wall Street Journal, 11 Jan. 2023, "*Republicans and Democrats, Unite Against Big Tech Abuses.* Congress can find common ground on the protection of privacy, competition and American children".

I. Need for an additional transparency principle generating a right to get an explanation and a remedy

68 **A general transparency principle.** We believe that a general transparency principle and a related right to transparency for the users of platforms should be imposed. The current reporting obligations imposed on platforms by the DSA will allow for the opening of platforms' data and mechanisms, but we believe more could be done. The importance of social media platforms for our democratic societies justifies that transparency should be the norm, not the exception; platforms should offer their users and society, in general, an accurate picture of the way they operate and make decisions about prioritizing and spreading information.[164] We therefore propose to impose a general transparency principle on platforms, similar to the one applicable to public administration[165] (and to some extent to the transparency principle included in the GDPR).[166]

69 Transparency obligations related to the design of online platforms and their moderation policies could foster accountability and allow users and external actors to test the efficiency and effectiveness of the platforms' moderation tools, just as administrative transparency theoretically allows citizens to oversee the actions of the administration.[167] Furthermore, obligations analog to those of administrative transparency could reduce the secrecy around the operations of platforms, allowing for better oversight thereafter.

70 This transparency principle should be accompanied with an accountability principle. Platforms should not only comply with the various transparency obligations contained in the legislation but should also be able to demonstrate their compliance. Shifting the burden of proof of compliance on VLOPs makes sense given their role as gatekeepers online.[168] The extent of such change in the burden of proof should be further analyzed, and in any case well-targeted, as VLOPs' freedom to conduct their business cannot be disproportionately curtailed.[169]

II. Co-regulation with vetted researchers and other certified stakeholders involved in the process

71 **A more active role for users and third parties.** For years, the circulation of information and the mitigation of disinformation have been ordered by platforms through tech design twists and self-regulation. Content orientation and recommendations were thus only left to "private ordering". The DSA marks a step towards more intervention by public authorities. However, such an approach should remain minimal as freedom of expression rightly limits how far the State can interfere in the public debate and in the process leading to the collective construction of truth. To go further, we believe it is important to empower users and third parties such as academic scholars and NGOs so that they can play a more active role in the fight against disinformation. The DSA takes some steps in that direction (see above on data access and Article 40), but more could be done.

72 **Empowering users through middleware.** Middleware has been defined in this context as "software and services that would add an editorial layer between the dominant internet platforms and in-

164 Amélie Heldt and Stephan Dreyer, 'Competent Third Parties and Content Moderation on Platforms: Potentials of Independent Decision-Making Bodies From A Governance Structure Perspective' (2021) 11 Journal of Information Policy 266.

165 In the 1970s, a growing movement called for more transparency on the part of public administrations. The doctrine of administrative transparency developed itself in opposition to the culture of secret which had been prevalent in the public administration. Jacques Chevallier, « Le mythe de la transparence administrative », in Information et transparence administratives, PUF, 1988.

166 Élise Degrave and Yves Poullet, *L'e-Gouvernement et La Protection de La Vie Privée: Légalité, Transparence et Contrôle* (Larcier 2014) 314. Its aim would be to allow citizens to understand "how the governments operate on their behalf". See Christopher Hood and David Heald, *Transparency The Key to Better Governance?* (2012) 49.

167 ibid.

168 Philip M Napoli, 'Social Media and the Public Interest: Governance of News Platforms in the Realm of Individual and Algorithmic Gatekeepers' (2015) 39 Telecommunications Policy 751.

169 Article 16 of the EU Charter of Fundamental Rights only timidly recognises the freedom to engage in business activities, and the CJEU interpretation of this general principle of law, which predates its incorporation in the Charter, is not a bar to an increased burden of proving some level of compliance (still to be defined). See for ex. Thierry Leonard and Julie Salteur, Article 16 - Liberté d'entreprise, in Fabrice Picod, Cecilia Rizcallah et Sébastien Van Drooghenbroeck (eds.), *Charte des droits fondamentaux de l'Union européenne. Commentaire article par article*, Larcier, 2023, 3rd ed., p. 401 ff.

ternet users".[170] Middleware would allow users to better control the content they receive on social media. While several solutions for users do exist, those solutions are usually reserved to tech-handy users.[171] Articles 27 and 38 of the DSA, which encourage platforms to give users more choice regarding the way content is formatted, prioritized and proposed to them, is a first step towards a broader and user-friendlier introduction of middleware on online platforms.

73 **Broader access right beyond the vetted researcher status.** In order to better integrate additional actors in the regulatory process, a larger opening of the vetted researcher status should be considered. Under the DSA, the DSC are responsible for granting the status of vetted researchers allowing them to access the data related to risks assessments of VLOPs and their mitigation measures. We suggest to leave the certification process in the hands of the ethics committees of the research institutions (thus reducing the role of the DSCs). More could also be done to allow some NGOs to benefit from the vetted researchers' access rights.[172] A strong certification mechanism should therefore be put in place in order to safeguard online privacy as well as the commercial interests of platforms.

74 **Better compliance and enforcement for self-regulatory instruments.** The self-regulatory tools used by platforms are currently left mostly unchecked. Tools such as the Code of Practice against Disinformation (see above under C) have been criticized for the lack of enforcement and compliance mechanism. Article 45 of the DSA specifically addresses codes of conduct such as the Code of Practice and allows the Commission as well as the Board to take actions in case of systematic failure to comply with a code of conduct—providing the existing Code of Practice with co-regulatory features.[173] (An explicit reference to the Code of Practice is by the way included in recital 106 of the DSA.) However, the current wording of Article 45 only allows the Commission and the Board to "invite the signatories to the codes of conduct to take the necessary action". It does not seem to give the EU authorities the necessary power to go further.

III. An independent authority to regulate online platforms

75 **Potential issues with the DSA enforcement.** The current enforcement methods of the DSA, splitting responsibilities between DSCs at the Member State level and the Commission, might cause issues similar to what has already been observed with the enforcement of the GDPR[174]: domestic issues might hinder the efficiency of the DSC in some EU countries[175] while there might be some pushback from certain DSCs to adequately address pressing issues, justified for instance by a lack of resources.[176] This could open the way for a form of forum shopping between Member States.[177] However, the European Commission services (in particular, the division on platforms at DG CONNECT) will be directly involved for the DSA enforcement. The prominent role given to the Commission might make the regulation of online platforms dependent on the political willingness of the Commission to use its new regulatory powers. A shift of policy objectives could therefore undermine the long-term enforcement of the obligations contained in the DSA.

170 Francis Fukuyama et alii, Middleware for Dominant Digital Platforms: Technological Solution to a Threat to Democracy, Stanford Cyber Policy Center, available, but not dated, at: <https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/cpc-middleware_ff_v2.pdf>, accessed 8 Sept. 2022 .

171 Several browser extensions are available online to tweak the ranking mechanisms of social media. For example, Social Fixer for Facebook (<https://socialfixer.com/>) allows the user to disable certain features of the platform, such as infinite scrolling or advertised posts.

172 Strowel and Somaini (n 64).; T Marsden, I Brown and M Veale, 'Responding to Disinformation: Ten Recommendations for Regulatory Action and Forbearance' in M Moore and D Tambini (eds), *In: Moore, M and Tambini, D, (eds.) Regulating Big Tech: Policy Responses to Digital Dominance. (pp. 195-230). Oxford University Press: Oxford, UK. (2021)* (Oxford University Press 2021) <http://doi.org/10.1093/oso/9780197616093.003.0012> accessed 25 April 2022.

173 DSA, Article 45.

174 'Has GDPR Delivered on Its Central Promise?' (n 155).

175 See for example the numerous accusations of malfunctioning of the Belgian Data Protection Autority (APD/GBA), which almost led to an official procedure of the European Commission against Belgium in front of the ECJ – see https://www.lesoir.be/438557/article/2022-04-27/lapd-est-inoperante-un-et-demi-dalertes-de-ses-deux-codirectrices.

176 See for example the tensions between the European Commission and the Irish DPA regarding Meta - <https://iapp.org/news/a/what-the-dpc-meta-decision-tells-us-about-the-gdprs-dispute-resolution-mechanism/?mkt_tok=MTM4LUVaTS0wNDIAAAGJO9479tKXSTPebi5oJZaJ5y7hxaF3KMUwUiTwQamXWTXoNesognmhoyE5N2RKcskx-N27jhO14TlzjA_TzQK1xIWS9SMpQGcu7vvQ1a2pD3nY>.

177 Dan Jerker B Svantesson, 'EDPB's Opinion 8/2019 on the Competence of a Supervisory Authority in Case of Establishment Changes Reports: European Union' (2020) 6 European Data Protection Law Review (EDPL) 98.

76 **An independent EU authority to regulate platform.** We therefore suggest the creation of an independent, European-wide entity solely in charge of the regulation of online platforms. The creation of the European Board for Digital Services is a positive first step. Such an independent authority would be responsible for the enforcement of the transparency principle described above and to organize the relations between platforms, their users and the different stakeholders involved in the production and regulation of content online. This authority should fulfill the standards imposed on any regulator, such as independence and accountability towards the public, and be well-equipped (sufficient funding and staffing with data and algorithms experts).

Authorless AI-assisted productions

Recent developments impacting their protection in the European Union

by **Marta Duque Lizarralde and Christofer Meinecke***

Abstract: The question of whether AI-generated works can be protected by copyright has become a hot topic over the last few years. However, "AI-generated works", at least as currently defined in some policy and legal texts, do not exist. This article seeks to explain how machine learning and natural language processing, which are two subfields of Artificial Intelligence, are used in the creative process. It then outlines the obstacles that works created with the help of AI face in order to be classified as protectable subject matter. After that, it briefly analyses whether such works can be protected by existing related rights and concludes by discussing the arguments put forward in the academic literature in favour of the creation of a new exclusive right to encourage investment in "creative AI".

Keywords: Copyright; Authorship; Originality; AI-generated works; Authorless AI-assisted productions

Recommended citation: Marta Duque Lizarralde and Christofer Meinecke, Authorless AI-assisted productions: Recent developments impacting their protection in the European Union, 17 (2023) JIPITEC 84 para 1.

A. Introduction

1 In the report on intellectual property rights (IPRs) for the development of artificial intelligence (AI) technologies, published in October 2020, the European Parliament (EP) stressed that "the growing autonomisation of certain decision-making processes can give rise to technical or artistic creations."[1] Therefore, "assessing all IPRs in the light of these developments must be a priority for this area of EU law."[2] Such assessment is likely to address, amongst others, whether AI-generated outputs can be protected by IPRs. Should AI-generated results be protectable under IP, the next question would be whether an AI system could be recognised as the 'author' or the 'inventor' of such results. If not, it is necessary to discuss whether changes in the IP system are needed to encourage investment in AI technology. This article will be centred on the authorship claims.[3]

* Marta Duque Lizarralde, LL.M., is Research Associate, Doctoral candidate at the Technical University in Munich, Germany.Christofer Meinecke, M.Sc., is Research Assistant, Doctoral candidate at Leipzig University, Germany. The views expressed herein are those of the authors and do not necessarily reflect the opinions of former, present, or future employers or organisations. Any errors in the legal analysis remain those of Marta Duque Lizarralde. All links last accessed on the 24th of June 2022.

1 *European Parliament (EP) Report on intellectual property rights for the development of artificial intelligence technologies*, (2020/2015(INI) (2.10.2020), Explanatory Statement, <https://www.europarl.europa.eu/doceo/document/A-9-2020-0176_EN.html>.

2 *Ibid*, para. 14.

3 For an overview on the inventorship claims, see Daria Kim 'AI-Generated Inventions': Time to Get the Record Straight? ´(2020) *69 (5) GRUR International* 443,456; Kaelyn R. Knutson, 'Anything You Can Do, AI Can't Do Better: An Analysis of Conception as a Requirement For Patent Inventorship And A Rationale For Excluding AI Inventors' (2020) *11(2) Cybaris*; https://open.mitchellhamline.edu/cgi/viewcontent.cgi?article=1097&context=cybaris>; and Daria Kim, Maximilian

2 Although today's AI systems deliver far greater functionality and capabilities than software from the 80s[4], current discussions focus on the wrong question, that is, whether AI systems, without human intervention, are capable of creating copyrightable results. Instead, the real question should be whether creations generated with the assistance of AI, where the human contribution is not of an original nature, are protectable.[5]

3 This article aims to explain what is the role of AI in the creative process and the main obstacle against AI creations' eligibility for copyright protection, *i.e.*, meeting the requirement of originality. It also discusses briefly why some states' regulations on this issue do not address it satisfactorily. Next, it analyses whether such creations can be protected by existing related rights, or whether the creation of a new related right is needed for their protection.

B. Artificial Intelligence and the culture industry

4 The current surge in AI development began in 2013.[6] Several factors triggered the boom, including the increase in ICT R&D funding, which allowed for greater availability of computing power and connectivity, the enormous production of large volumes of data, and the improvements in algorithms.[7]

I. Examples of Artificial Intelligence systems used in the cultural industry

5 Various AI systems are used in the cultural industry. The most cited project so far is 'The Next Rembrandt', based on 168,263 pictorial fragments from 346 of the painter's works. To identify and classify the most common Rembrandt patterns, a facial recognition algorithm and a deep learning system were used. The result was then printed in 3D with more than 149 million pixels and in several layers to resemble an oil painting.[8] Other examples of well-known systems are 'Flow Machines', a system that generates melodies from a database of 13,000 roadmaps of different genres[9]; or 'Tencent Dreamwriter'[10], 'Automated

Alber, Man Wai Kwok, Jelena Mitrovic, Cristian Ramirez-Atencia, Jesús Alberto Rodríguez Pérez, Heiner Zille, ´Ten Assumptions About Artificial Intelligence That Can Mislead Patent Law Analysis´ (2021), *Max Planck Institute for Innovation & Competition Research Paper No. 21-18* <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3910332>.

4 For an overview of the debate on how computer programs may affect the IP legal framework at the time, see Timothy L. Butler, ´Can a Computer be an Author, Copyright Aspects of Artificial Intelligence´ (1982) *4 Hastings Comm. & Ent.L.J.* 707,747; Pamela Samuelson, ´Allocating Ownership Rights in Computer-Generated Works" (1985) 47 *Berkeley Law Scholarship Repository* 1186,1224; and Ralph D. Clifford, ´Intellectual Property in the Era of the creative Computer Program: Will the True Creator Please Stand Up?´(1997), 71 *Tulane Law Review* 1676,1702. For a distinction between the elaboration of computer programs and the creation of ML models, see Begoña Gonzalez Otero, 'Machine Learning Models under the copyright microscope: is EU Copyright fit for purpose?' (2021) *GRUR International* 1043,1055.

5 James Grimmelmann, ´There's No Such Thing as a Computer-Authored Work – And It's a Good Thing, too´ (2016), *39 Colum. J. L. & Arts* 403.

6 WIPO, WIPO Technology Trends 2019, 30,36 <https://www.wipo.int/edocs/pubdocs/en/wipo_pub_1055.pdf>

7 *Ibid;* Josef Drexl, Reto M. Hilty et al., 'Technical Aspects of Artificial Intelligence: An Understanding from an Intellectual Property Law Perspective, Version 1.0' (2019) <https://ssrn.com/abstract=3465577>; Annoni Alessandro; Benczur Peter; Bertoldi Paolo; Delipetrev Blagoj; De Prato Giuditta; Feijoo Claudio; Fernandez Macias Enrique; Gomez Gutierrez Emilia; Iglesias Portela Maria; Junklewitz Henrik; Lopez Cobo Montserrat; Martens Bertin; Figueiredo Do Nascimento Susana; Nativi Stefano; Polvora Alexandre; Sanchez Martin Jose Ignacio; Tolan Songul; Tuomi Ilkka; Vesnic Alujevic Lucia, *'Artificial Intelligence: A European Perspective'* (Publications Office of the European Union, 2018), 19, 24; See the EC ISA2 webpage: <https://ec.europa.eu/isa2/news/european-commission-has-announced-investment-€92-billion-align-next-long-term-eubudget-2021en>: In Europe, for example, €2.5 billion is planned to help spread AI across the European economy and society between 2021 and 202.

8 See "The Next Rembrandt": <https://www.nextrembrandt.com/>.

9 See Flow Machines: <https://www.flow-machines.com/>; James Vincent, ´This AI-written pop song is almost certainly a dire warning for humanity´ (*The Verge, 2016*) <https://www.theverge.com/2016/9/26/13055938/ai-pop-song-daddys-car-sony>.

10 See Kan He, ´Another decision on AI-generated work in China: Is it a Work of Legal Entities? ´ *(The IPKAT, 2020*) <Another decision on AI-generated work in China: Is it a Work of Legal Entities? – The IPKat (ipkitten.blogspot.com)>; and Vivian Demonts and Ivy Liang, ´Is the Chinese 'Dreamwriter' Case Really a Groundbreaking Case for AI-Generated Works? *(GOWLING GWL, 2020)* <https://gowlingwlg.com/en/insights-resources/articles/2020/china-dreamwriter-case/> explaining the *Shenzhen Tencent v Yinxun* case, before

Insights natural language generation (NGL)'[11], and 'Editor'[12], AI systems that operate in the field of 'automated' or 'robojournalism'. But there are many more. For instance, platforms such as 'Artbreeder'[13] allow the collaborative creation of new images by modifying existing ones and combining their style using neural networks; or systems such as 'GhostWriter'' enable the creation of books from an initial story outline. [14]

II. Fundamentals on the functioning of Artificial Intelligence

1. Definition of "Artificial Intelligence"

6 There are different definitions of AI. For the purposes of this article, the authors will follow the World Intellectual Property Organization (WIPO) definition, according to which AI is "a discipline of computer science that is aimed at developing machines and systems that can carry out tasks considered to require human intelligence."[15] It is important to note, however, that the WIPO definition includes 'human intelligence', which is conflicting with the definition applied by most AI researchers, that focus rather on 'intelligent agents', precisely to avoid the problem of measuring 'human intelligence'.[16] In any case, the goal of AI is to automate and accelerate the performance of an intellectual task, traditionally performed by humans, through systematisation. The tasks that AI systems can accomplish are becoming progressively more complex, but their purposes remain limited. Since current AI systems can only perform specific tasks, they belong to the category of narrow AI, but not to the category of 'artificial general intelligence' (AGI), which would encompass systems that can undertake any intellectual endeavour. The latter remains in the realm of science fiction.[17]

2. Machine Learning

7 Machine learning (ML) is the most prominent subfield of AI. It aims to create pattern-recognition models that 'learn' to make predictions about new data by adjusting to previous data.[18] There are three main types of ML: supervised, unsupervised, and reinforcement. In supervised learning, the system is trained with labelled data and must be able to apply this knowledge to recognise the labels in a new dataset. This requires that the correct labels are provided in the first place.[19] On the contrary, unsupervised learning involves providing unlabelled training data samples with the goal of covering the hidden structure underlying the data.[20] The quality and size of the training dataset are crucial in the success of both learning processes.[21]

8 One example of unsupervised learning is 'generative modelling'. Generative modelling has become more prominent recently, as two deep learning (DL)[22] techniques called 'variational autoencoders'

---

the Nanshan District Court of Guangzhou Province. In this case, the Court granted copyright protection to an article that was said to be written by Dreamwriter, as it considered that Dreamwriter was used rather as a writing tool.

11 See Automated Insights: <https://automatedinsights.com/>.

12 See Editor: <https://nytlabs.com/projects/editor.html>.

13 See Artbreeder: <https://www.artbreeder.com/>.

14 Satoshi Sato, A challenge to the third Hoshi Shinichi award, Proceedings of the INLG 2016 Workshop on Computational Creativity in Natural Language Generation (2016) 31,35.

15 WIPO, ´What is Artificial Intelligence? <https://www.wipo.int/about-ip/en/artificial_intelligence/faq.html>.

16 See Stuart J Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach* (Prentice Hall., 2009) 1,5; or David L. Poole and Alan M. Mackworth, *Artificial Intelligence, Foundations of Computational Agents* (Cambridge University Press, 2010) 3, defining AI as *"the field that studies the synthesis and analysis of computational agents that act intelligently"*.

17 Cormen, Thomas H., Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein, *Introduction to Algorithms* (MIT Press, 2009) 5; Marta Duque Lizarralde and Héctor Axel Contreras, ´The real role of AI in patent law debates´ (2022) <https://academic.oup.com/ijlit/advance-article-abstract/doi/10.1093/ijlit/eaac008/6555494>.

18 Mehryar Mohri, Rostamizadeh Afshin and Ameet Talwalkar, *Foundations of Machine Learning* (The MIT Press, 2018) 1,2; Matt Taddy, ´The Technological Elements of Artificial Intelligence´ (2019) NBER Working Paper 24301 <https://www.nber.org/system/files/working_papers/w24301/w24301.pdf>.

19 Josef Drexl, Reto M. Hilty et al., (n.14); Anthony Man-Cho So, ´Technical Elements of Machine Learning for Intellectual Property Law´, in J.-A. Lee, K.-C. Liu, R. M. Hilty (eds.), *Artificial Intelligence & Intellectual Property* (Oxford University Press, 2020).

20 *Ibid.*

21 Mohri et al (n. 18) 1.

22 Matt Taddy (n.18): Deep learning relates to some machine learning techniques in which several layers of simple pro-

and 'generative adversarial networks', enabled major breakthroughs in terms of creative content creation.[23] It must be recalled, however, that there is nothing magical in the functioning of creative AI systems. These systems simply perform mathematical operations, previously programmed, to learn a latent space from the data they are trained on. The latent space can be defined as "an abstract multi-dimensional space that encodes a meaningful internal representation of externally observed events."[24] In this space, similar data entries are placed close to each other and, by sampling it, these systems produce new works with similar characteristics.[25]

9 For example, a Variational Autoencoder (VAE) is a combination of an encoder and a decoder network that learns a general encoding from an unlabelled dataset. The encoder maps the input data to a latent space and the decoder tries to map the representation in the latent space back to the input data. The VAE learns a continuous latent space from the input data, which is achieved by creating two encodings by the encoder based on their mean and the standard deviation. This leads to different encodings for the same input data. Through this, the decoder learns for a specific input sample to refer to an area in the space instead of a single point. Further, the training process minimizes the differences between the areas of different training samples in the latent space in order to allow arithmetic on them to generate new features, e.g., adding an accessory to a person in an image, or combining faces of celebrities.[26]

10 Generative adversarial networks, in turn, are a set of algorithms that aim to make two neural networks compete to learn and evolve. Both networks are trained with the same dataset, but the first generating network must create variations of the data and produce a creative result that looks genuine. This output will be analysed by a second discriminative network to determine if it is part of the original training dataset or a fake output. Depending on its quality, the discriminative network will give it a score on a scale of 0 to 1. If the score is low, the generative network corrects the result and forwards it to the discriminative network. The generative networks then repeat the cycle until they create high-scoring results. In this way, images and sounds with a high degree of realism[27], or even level for video games, are produced.[28]

11 Lastly, in reinforcement learning, the system must achieve a certain goal and receives penalties or rewards for its performance, the goal being to maximise the total reward.[29] It has been an area of great success in training AI systems for playing games, as illustrated by the example of AlphaGo defeating a professional human Go player.[30]

3. Natural Language Processing

12 Another subset of AI worth mentioning is Natural Language Processing (NLP), which is used, among other things, for machine translation, text summarisation and the creation of texts, which can be short, as in the case of answers in chatbots; but also longer, as in the case of passages in articles and reports on events.[31] NLP is an area that, as its name suggests, deals with processing natural languages. This processing entails the translation of natural language into numerical data that a computer can

cessing units are connected in a network, so that the input to the system passes through each of them successively.

23 Nina I. Brown, ´Artificial Authors: a Case for Copyright in Computer-Generated Works´ (2018), *XX The Columbia Science and Technology Law Review,* 8; François Chollet, *Deep Learning with Python* (Manning, 2018) 296, 313: Although a large number of academic articles point to the great revolution that generative adversarial networks are bringing about, François Chollet points out that "*the most successful practical applications I have seen with images rely on variational autoencoders.*"

24 Panagiotis Antoniadis, ´Latent Space in Deep Learning´ (March 4, 2022, Baeldung) <https://www.baeldung.com/cs/dl-latent-space>

25 François Chollet (n.23) 270. For an in-depth comprehension of how ML is applied to generate text and images see chapter 8 of this book.

26 Xianxu Hou, Linlin Shen et al., Deep feature consistent variational autoencoder, 2017 IEEE Winter Conference on Applications of Computer Vision (WACV) (2017) 1133,1141.

27 Joseph Roca, ´Understanding Generative Adversarial Networks (GANs), Building, step by step, the reasoning that leads to GANs´ (towards data science, 2019) <https://towardsdatascience.com/understanding-generative-adversarial-networks-gans-cd6e4651a29>; Marta Duque Lizarralde, 'Las obras creadas por Inteligencia Artificial, un nuevo reto para la propiedad intelectual '(2020), *64 Revista pe.i* 13,67.

28 Ruben Rodriguez Torrado, Ahmed Khalifa, et al., Bootstrapping conditional gans for video game level generation, 2020 IEEE Conference on Games (CoG) (2020) 41,48.

29 Anthony Man-Cho So (n.18).

30 See DeepMind website: https://deepmind.com/research/case-studies/alphago-the-story-so-far

31 Hannes Hapke, Cole Howard, Hobson Lane, *Natural Language Processing in Action: Understanding, analyzing, and generating text with Python* (Manning, 2019) Ch.1.

use to learn.[32] NLP relies on unstructured data, which can be more challenging to interpret.[33] But structured data like semantic lexicons, or linguistic rules can be applied to induce domain knowledge into a model, e.g., word relations.[34] Processing the text consists of several stages. First, the text is converted into a format that computers can process. To do this, several steps must be taken. In the first place, the text is analysed and divided into several pieces, which is called tokenisation. Subsequently, the text is normalised, which means converted to be easier to process, for example by removing punctuation marks or contractions. The next step would be to remove affixes and suffixes, known as stemming, and to reduce a word to its base form to group the different existing forms of the same word, that is, to lemmatise. The system must then understand the overall meaning of the text. For this, there are different techniques, and DL is frequently employed. As a result of the process, the system must be able to discover hidden structures in sets of texts or documents.[35]

13 The development of AI "creative" systems requires significant investment. With the aim of protecting and recovering this investment, it has been proposed to protect the results generated with AI through exclusive rights. The first question in this regard is whether these creative outputs would be eligible for copyright protection.

C. Copyright

I. Protectable subject-matter

14 The object of copyright protection is the work, which is the formal expression of an idea or feeling communicated to the public. The work is an immaterial good, so the object of protection is the form, the expression, but not its tangible medium or the ideas it comprises.[36]

15 For a work to be eligible for copyright protection, it must be original.[37] There is no rule at international or EU level defining what is meant by originality. At the EU level, however, the Court of Justice of the European Union (CJEU) has specified that a work is original if it is "the author's own intellectual creation", which "is manifested by the author's free and creative choices."[38] This requires the existence of a field of choice, which means the requirement of originality is not met when the result is dictated by technical considerations, rules, or other subject-matter constraints which leave no room for creative freedom.[39] In addition to this, although not explicitly stated, it follows from the case law of the CJEU, the provisions of the Berne Convention[40], and some of the EU copyright directives,[41] that the author must be a natural person.

II. Demystifying the role of Artificial Intelligence in the creative process

16 Following the academic debate, a distinction must be made here between AI-assisted works and AI-generated works. According to WIPO, 'AI-assisted works' are those "that are generated with material

32 *Ibid.*

33 Tom Taulli, *Artificial Intelligence Basics, A Non-Technical Introduction* (Apress, 2019) Ch.6; Adam Geitgey, ´Natural Language Processing is Fun! How computers understand Human Language´ (Medium, 18 July 2018) <https://medium.com/@ageitgey/natural-language-processing-is-fun-9a0bff37854e>

34 Manaal Faruqui, Jesse Dodge et al., ´Retrofitting Word Vectors to Semantic Lexicons in Proceedings of NAACL´ (2015) <https://arxiv.org/abs/1411.4166>

35 Tom Taulli (n.33) Ch.6; Adam Geitgey, ´Natural Language Processing is Fun! How computers understand Human Language´ (Medium, 18 July 2018) <https://medium.com/@ageitgey/natural-language-processing-is-fun-9a0bff37854e>

36 Claude Masouyé, ´*Guide to the Berne Convention for the Protection of Literary and Artistic Works* (WIPO 1978) 33.

37 Art. 2 of the Berne Convention for the Protection of Literary and Artistic Works of September 9, 1886;

38 Among others, C-145/10, Painer v. Standard Verlags GmBH and others (2011) ECLI:EU:C:2011:798, para 119,120; C-604/10, Football Dataco Ltd v. Yahoo! UK Ltd y and others (2012) ECLI:EU:C:2012:115, para 37,39; C-403/08 and C-429/08, Football Association Premier League v. QC Leisure and Karen Murphy v. Media Protection Services (2011) ECLI:EU:C:2011:631, para 97.

39 C-683/17, Cofemel (2019) ECLI:EU:C:2019:721, para 31; C-833/18, Brompton Bicycle (2020) ECLI:EU:C:2020:461, para 23,24.

40 See Arts. 3 and 7 Berne Convention.

41 See Art. 3 Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases; Recital 16 and Art. 6 Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights; and Art.1 Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs.

human intervention and/or direction"[42], while 'AI-generated works' "refers to the generation of an output by AI without human intervention. In this scenario, AI can change its behaviour during operation to respond to unanticipated information or events."[43] Nonetheless, these definitions do not reflect the state of the current debate, since AI systems are still not capable of producing results autonomously, i.e., without any sort of human intervention.

17 In ML development, human involvement is needed in distinct phases and has a significant impact on the results. First, the training data is chosen and pre-processed by practitioners. This may include actions that require domain knowledge, for example, to exclude specific information or samples from the data that could impair the training. In the case of supervised learning approaches, the labelling of the data must also be performed by professionals with expertise in the field, although this task can be supported by an ML algorithm in a human-in-the-loop process.[44] Before training the ML model, programmers set the hyperparameters, which are those parameters that do not change during training. The first step in this regard is to design the architecture of the model, i.e., its structure. Each model is suitable for different sets of tasks, so establishing the architecture also requires expertise.[45] Subsequently, practitioners also decide on the learning rate and the algorithms used for the optimisation and regularisation of the trainable parameters of the model. Trainable parameters, unlike hyperparameters, are adjusted to better fit the data as the training dataset is analysed. To assess whether training the model is successful, a loss/cost function must be established beforehand as well. After training, decisions such as output and model selection further influence the final results.[46] It is important to keep in mind that at each step of the human intervention a bias is induced in the model in addition to the bias already present in the original data. It is also relevant to clarify that all these steps are not performed by the same person, but rather multiple actors are involved. Moreover, once the model has been trained, it can be applied by users completely unrelated to the training process.

18 In NLP, a subfield of particular relevance to our analysis is Natural Language Generation (NLG), which deals with the processing of unstructured data into human-readable text. The process of automated text generation entails various stages. First of all, as data often comprises more information than needed, the content to be produced must be delimited (content determination); then the data structures are arranged to create the narrative structure and the documentation plan (document/discoursing planning). Next, data are analysed and contextualised, often using ML (data interpretation). This involves the selection of phrases and words to express the domain-specific concepts and relationships in the texts (referring expression generation and lexicalisation). Subsequently, it must be ensured that the entire text adheres to the correct grammatical form, spelling, and punctuation (grammaticalization/linguistic realisation). And finally, the data is entered into the appropriate templates to check that the output is correctly formatted (language implementation). Human involvement in this process remains significant, although a number of tools exist that are useful for automating individual steps.[47]

42 WIPO, 'Revised Issues Paper on Intellectual Property Policy and Artificial Intelligence' (21 May 2020) <https://www.wipo.int/edocs/mdocs/mdocs/en/wipo_ip_ai_2_ge_20/wipo_ip_ai_2_ge_20_1_rev.pdf>.

43 *Ibid.*

44 Human-in-the-loop processes, like Active Learning and Visual Interactive Labelling, have gained more importance in recent years, as they enable a conversation between an-ML model and the programmers to improve the training process and allow obtaining the desired results with fewer data. See Burr Settles, ´Active learning literature survey´ (2009) <https://research.cs.wisc.edu/techreports/2009/TR1648.pdf>; and Jürgen Bernard, Marco Hutter et al., ´Comparing visual-interactive labeling with active learning: An experimental study in IEEE transactions on visualization and computer graphics´(2017) IEEE *transactions on visualization and computer graphics 298, 308.*

45 Josef Drexl, Reto M. Hilty et al. (n.14); Emmanuel Ameisen, *Building Machine Learning Powered Applications, Going from Idea to Product* (O´Reilly, 2020) 95.

46 François Chollet (n. 23); Wolfgang Ertel, *Introduction to Artificial Intelligence* (Springer, 2011) 175,179; Ethem Alpaydin, *Machine Learning* (The MIT Press, 2016) 166,178; John D. Kelleher, *Deep Learning* (The MIT Press, 2019) 12,13; David Watson, ´The Rhetoric and Reality of Anthropomorphism in Artificial Intelligence´ (2019) *29 Minds and Machines* 417,440.

47 Sciforce, ´A Comprehensive Guide to Natural Language Generation´ (July 4, 2029, Medium) <https://medium.com/p/dd63a4b6e548; https://research.aimultiple.com/nlg/>; Alina Trapova and Péter Mezei, ´Robojournalism – A Copyright Study on the Use of Artificial Intelligence in the European News Industry´ (2022) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4032020>.

III. "AI-assisted works" vs. "Authorless AI-assisted" productions

19 From what has been discussed so far, we can conclude that human intervention in the different phases that predetermine the outcome is still relevant. Consequently, the creations that are called 'AI-generated' are in fact 'AI-assisted'. In many works the human contribution to the final result is not only relevant, but also original, and therefore copyrightable.[48] This would be the case, for example, of 'The Next Rembrandt'.[49] However, there are some outputs, such as initial translations performed by DeepL[50], in which the human input may not be of an original nature, although the results are still linked to pre-existing data and parameters provided by the AI developers. Then, they are not copyrightable.[51] Nonetheless, these outputs are not 'AI-generated', and a more accurate term for this type of existing creations that do not deserve copyright protection is that of 'Authorless AI-assisted productions', adopted in the 'Trends and developments in AI final report'.[52] This report explains that there are three stages in the creative process of a work, namely conception, execution, and redaction. It also indicates that even if automated translators, such as DeepL, generate nearly usable results, some human intervention by the user in the redaction phase is still needed to turn the outputs into workable translations. Thus, if a natural person, based on the initial translation, which would not be protectable, makes further modifications, such as rephrasing words and changing the order of parts of the text, the result may be eligible for copyright protection.[53]

20 In the same vein, Trapova and Mezei argue that when NLG is employed in the field of robojournalism, at least in the phases of discourse planning and lexicalisation there is room for expressing the free and creative choices of individuals. Hence, the resulting outcomes may be protected.[54] Nevertheless, as these authors correctly observe, there are reports that, even if written by individuals, would not merit protection because the requirements regarding their presentation leave no margin for "originality".[55] In these cases, it makes no difference whether or not AI has been used to produce the text.

21 In short, to determine whether a result generated with AI is copyrightable, its creation process must be examined. There is no general rule but depending on the steps required to develop a particular project, as well as its domain of application, the type of human involvement in the different stages may or not be of an original nature. Therefore, on a case-by-case basis, there may be one person, several, or none at all who qualifies as the author.

48 Marta Duque Lizarralde (n.27); Robert Yu, ´The Machine Author: What Level of Copyright Protection is appropriate for Fully Independent Computer-Generated Works? (2017), *165 U. Pa. L. Rev. 1245;* Jane C. Ginsburg and Luke Ali. Budiardjo, ´Authors and Machines´ (2019), *34 (2) Berkeley Technology Law Journal* 6; Concepción Saiz García, ´Las obras creadas por sistemas de inteligencia artificial y su protección por el Derecho de autor´(2019) <https://indret.com/las-obras-creadas-por-sistemas-de-inteligencia-artificial-y-su-proteccion-por-el-derecho-de-autor/>; Bernt Hugenholtz and João Pedro Quintais, ´Copyright and Artificial Creation: Does EU Copyright Law Protect AI-Assisted Output?´, *52 IIC – International Review of Intellectual Property and Competition Law volume,* 1200, 1207.

49 Jane.C. Ginsburg, ´People Not Machines: Authorship and What It Means in the Berne Convention` (2018) *49 IIC – International Review of Intellectual Property and Competition Law* 133,134; Bernt Hugenholtz et al. 'Trends and Developments in Artificial Intelligence, Challenges to the Intellectual Property Rights Framework, Final Report'(2020) <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=71915>; Andrés Guadamuz, ´Do Androids Dream of Electric Copyright? Comparative Analysis of Originality in Artificial Intelligence Generated Works´ (2017) *2 Intellectual Property Quarterly,* 169,186. Nevertheless, the European Parliament (n..1) 13 argues that "*At a time when artistic creation by AI is becoming more common (one example being 'The Next Rembrandt' painting generated after 346 works by the painter were digitized so that they could be processed using AI), we seem to be moving towards an acknowledgement that an AI-generated creation could be deemed to constitute a work of art on the basis of the creative result rather than the creative process".* See also Reto Hilty, Jörg Hoffmann and Stefan Scheuerer ´Intellectual Property Justification for Artificial Intelligence´ in J.-A. Lee, K.-C. Liu, R. M. Hilty *(eds.), Artificial Intelligence & Intellectual Property, Oxford University Press,* 2020, stating that: *"The outcome of "The Next Rembrandt" project, a computer generated "new painting" in the style of Rembrandt, was simply founded on all available pre-existing Rembrandt paintings. In contrast, combining input from different artists in a targeted way to create a new style mix might qualify as an expression of personality."*

50 Bernt Hugenholtz et al. (n.49); Bernt Hugenholtz and João Pedro Quintais (n.48).

51 *Ibid;* As in the case of translations, if the initial reports and texts are subsequently modified by a natural person, the final result could be copyrightable; See Kan He (n.8).

52 Bernt Hugenholtz et al. (n.49).

53 *Ibid.*

54 Alina Trapova and Péter Mezei (n.47).

55 *Ibid.*

22 This idea is developed by Deltorn and Macrez in their analysis of the role of AI (especially DL) and authorship claims in the music industry.[56] In line with the previous discussion in this section, these authors point out that the functioning of DL systems relies on a series of human decisions made before, during and after the training of the model. The more difficult question then becomes whether there is an author according to the role of the different actors in the generative process, as well as the interactions between humans and the generative model in question.[57] When creating music compositions with AI, there is space to shape the output either by selecting the training dataset; by modifying the model parameters while interacting with it; or by iteratively guiding the selection of the output through the selection of various parameters, as in the case of 'Flowmachines'.[58] But the fact that this space exists does not mean that 'free and creative choices' are always expressed. As this depends on the specific case, the question of whether works created with AI are copyrightable has lawyers frequently answering: "it depends".

IV. Existing legislation on "computer-generated works"

23 Yet, some legal systems (Ireland, the UK, New Zealand, South Africa, India and Hong Kong) have special rules for 'computer-generated works', described as those generated where "there is no human author"[59] or "the author is not an individual."[60] Through a legal fiction, they grant the copyright of these works to "the person by whom the arrangements necessary for the creation of the work are undertaken"[61] or "the person who causes the work to be created."[62] While some advocate that this model is the best available, and should be adopted in more jurisdictions,[63] the issue is not satisfactorily addressed. A regulation that allows copyright to be granted to different persons on a case-by-case basis provides the necessary flexibility in this context. However, the vagueness of the terms "making the necessary arrangements" or "carrying out the creation of the work" is a point of criticism, as they are unclear as to what specific actions would be required to obtain copyright, thus requiring further interpretation.[64] Furthermore, these regulations classify as a 'work' a creation whose creative process is not original, and therefore must not be protected.[65] In fact, protecting "Authorless AI-assisted productions" by copyright is not optimal.[66]

56 Jean-Marc Deltorn and Franck Macrez, ´Authorship in the Age of Machine learning and Artificial Intelligence´ (2018) *Centre for International Intellectual Property Studies (CEIPI) Research Paper No. 2018-10* <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3261329>.

57 *Ibid.*

58 *Ibid: "The interaction between the neural network and the musician can also consist of a form of dialogue where the user can input a melody and where the system responds by either following up and continuing the priming musical sequence until the human counterpart takes over again, or by providing in return a variation on the initial proposed theme, that the musician can then select, discard, or build upon. This interactive creation is certainly at the core of Sony's Flow Machine creative process: ´In a typical session with Flow Machines, users first select a set of scores (lead sheets) that they want to take inspiration from. These scores determine the style of the scores generated by Flow Machines. Then they select a set of audio recordings that determine the sound textures of the audio stems generated by Flow Machines. Users can go back and forth between the generation of scores and the generation of audio renderings using an interactive interface, until they get a result they are satisfied with´. A particular expression of such a dialogue can take the form of co-improvisation between performers and the responses generated live (and adaptively) by an algorithmic process."*

59 Hong Kong, Ordinance 1997, Section 198 (1).

60 Irish Copyright and Related Rights Act 2000, Section 2.

61 UK CDPA 1998, Section 9.3; Irish Copyright and Related Rights Act 2000, Section 2(1); Hong Kong Copyright Act 2012, Section 11.3; New Zealand Copyright Act 1994, Section 5.2.

62 India Copyright Act 1957, Article 1. d).vi.

63 Annemarie Bridy, ´The Evolution of Authorship: Work Made by Code´ (2016), *39 Columbia Journal of Law & the Arts*, 395,401; Robert Denicola, ´Ex Machina: Copyright Protection for Computer-Generated Works´ (2016), *69 Rutgers University Law Review,* 251, 287; Andrés Guadamuz (n.49).

64 Jane.C. Ginsburg (n.49); Mercedes Morán, ´Creadores en riesgo de extinción´ (2018), *V Certamen de artículos jurídicos sobre Derecho del Entretenimiento, Premios DENAE* 25.

65 Jani Mccutcheon, ´Curing the Authorless Void: Protecting computer generated works, Following IceTV and Phone Directories´ (2013), *36(3) Melbourne University law review* 45,102; A Ramalho ´Will robots rule the (artistic) world? A proposed model for the legal status of creations by artificial intelligence systems´ (2017) *21 Journal of Internet Law* 12-25; Marta Duque Lizarralde (n.27).

66 In the US, it is also not possible to protect 'AI-generated works' under copyright. Section 306 of the Compendium of Practice of the US Copyright Office of 28 January 2021 expressly stipulates that the office register an original work of authorship, "*provided that the work was created by a human being*". Furthermore, section 313.2 specifies that machine-generated works, in which there is no creative input or human intervention, could in no case be copyrighted or

V. Possible ways forward

24 Some have suggested a reinterpretation of the concept of originality to protect such creations as long as they meet a certain degree of creative level and novelty.[67] The European Parliament, in the above-mentioned report, has also proposed an assessment of the advisability "of granting copyright to such a creative work to the natural person who prepares and publishes it lawfully, provided that the designer(s) of the underlying technology has/have not opposed to such use."[68] Nevertheless, this would contradict not only the current prevalent opinion in the academic community[69], but also the contemporary conception of copyright in the EU. The latter statement is particularly relevant considering that the CJEU in the *Levola v. Smilde* case reiterated the above-mentioned subjective criteria for assessing originality and ruled that the concept of a work "must normally be given an autonomous and uniform interpretation throughout the European Union."[70]

25 The European Commission (EC) has also addressed the topic in the Communication "Making the most of the EU's innovative potential. An intellectual property action plan to support the EU's recovery and resilience," published on 25 November 2020.[71] The EC followed the conclusions of the above-mentioned "Trends and developments in AI final report" and acknowledged that "creations autonomously created by AI technologies are still mostly a matter for the future", concluding that "AI systems should not be treated as authors". It also affirms that "the EU IP framework appears broadly suitable to address the challenges raised by AI-assisted creations," but maintains that there are gaps in harmonisation and margin for improvement, so dialogue with stakeholders is needed.[72]

D. D. Related Rights

I. Protection granted by existing related rights

26 Some have argued that authorless creations could be protected by certain related rights, such as the rights of phonogram producers[73], film producers[74], broadcasting organisations[75], publishers of press publications[76], and non-original photographs.[77] The reason is that these rights do not require originality or human authorship.[78] However, others claim that these rights are likewise conceived for human beings, and that legislative reform would be necessary to adapt their ownership.[79] In addition, it is also maintained that in most cases, authorless creations do not meet the requirements for protection set by

registered.

67 Susana Navas Navarro, ´Obras generadas por algoritmos, en torno a su posible protección jurídica´ (2018), *5(2) Revista de Derecho Civil*, 273,291; In a similar vein, Shlomit Yanisky-Ravid and Luis Antonio Velez- Hernandez, ´Copyrightability of Artworks Produced by Creative Robots and Originality: The formality-Objective Model´ (2018), *19(1) Minnesota Journal of Law, Science and Technology,* 51, 53. The authors argue that as the conclusion as to whether or not creative robots should have copyright in the works they generate depends on whether one views originality from a subjective or objective perspective, and conclude that adopting the objective perspective is more efficient, and that the requirement of originality should not hinder the recognition of copyright in works generated by creative and autonomous robots.

68 European Parliament (EP) Report (n.1) 13.

69 WIPO, ´ Summary of Second and Third Sessions, WIPO Conversation on Intellectual Property (IP) And Artificial Intelligence (AI)´ (4 November 2020) <https://www.wipo.int/edocs/mdocs/mdocs/en/wipo_ip_ai_3_ge_20/wipo_ip_ai_3_ge_20_inf_5.pdf >.

70 C-310/17, Levola Hengelo (2018) ECLI: EU: C: 2018:899, para33; Marta Duque Lizarralde (n.27).

71 COM(2020)760 EU - Communication Making the most of the EU's innovative potential An intellectual property action plan to support the EU's recovery and resilience <https://ec.europa.eu/docsroom/documents/43845/attachments/2/translations/en/renditions/native>.

72 *Ibid.*

73 Chapter II: Rights Related to Copyright, Directive 2006/115/EC of the European Parliament and of the Council of 12 December 2006 on Rental Right and Lending Right and on Certain Rights Related to Copyright in the field of Intellectual Property.

74 *Ibid.*

75 *Ibid.*

76 Art. 15 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.

77 Art. 6 Directive 2006/116/EC of the European Parliament and of The Council of 12 December 2006 on the term of protection of copyright and certain related rights.

78 Bernt Hugenholtz et al. (n.49).

79 Concepción Saiz García (n.48).

the related rights under which they are purported to be protected.[80]

27 More controversial is the question of whether authorless AI-assisted databases are protectable by the *sui generis* database right. For a database to be protected by this right, there must be substantial investment, quantitative or qualitative, either in obtaining, verifying, or presenting the content of the database.[81] Conversely, investment in the creation of data does not lead to protection.[82] In some cases it may be very cumbersome to determine whether the cost incurred by a legal database producer in developing and applying AI technology amounts to a substantial investment in data creation or collection. Even assuming that in this case the substantial investment is made in the collection of existing data, it might not be desirable for AI-generated data to be protected by the *sui generis* right. It has rightly been pointed out that in such a rapidly changing context, where new databases are constantly being produced, the risk is that protection may become perpetual, which could lead to anti-competitive effects.[83] Nevertheless, when AI is used to verify or present existing data, the result may be protected by the *sui generis* database right.[84]

28 Further research on this topic is indeed needed. What seems certain, however, is that those authorless creations that do not come within the scope of the existing related rights are unprotected and would fall into the public domain.[85] That said, the idea of authorless creation falling into the public domain is rejected by part of the academic community, and the introduction of a new related right is instead suggested.[86]

II. Creation of a new related right

29 Yet, the creation of a new related right may not be the best approach. Up to date there is neither economic nor theoretical justification (e.g., deontological or naturalistic), supporting that this related right would incentivise the creation of authorless AI-assisted productions, instead of producing saturation in the market.[87] What's more, it seems that while most jurisdictions do not have copyright or other exclusive rights to protect these productions, the development of AI, including creative AI, is in full swing.[88] Moreover, regardless of the protection of the results created by AI, those who use it as a tool to create content can benefit from first mover advantages.[89] Finally, sufficient tools are already available to those who employ creative AI systems to protect their results, such as trade secrets, factual

80 *Ibid;* Josef Drexl, Reto M. Hilty, Luc Desaunettes-Barbero, Jure Globocnik, Begoña Gonzalez Otero, Jörg Hoffmann, Daria Kim, Shraddha Kulhari, Heiko Richter, Stefan Scheuerer, Peter R. Slowinski and Klaus Wiedemann, ´Artificial Intelligence and Intellectual Property Law Position Statement of the Max Planck Institute for Innovation and Competition of 9 April 2021 on the Current Debate´ (2021) <https://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/MPI_PositionPaper__SSRN_21-10.pdf>: "*While in some situations AI-generated output can fall de lege lata under such protection, the desirability of such protection can be questioned from a welfare perspective*".

81 Art. 7 Directive 96/9/EC of The European Parliament and of The Council of 11 March 1996 on the legal protection of databases.

82 C-203/02, The British Horseracing Board and Others v William Hill Organization Ltd. EU:C:2004:695, para. 41, 42.

83 Josef Drexl, Reto M. Hilty et al. (n.80).

84 Bernt Hugenholtz et al. (n.49); Concepción Saiz García (n.48): contrarily, it has also been contended that databases created by an AI system may not be the result of the effort of their manufacturer, or may not have required large investment. Thus, the application of this right is not justified.

85 Bernt Hugenholtz et al. (n.49); Concepción Saiz García (n.48).

86 Anthoula Papadopoulou, ´Creativity in crisis: are the creations of artificial intelligence worth protecting?´ (2021), *12 JIPITEC,* 413,414; Ana Ramalho (n.65) argues that *"a disseminator's right, bearing a similar regime to the publisher's right in the publication of previously unpublished works as prescribed by the EU Term of Protection Directive, could be a solution."*. In favour of AI-created works falling into the public domain, see Daniel Gervais, ´The Machine as Author´ (2019) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3359524>.

87 Josef Drexl, Reto M. Hilty et al. (n.79); Mark Perry and Thomas Margoni, ´From Music Tracks to Google Maps: Who Owns Computer-generated Works? ´ (2010), *26 (6), Computer Law & Security Review,* 621,629: They claim that the introduction of a related right is likely to be contrary to the economic principle of maximising allocative efficiency, to become inefficient and to lead to market failures.

88 Jyh-An Lee, Reto Hilty and Kung.Chung Liu (eds.), *Artificial Intelligence and Intellectual Property* (Oxford University Press, 2021) 190,195.

89 Robert Yu (n.47) 1264, 1265; Marta Duque Lizarralde (n.27): For example, in the digital marketplace there is a high demand for immediately accessible content that is often hosted on websites that generate revenue from advertising. This implies that competitors compete to be first in the market to attract as many visitors as possible and increase their profits, for which AI can be of great help.

control, and unfair competition.[90] Rather than initially envisaging the creation of new exclusive rights, consideration should be given to the potential of these tools to provide adequate protection, and to whether further harmonisation, for example in the area of unfair competition, would be desirable.

E. Conclusions

30 In recent years, the debate on how to protect AI-generated works has become a hot topic. However, it should also be noted that nowadays AI systems belong to the category of narrow AI, as they can only perform specific tasks, and artificial general intelligence (AGI) is still science fiction. As highlighted by François Chollet, creator of Keras[91], "AI isn´t anywhere close to rivalling human screenwriters, painters, and composers. But replacing humans was always beside the point: AI isn't about replacing our own intelligence with something else, it is about bringing into our lives and work more intelligence, intelligence of a different kind. In many fields, but especially in the creative ones, AI will be used by humans as a tool to augment their own capabilities, more augmented intelligence than artificial intelligence".[92]

31 Many so-called 'AI-generated works' are actually 'AI-assisted works', in which human involvement in various stages of their creation remains relevant and original. Therefore, they do not raise concerns in terms of copyright protection. AI systems cannot generate works autonomously, without any human intervention. Hence, the discussion should focus on how, and whether it is desirable, to protect those AI-assisted productions in which a natural person's contribution to the final result is not original.

32 Definitions of AI-generated works, such as the one adopted by WIPO, do not reflect the current state of AI technology. Hence, a first step to progress in this debate is to strengthen the dialogue between the technical and legal sectors, and thus create a win-win situation for all. On the one hand, AI developers must have a proper IP strategy that allows them to make profits. On the other hand, those in the legal world must understand the technology and the market in order to advise on and regulate it, based on factually correct premises.

33 Copyright is not a suitable means for protecting authorless results. This is because they cannot meet the subjective criterion used by the CJEU in examining originality, nor the requirement that the author must be human, which is presupposed in some provisions of the Berne Convention and in some European directives.

34 Although some argue that authorless creations could be protected by certain related rights, further research is needed on this issue. In any case, introducing a new related right to protect authorless creations is not be the best solution. Those using creative AI systems may already have sufficient tools to protect their results.

90 Bernt Hugenholtz et al. (n..49); Marta Duque Lizarralde (n.27); Jean-Marc Deltorn and Franck Macrez (n.56).

91 Keras is one of the most relevant existing deep-learning frameworks. See Keras´s website: <https://keras.io/>.

92 François Chollet (n.23) 270.

Creations of artificial intelligence

In search of the legal protection regime

by **Anna Shtefan***

Abstract: Pictures, texts, music, sound recordings autonomously generated by artificial intelligence systems have already become part of the global market for goods and services. Unlike works and objects of related rights, AI-generated objects fall into the public domain from the moment of their appearance because there is no legal regime for their protection. Whether this status should be maintained in the future is one of the most difficult questions. In 2020, the European Parliament concluded that it is necessary to introduce legal protection for such objects but it has not yet been determined how this should be done. There are various scientific arguments in favour of such protection, which, however, raise reasonable doubts due to the fact that they are not confirmed by practice. Many proposals have been made regarding the legal regime for the protection of objects generated by AI without human participation, which are also quite controversial. This article examines the rationale for the legal protection of autonomous computer creations and possible concepts of their legal protection. Objecting to the protection of computer creations by copyright and related rights, this article justifies that, if the need for their legal protection is proven, it requires the development of a special legal regime.

Keywords: artificial intelligent; creativity; originality; copyright; intellectual property; legal protection; sui generis

Recommended citation: Anna Shtefan, Creations of artificial intelligence: in search of the legal protection regime, 14 (2023) JIPITEC 95 para 1.

A. Introduction

1 In the studies of intellectual property law in recent years, it is difficult to find a more debated issue than the legal protection of images, texts, music, sound recordings, and other similar objects created by artificial intelligence (AI) systems without direct human involvement. Although there are many initiatives to seek an appropriate legal regime, the legal systems of the world do not yet have an answer to the question of how to protect computer creations.

2 The European Parliament in the resolution on intellectual property rights for the development of artificial intelligence technologies of 20 October 2020 (EU Resolution) concluded that "technical creations generated by AI technology must be protected under the intellectual property rights legal framework", however, "works autonomously produced by artificial agents and robots might not be eligible for copyright protection, in order to observe the principle of originality, which is linked to a natural person, and since the concept of 'intellectual creation' addresses the author's personality" (para 15).[1] On April 21, 2021, the European Commission presented the Proposal for a Regulation laying down harmonised rules on artificial intelligence (EU Proposal for AI

* Doctor of Legal Sciences/Dr. Habil, (Law), Associate Professor, Head of the Copyright and Related Rights Department of the Intellectual Property Scientific Research Institute of the National Academy of Legal Sciences of Ukraine, Kyiv. The author can be contacted by email anna_shtefan@ukr.net.

1 European Parliament resolution of 20 October 2020 on intellectual property rights for the development of artificial intelligence technologies (2020/2015(INI)) <https://www.europarl.europa.eu/doceo/document/TA-9-2020-0277_EN.pdf> accessed 15 November 2022.

Regulation).[2] This document covers a wide range of issues related to the introduction and use of AI systems, but it lacks provisions for the protection of objects generated by AI. Therefore, the declared intention regarding their potential protection at the EU level has not yet been determined. Other jurisdictions also do not yet have a solution to this issue. Currently, at the global level, the results of the autonomous operation of a computer program are not protected, and in addition, some countries expressly prohibit the registration of copyrights on such objects.[3]

3 In studies of this issue, conclusions have been repeatedly made about the need for legal protection of objects generated by AI without human intervention, but today there is no convincing evidence that this is really necessary. Although scholars from different parts of the world have proposed a number of arguments in favour of the introduction of such protection, each of them raises reasonable doubts presented in this study. This article also briefly describes the essence of autonomous computer creations and considers possible regimes of their potential legal protection. As a result of the study, it is argued that if objects generated by AI without human intervention deserve legal protection, this requires the development of a special regime. However, the existing concepts of this special regime are still debatable and cannot yet serve as a basis for the adoption of legislation in this area.

B. Autonomous computer creation as a potential object of legal protection

4 For many years, software has served as a tool for creating works by analogy with other means, such as paints and brushes for drawing, pen and paper for writing. When computer technology is only a device for the implementation of creative ideas, there is no doubt that the result is a product of human activity. When a work is created with the help of AI, the possibility of human authorship depends on how much a person contributed to the creation of the work. If AI analysed certain data, and a person wrote an article based on it, or AI generated a series of colours, and a person drew a picture with these colours, that is, "AI was only employed as a tool for implementing human decisions",[4] it seems obvious that such a work was created by a person. When a person modifies or reworks an AI-generated object and makes certain creative choices, the end result may be considered a work created by that person; at the same time, the modification may have a purely technical nature, so each such case should be considered individually.[5] Along with this, there are many examples when an object is generated by a computer, and no person has had a direct creative influence on this object. Such objects are considered the results of the autonomous functioning of AI.

5 There are many definitions of AI that explain its nature and features. The most important aspect in understanding AI is that the term "intelligence" in this case means the ability of a computer to perform certain operations inherent in the human brain while AI as such is not a brain. It is a software that can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with (Art. 3(1) of the

2 Proposal for a Regulation of the European Parliament and the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206> accessed 15 November 2022.

3 In particular, according to the requirements of the U.S. Copyright Office, the registration is only possible for "an original work of authorship, provided that the work was created by a human being. The copyright law only protects 'the fruits of intellectual labor' that 'are founded in the creative powers of the mind'. Because copyright law is limited to 'original intellectual conceptions of the author', the Office will refuse to register a claim if it determines that a human being did not create the work". See: Compendium of U.S. Copyright Office Practices § 101 (3d ed. 2021), para 306.

4 Patrick Zurth, 'Artificial Creativity? A Case Against Copyright Protection for AI-Generated Works' (2021) 25(2) UCLA Journal of Law & Technology <https://uclajolt.com/wp-content/uploads/2021/12/Zurth_Artificial-Creativity.pdf> accessed 15 November 2022.

5 As the experts of the Max Planck Institute for Innovation and Competition concluded, "it is highly case-dependent whether 'works' generated with the help of AI tools can meet the protection threshold in view of the human creativity involved". See: Josef Drexl et al., 'Artificial Intelligence and Intellectual Property Law Position Statement of the Max Planck Institute for Innovation and Competition of 9 April 2021 on the Current Debate' (2021) <https://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/MPI_PositionPaper__SSRN_21-10.pdf > accessed 15 November 2022.

EU Proposal for AI Regulation).[6] It is a computer programme capable of performing specific tasks according to a built-in algorithm by processing information, analysing it, and giving definite results.[7] AI works with a huge amount of data that the human brain is not able to keep in memory, performs operations with this data that are inaccessible to humans without the use of technical means,[8] and in general, can process and structure information much better than one person or team do.

6 However, AI cannot think and generate new ideas. It is completely dependent on the functions programmed into it; it cannot go beyond its built-in algorithm and perform tasks not provided for in its codes. Moreover, AI "does not have the freedom to decide about its tasks and utilization by humans; it cannot define its own norms and goals."[9] Therefore, when we say that AI is able to autonomously generate certain objects, it is not an absolute concept but rather a relative category.

7 The main characteristics of autonomy can be considered "the ability to make independent decisions or draw conclusions"[10] while AI is able to make only those decisions that are provided by its codes. If AI is designed to write texts, it cannot decide to write music because its algorithm is not meant for this. It has only a certain technical autonomy, which means its ability to execute programmed commands without the need for constant human guidance and control, the ability "of producing outputs with minimal user input."[11] A person configures the AI, loads certain data into it, and gives a command to start the process of data analysis or synthesis of information based on the analysis, but a person does not control every step that the computer needs to take in the process of analysis or synthesis. AI performs this activity independently and this is where its autonomy is displayed.

8 The specificity of the functioning of many AIs is that no one knows and cannot predict what the specific content or the look of the object generated by AI will be. This phenomenon, the so-called "black box", is caused by the ability of AI to learn, create internal structures with data, and make choices among these data. No one can explain why AI made one or another choice, and "even the programmers cannot tell you why a specific output was generated."[12] Developers, end-users and other specialists who operate with AI know in advance the type of object that the algorithm is supposed to create (text, images, music, etc.), and may know the kind of this object. For example, The Next Rembrandt was designed to create a new portrait that imitates the style of Dutch artist Rembrandt Harmenszoon van Rijn.[13] It is quite clear that The Next Rembrandt will not paint a landscape or still life because its program codes are focused only on the image of a person. Nevertheless, no one knew what facial features and hairstyle the person in the portrait would have; all these elements are the result of a series of choices made by the computer based on preliminary calculations. Therefore, it is quite true to say that AI is "creating unpredictable works"[14] as the specific content of the generated object is not determined by a person, it is done by a computer.

9 Thus, an autonomous computer creation is the result of the functioning of AI with so little human intervention that the content of the generated object depends only on the choice of the computer and cannot be expected or predicted by humans. The special nature of these objects raised the question of whether they can receive legal protection and whether they should be protected at all.

6 Proposal for a Regulation (Artificial Intelligence Act), (n 2).

7 Anna Shtefan, 'Creativity and artificial intelligence: a view from the perspective of copyright' (2021) 16(7) *Journal of Intellectual Property Law & Practice* 720, 727.

8 According to Shlomit Yanisky Ravid, AI "breaks the data down into 'tiny' electronic signals, undetectable by humans, and tries to identify hidden insights, similarities, patterns, and connections." See: Shlomit Yanisky Ravid, 'Generating Rembrandt: Artificial Intelligence, Copyright, and Accountability in the 3A Era – The Human-like Authors are Already Here – A New Model' (2017) Michigan State Law Review 659, 676.

9 Tim W. Dornis, 'Of 'Authorless Works' and 'Inventions without Inventor' – The Muddy Waters of 'AI Autonomy' in Intellectual Property Doctrine' (2021) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3776236> accessed 15 November 2022.

10 Daniel J. Gervais, 'The Machine as Author' (2020) 105 Iowa Law Review 2053, 2098.

11 Jane C. Ginsburg and Luke Ali Budiardjo, 'Authors and Machines' (2019) 34 Berkeley Technology Law Journal 343, 433.

12 Aleksandre Asatiani et al., 'Challenges of Explaining the Behavior of Black-Box AI Systems' (2020) 19(4) MIS Quarterly Executive 259, 259-260.

13 Next Rembrandt <https://www.nextrembrandt.com/> accessed 15 November 2022.

14 Shlomit Yanisky Ravid, (n 8) 679.

C. Issues of justification for the protection of AI-generated objects

10 AI-generated objects are already part of the world market.[15] They are sold in the same way as copyrighted works but unlike works, the use of which can be authorised or prohibited by the author or another right holder, there is no such authority for objects created by AI. Currently, everyone can use these objects as they wish and benefit commercially, and AI investors have no control over this because computer-generated works belong to the public domain. The question, however, is whether this status should be maintained in the future.

11 There are various arguments against the introduction of the legal protection for the results of autonomous functioning of a computer. In particular, people should be able to freely use machine results in their own creativity or other activities that will benefit society; that is, objects generated by AI should serve the benefit of humanity, and access to them should not be restricted by establishing a regime of their legal protection.[16] Also, there is potential for negative impact of these objects on the market of human works, as these objects "may create value in some areas, but it will pose risks in others, not the least of which is to the future of human creativity".[17] Considering that AI can produce many conventionally new results per day, it is possible that these objects will supplant the results of human creativity since humans are unable to compete with computers in the frequency and number of new proposals. As a result, it will at least reduce the income of authors, and in some sectors, it can significantly devalue human creativity. However, if computer creatures stay in the public domain, this "would ensure that humans remain an integral part of the creative fields".[18] It is widely believed that legal protection of the results of the autonomous functioning of a computer will lead to excessive rewards for AI developers and other persons who provide the functioning of AI. Since these persons receive remuneration for their work as employees of the company or independent specialists engaged on the basis of contracts, as well as receive a copyright or patent for AI as software and hardware, additional protection of their interests is considered unreasonable.[19] In addition, Zurth states that the legal protection of the computer creatures may give rise to a large number of monopolies which in general will have a negative effect on innovation since "the access to that technology is limited to relatively few actors; the monopolies to be concentrated among those who are already powerful".[20]

12 These opinions are quite interesting for analysis and discussion since there is no data to confirm that the refusal to grant legal protection to AI-generated objects will have a significant public benefit or prevent a threat to the interests of authors or society. However, these arguments deny the possibility of legal protection of autonomous computer creations while the purpose of this article is to find evidence in favour of granting such protection.

13 The legal protection of intellectual property can be justified by the purpose of ensuring the interests of the creator or the purpose of protecting investments. In the first case, it concerns the establishment of legal means that will be able to reward the creative efforts of persons and provide them with economic incentives for creativity. The second case may be related to the support of financial, organizational, and other non-creative efforts made in the creation of certain objects and ensuring the normal functioning of the market; "relying on remedying a market failure in public goods markets."[21] There is no doubt that AI as such does not need moral and economic incentives to function and generate certain objects. Therefore, the main argument for the introduction of the legal protection of autonomous computer creations is to support innovators in the AI industry, to encourage and protect investments made in the creation and operation of AI.

14 This position states that in the absence of legal protection "innovators may eventually shy away from investing their time and effort in this field",[22]

15 For example, the site https://booksby.ai/ sells science fiction novels generated by AI.

16 As Daniel Schönberger noted, "What would be so negative about robot-creation falling into the public domain anyway? Might it not be seen as a chance to give birth to new artistic genres and whole new areas of innovation, where humans could build freely upon initial machine-output? The fruits of AI should be used for the good of society." See: Daniel Schönberger, 'Deep Copyright: Up – And Downstream Questions Related to Artificial Intelligence (AI) and Machine Learning (ML)' (2018) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3098315> accessed 15 November 2022.

17 Daniel J. Gervais, (n 10) 2060.

18 Victor M. Palace, "What if Artificial Intelligence Wrote This? Artificial Intelligence and Copyright Law" (2019) 71(1) Florida Law Review 217, 242.

19 Tim W. Dornis, (n 9).

20 Patrick Zurth, (n 4).

21 Josef Drexl et al., (n 5).

22 Nina I. Brown, 'Artificial Authors: A Case for Copyright in Computer-Generated Works' (2019) 20(1) Science and

"non-protection of emergent works lowers the overall level of investment in technical innovation and, ultimately, the actual production of creative AI."[23] Legal protection is needed to "promote the development of AI systems' programming and encourage entities to control the functions of AI systems and to take responsibility for their outcomes."[24] The criterion of protecting economic interests and supporting investments is also the basis of the conclusion in the EU Resolution (para 15).[25] It is quite possible to assume that without the protection of their economic interests, investors will not be interested in funding further AI development and research which could result in a significant reduction in the development of this field, and its potential social benefits will not be achieved. However, this assumption does not find practical confirmation.

15 First, the lack of legal protection does not have a negative impact on the development of AI; on the contrary, the scope of investment in this area is constantly increasing. Only in the USA, funding for AI companies has increased from a little under 300 million U.S. dollars in 2011 to around 16.5 billion in 2019;[26] the global AI software market is forecast to reach around 126 billion U.S. dollars by 2025.[27]

16 Second, belonging of AI-generated objects to the public domain does not create obstacles to their participation in the market circulation and does not limit the possibility of their sale in comparison with protected works. So far, there are no known negative market phenomena caused by the lack of legal protection of AI-generated objects. In this context, the opinion was expressed that recognition of rights to AI-generated objects "would be justified only if solid empirical economic analysis were to reveal that the absence of legal exclusivity negatively affects overall economic welfare."[28] That is, there must be a certain market failure that could be overcome by introducing legal protection of the results of autonomous operation of the computer but there is no data on such market failure yet.

17 Third, investors have not yet taken the initiative to obtain rights to AI-generated objects. It is fair to say that "whoever intends to establish a monopoly through an exclusive right has to prove its economic efficiency and necessity";[29] this is the approach that has been historically developed in the field of intellectual property. In particular, in the 15th century, after the invention of the printing press, publishers secured privileges that protected their investments and limited competition with other publishers. At the end of the 17th century, there was a powerful movement to protect the interests of authors which culminated in the adoption in 1710 of Queen Anne's Statute, the first copyright law.[30] Similarly, in due time, producers of phonograms and broadcasting organizations proved that they need protection from the use of their phonograms and broadcasts by third parties; this resulted in the adoption of the Rome Convention in 1961 which established legal protection of related rights.[31] As for AI investors, there have been no such initiatives from their side so far. It is paradoxical that this issue is actively discussed by scientists, while it is not known whether investors themselves seek legal protection for autonomous creations of their ward computers.

18 Thus, the purpose of investment protection is not yet supported by any data that would indicate the need to guarantee such protection. I am inclined to believe that the interests of investors can serve as a basis for providing them with legal means of influencing the use of objects generated by AI and the possibility of obtaining economic benefits from it. Nevertheless, there is currently no evidence that this is really

Technology Law Review 1, 5.

23 Tim W. Dornis, 'Artificial Creativity: Emergent Works and the Void in Current Copyright Doctrine' (2020) 22 Yale Journal of Law & Technology <https://yjolt.org/sites/default/files/22_yale_j.l._tech._1_ai_creativity.pdf> accessed 15 November 2022.

24 Shlomit Yanisky Ravid, (n 8) 701.

25 EU resolution (n 1).

26 Bergur Thormundsson, 'Artificial Intelligence funding United States 2011-2019' (2022) <https://www.statista.com/statistics/672712/ai-funding-united-states/> accessed 15 November 2022.

27 Bergur Thormundsson, 'Artificial intelligence software market revenue worldwide 2018-2025' (2022) <https://www.statista.com/statistics/607716/worldwide-artificial-intelligence-market-revenues/> accessed 15 November 2022.

28 Christian Hartmann et al., 'Trends and Developments in Artificial Intelligence. Challenges to the Intellectual Property Rights Framework: Final report' (European Commission: 2020), 95 <https://www.ivir.nl/publicaties/download/Trends_and_Developments_in_Artificial_Intelligence-1.pdf> accessed 15 November 2022.

29 Patrick Zurth, (n 4).

30 Delia Lipszyc, *Copyright and neighbouring rights* (UNESCO Publishing 1999) 39-40.

31 Guide to the Rome Convention and to the Phonograms Convention (1981) WIPO publication No. 617(E) 10-12 <https: wipo.int/edocs/pubdocs/en/copyright/617/wipo_pub_617.pdf> accessed 15 November 2022.

necessary for investors. Taking into account that legal protection provides not only benefits but also imposes certain obligations on the right holder, including liability for possible violations committed in the course of AI functioning, investors may not wish to receive such protection at all.[32]

19 Another approach, which supports the need for the legal protection of the results of the autonomous functioning of a computer, focuses on market competition. It is believed that consumers may confuse the results of human creativity with cheaper computer creations, which can create unfair competition.[33] It is impossible to reliably predict what the competition will be like when more AI-generated objects appear on the market; at the same time, there is no reason to believe that they will be in greater demand than works due to lower cost or any other reasons. The consumers' choice of a creative product is determined by various factors and the low cost of the product is decisive only for a certain part of consumers. The demand for creative products, regardless of their origin, will always be different, some of them become part of mass culture, and some occupy only a small niche. Furthermore, there are no studies or other data that would indicate that there is a real threat to market competition due to the fact that computer creations are not protected.

20 An additional argument for the introduction of the legal protection is that its absence may encourage abuse. Human authors who have created works using AI technologies can hide the AI's involvement in the creation of the work because it "would make the resulting works unprotectable."[34] Investors may start claiming authorship of objects created by AI and get copyright protection on things they did not create[35] while the true origin of such objects will be deliberately concealed.[36] This is quite realistic if the object has commercial potential for use similar to the use of the work, and there is no mechanism for its protection. Taking into account the presumption of authorship according to which, until proven otherwise, the person whose name appears on work is considered the author, and the AI will not be able to prove that the creation of this object is the result of the autonomous operation of a computer. On the other hand, the availability of the legal protection for AI-generated objects will not necessarily avoid abuse. If the duration of such protection is relatively short, certain investors may assign authorship to computer creations because long-term copyright protection will be more profitable for them. Accordingly, the goal of avoiding theoretically possible abuses does not seem sufficient to explain the expediency of legal protection of AI-generated objects.

21 The above shows that it is difficult to find a convincing and properly confirmed argument in favour of the introduction of the legal protection for autonomous computer creations. However, given that the European Parliament has expressed such an intention, the question of a possible legal regime of protection remains relevant and needs to be answered.

32 It is worth supporting the opinion that "if the grant of rights in robot creations implies liability for potential infringements of third party rights, robot users may find the acquisition of rights no longer attractive. The risk of liability for infringement may thwart the attainment of the goals of incentive theory. Instead of seeing the grant of protection as a stimulus for stronger efforts to develop the full potential of creative AI machines, robot users may eschew the right holder status to escape liability for potential infringements". See: Martin Senftleben and Laurens Buijtelaar, 'Robot Creativity: An Incentive-Based Neighboring Rights Approach' (2020) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3707741> accessed 15 November 2022.

33 In particular, Anthoula Papadopoulou explained a need for a specific legal protection of AI-generated objects by the proper functioning of competition rules: "once a work or an AI-generated output is exploited, it is on a market, which would thus justify applying competition law. In any case, the perception of the AI output as a creative one by the average consumer combined with the expectedly low price compared to human creations of art could possibly create conditions of unfair competition and consumer deception". See: Anthoula Papadopoulou, 'Creativity in crisis: are the creations of artificial intelligence worth protecting?' (2021) 12(3) JIPITEC para 21.

34 Enrico Bonadio and Luke McDonagh, 'Artificial Intelligence as Producer and Consumer of Copyright Works: Evaluating the Consequences of Algorithmic Creativity' (2020) 2 Intellectual Property Quarterly <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3617197> accessed 15 November 2022.

35 In this regard, Tim W. Dornis noted that owners and users of autonomous AI applications "will instead portray themselves (as humans) as authors or creators of the emergent works at issue. It will be hard, if not impossible, to solve this problem in practice since the relevant facts are virtually always private. Quite paradoxically, this practical disincentive may ultimately result in the acquisition of full copyright protection for emergent works – particularly if the AI owner or user succeeds in establishing herself as the author or creator". See: Tim W. Dornis, (n 23).

36 Kalin Hristov, 'Artificial Intelligence and the Copyright Dilemma' (2017) 57(3) IDEA 431, 450.

D. Potential regimes of the legal protection of AI-generated objects

22 There are three main theories regarding the regime that will be most justified and appropriate for the protection of AI-generated objects: 1) copyright; 2) related (neighbouring) rights which are valid in European countries for the protection of performances, phonograms, broadcasts, and some other objects; 3) a separate special regime. Further analysis will demonstrate that the legal protection of computer creations if it is considered appropriate and necessary, requires the development of a special legal regime that does not interfere with the intellectual property paradigm.

I. Copyright

23 The copyright system is formed around the figure of the author, a person who created a work through their creative efforts. The laws of many European countries, in particular, Bulgaria,[37] Latvia,[38] Lithuania,[39] Malta,[40] Romania,[41] Slovakia,[42] Slovenia,[43] Spain,[44] Switzerland,[45] directly determine that an author is only a natural person. In other countries where there is no such specification, the limitation of the circle of authors to natural persons follows from the provision of the general term of copyright which is the life of the author and a certain period after their death. The categories "life" and "death" are characteristic only of living beings, and since animals are recognised by the legislation of most countries as a special object of law and not a subject and participant in legal relations, by the method of logical exception in the category of "author" only human beings remain.

24 AI does not fit into the copyright paradigm because it is not human and, unlike humans, can exist indefinitely. This, however, did not prevent the emergence of various theories regarding the extension of copyright to computer creations. It was proposed to grant copyright for autonomous computer creations to the AI itself,[46] or to the developer,[47] or to the end user,[48] or to consider that the object generated by the AI is a work for hire.[49] There are many objections to such proposals, justified by the fact that the purpose of copyright is to encourage human creativity[50] while

37 Art. 3(1) of Law on copyright and related rights of Bulgaria <https://wipolex.wipo.int/en/text/544110> accessed 15 November 2022.

38 Art. 1(1) of Law on copyright of Latvia <https://wipolex.wipo.int/en/text/520008> accessed 15 November 2022.

39 Art. 6(1) of Law on copyright and related rights of Lithuania <https://wipolex.wipo.int/en/text/349855> accessed 15 November 2022.

40 Art. 2 of Copyright act of Malta <https://wipolex.wipo.int/en/text/355524> accessed 15 November 2022.

41 Art. 3(1) of Law on copyright and related rights of Romania <https://wipolex.wipo.int/en/text/545969> accessed 15 November 2022.

42 Art. 13(1) of Law on copyright and related rights of Slovakia <https://wipolex.wipo.int/en/text/542163> accessed 15 November 2022.

43 Art. 10 of Copyright and related rights act of Slovenia <https://wipolex.wipo.int/en/text/582063> accessed 15 November 2022.

44 Art. 5(1) of Law on intellectual property of Spain <https://wipolex.wipo.int/en/text/584952> accessed 15 November 2022.

45 Art. 6 of Federal act on copyright and related rights of Switzerland <https://wipolex.wipo.int/en/text/584729> accessed 15 November 2022.

46 According to Tess Buckley, "AI is creative in its own right: therefore, it should have partial ownership/authorship of its creations. As a creator, autonomous robots should receive the copyrights of that which it produces". See: Tess Buckley, 'Computers, Creativity and Copyright: Autonomous Robot's Status, Authorship, and Outdated Copyright Laws' (2019) <https://montrealethics.ai/computers-creativity-and-copyright-autonomous-robots-status-authorship-and-outdated-copyright-laws/> accessed 15 November 2022.

47 In the opinion of Atilla Kasap, "the programmer who invested skill, labor, and other resources to design the AI-system producing the creative output is the best candidate for authorship as far as copyright law is concerned". See: Atilla Kasap, 'Copyright and Creative Artificial Intelligence (AI) Systems: f Twenty-First Xentury Approach to Authorship of AI-Generated Works in the United States' (2019) 19(4) Wake Forst Journal if Business and Intellectual Property Law 335, 369.

48 Robert C. Denicola, 'Ex Machina: Copyright Protection for Computer-Generated Works' (2016) 69 Rutgers University Law Review 251, 286-287.

49 Annemarie Bridy, 'The Evolution of Authorship: Work Made by Code' (2016) 39 Columbia Journal of Law & the Arts 395, 400; Shlomit Yanisky Ravid, (n 8) 707-717; Kalin Hristov, (n 36) 446-451.

50 In words of Daniel J. Gervais, "copyright is a legal mechanism designed to help produce works that are the result of a human creative process; the incentive is for humans to engage in the process not knowing whether the result will

a computer creation made without direct human intervention does not meet the conditions of copyright protection. Joining these objections, I would like to give reasons why AI does not create works that could be protected by copyright.

25 There is no definition of a work in international copyright treaties because it is a philosophical and universal category rather than a legal one. Therefore, most national copyright laws do not interpret the concept of a work, but only provide a non-exhaustive list of them. To some extent, I can agree with the opinion that "the work is simply not subject to an all-purpose formal definition",[51] after all, each type of work has its own characteristics which cannot be reflected in one common definition. However, a general concept of a work should exist since it is one of the central categories of copyright.

26 Many European states explain in their legislation that a work is the result of creative activity;[52] an original intellectual creation;[53] an original intellectual creation having an individual character.[54] All these definitions express the main essence of the work: it is the result of the intellectual creative activity of the author. Copyright is indifferent to the process of creating a work and the idea behind it; it extends only to the result that crowned the implementation of a particular idea. At the same time, not every result of a human activity receives legal protection but only those that appear as a product of creative efforts.

27 The concept of creativity is one of the most complicated. Different theories of creativity treat it from different positions and with different criteria, so there is no generally accepted definition that will suit all possible cases. In terms of copyright, creativity is essentially a reflection or transformation of reality, embodied in a certain form. The reflection of reality occurs when the author embodies prototypes of objects, fragments of nature, or other elements of human life that exist in the real world. The transformation of reality takes place when the author invents something that does not exist in reality, and the work itself may be aimed at forming such a result (for example, the invention of new technology), or this result may not appear in the real world (for example, a fantastic creature from another planet).[55] Copyright does not explain the essence of creativity but widely applies its main feature, namely, originality, as a criterion for granting copyright protection.

28 In the EU, the concept of originality was first formulated in Directive 91/250/EEC regarding computer programs that shall be protected if it is original in the sense that it is the author's own intellectual creation (Art. 1(3)).[56] Later, the copyright protection of photographs (Art. 6 of Directive 93/98/EEC[57]) and databases (Art. 3(1) of Directive 96/9/EC[58]) was determined according to the same criterion. In sum, the definition "the author's own intellectual creation" "constituted a European criterion for originality, at least for these categories of works"[59] and some states have reflected this provision in their legislation.[60] The CJEU explained originality as having several components: "the work is original in the sense that it is its author's own intellectual creation; an intellectual creation is an author's own if it reflects the author's personality; if the author

be a blank page or the Great American Novel". See: Daniel J. Gervais, (n 10) 2093. Martin Senftleben and Laurens Buijtelaar noted that "copyright protection is justified as far as it is necessary to provide the incentive needed to encourage the creation and dissemination of creative expression". See: Martin Senftleben and Laurens Buijtelaar, (n 32).

51 Michael J. Madison, 'The End of the Work as We Know It' (2012) 19(2) Journal of Intellectual Property Law 325, 332.

52 Art. 3(1) of Law of Bulgaria (n 37); Art. 2(1) of Law on copyright and related rights of Czech Republic <https://wipolex.wipo.int/en/text/546060> accessed 15 November 2022; Art. 1(2) of Law of Latvia (n 38); Art. 2(19) of Law of Lithuania (n 39).

53 Art. 1(1) of Federal law on copyright in literary and artistic works and related rights of Austria <https://wipolex.wipo.int/en/text/503811> accessed 15 November 2022; Art. 2(1) of Law on copyright, related rights and cultural matters of Greece <https://wipolex.wipo.int/en/text/480967> accessed 15 November 2022.

54 Art. 5(1) of Copyright and related rights act of Croatia <https://wipolex.wipo.int/en/text/537702> accessed 15 November 2022; Art. 2(1) of Law of Switzerland (n 45).

55 Anna Shtefan, (n 7) 725.

56 Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs, *OJ L 122.*

57 Council Directive 93/98/EEC of 29 Oct. 1993 harmonizing the term of protection of copyright and certain related rights, *OJ L 290.*

58 Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, *OJ L 77.*

59 Tatiana Synodinou, 'The Foundations of the Concept of Work in European Copyright Law' in Synodinou (ed.) *Codification of European Copyright, Challenges and Perspectives* (Kluwer Law International: 2012), 97.

60 In particular, according to Art. 4(2) of Copyright act of Estonia, a work is original if it is the author's own intellectual creation <https://wipolex.wipo.int/en/text/510476> accessed 15 November 2022.

was able to express their creative abilities in the production of the work by making free and creative choices".[61]

29 In other jurisdictions, the interpretation of originality may differ slightly. Nevertheless, so far there is no other understanding of it than the independent creation of a work and the creative choice or expression of the author.[62] Originality lies in the fact that the author independently selects the way to implement their idea in the work, not copying the works of other authors but following their own path. Each author has their own system of values, a spiritual world, aspirations, feelings and experiences, and each work contains a particular mental and emotional contribution of the author who reflects their personality through their work.[63]

30 Unlike a human, AI has only a built-in algorithm, according to which it is capable of performing specific tasks by processing information, analysing it, and giving results. Works of a particular type are loaded into AI designed to generate objects similar to copyrighted items. These works serve as the subject of analysis and a pattern based on which an object with the same expression appears. The computer performs algorithmic calculations and makes a choice that results in text, images, music, etc, by analysing and comparing specific data. Any object generated by AI is the result of synthesizing certain data based on its analysis.[64]

31 Generating a particular object in the course of its operation, AI makes a series of choices. However, is there any reason to believe that any of these choices are creative? This question is quite rightly asked by researchers who do not believe in the possibility that the results of the autonomous activity of a computer program can be protected by copyright. According to a fair statement by Anthoula Papadopoulou, "the free and creative choices that leave the author's personal touch, as established by the CJEU, cannot be equated with random outputs by neural networks".[65] Indeed, there is no evidence that AI makes something more than purely technical choices based on its calculations. Unlike a person, AI is not aware of its activity and does not manage it but only obeys the tasks assigned to it and executes its programmed commands. Every choice it makes is the fulfilment of a function provided for in its codes, not the result of its own will. There is even less reason to believe that the computer expresses something in its creation. There is no deep meaning or subtext in an object created by AI because a computer has no personality, inner self, feelings, or beliefs that could affect the work as it does in human creation. Thus, an AI-generated object is not original because there is no creative choice behind it, and it does not contain the imprint of any personality. Therefore, AI is not capable of creating works that could be protected by copyright.

32 The mission of copyright is focused on people and their creativity. This priority should not disappear under the influence of the need to protect the economic interests of persons investing in AI. Even if in the future AI is developed that can independently decide to generate a certain object and do things that are not provided for by its program codes, it will still remain an imitation of creativity. Therefore, I cannot agree with the thesis that "the traditional solution to look for the human behind the creative process is untenable in the long run".[66] A computer will never have an analogue of a human personality and will not be able to feel the need for self-expression, and therefore its creations will lack the personal touch that characterises human creations. A computer will never become a full-fledged author: as Ana Ramalho aptly observed, "real authorship seems to be linked to the quality of being human"[67] which is not possible with the most advanced technology.

33 No matter how technology develops further, AI will never acquire human traits and characteristics, and its work will never replace human creativity. Currently, AI is only able to generate something by using something that humans have already created. Even if future AIs become autonomous in making the decision to create an object and are able to go beyond

61 Judgment in *Eva-Maria Painer v Standard Verlags GmbH*, Axel Springer AG, Süddeutsche Zeitung GmbH, SPIEGEL-Verlag Rudolf AUGSTEIN GmbH & Co KG and Verlag M. DuMont Schauberg Expedition der Kölnischen Zeitung GmbH & Co KG, C145/10, ECLI:EU:C:2011:798, para 87–89.

62 For instance, in the USA originality means that the work was independently created by the author (as opposed to copied from other works), and that it possesses at least some minimal degree of creativity (the selection should have a modicum of creativity; there is nothing remotely creative about a work that merely reflects an age-old practice, firmly rooted in tradition and so commonplace that it has come to be expected as a matter of course). See: Feist Publications, Inc, v Rural Telephone Service Co, 499 US 340 (1991), para 10, 55, 57.

63 Anna Shtefan, (n 7) 727-728.

64 Anna Shtefan, (n 7) 727.

65 Anthoula Papadopoulou, (n 33) para 13.

66 Shlomit Yanisky Ravid, (n 8) 726.

67 Ana Ramalho, 'Will robots rule the (artistic) world? A proposed model for the legal status of creations by artificial intelligence systems' (2017) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2987757> accessed 15 November 2022.

the limits of their programmed functionality, they will not learn to make creative choices. It requires a human personality, soul, and inner world, which cannot be created by technology. Creativity is the exclusive prerogative of humans while AI can only imitate creative processes. Hence, copyright must remain the legal regime only for the protection of human creativity.

II. Related (neighbouring) rights

34 In European countries, related (neighbouring) rights protect objects that do not belong to works, namely, performances, phonograms, audio-visual recordings, broadcastings, and some other objects that are individually determined by the legislation of certain states. These objects do not require originality and human authorship that quite logically led to the formation of a proposal to protect AI-generated objects with related rights. This decision is advantageous because "it allows the introduction of a period of protection that is long enough to enable the user of a creative robot to recoup his investment, but still short enough to prevent unnecessary obstacles to transformative remix activities that support cultural follow-on innovation".[68] In this regard, two approaches have been developed on how to implement this proposal.

35 The first idea boils down to extending related (neighbouring) rights to similar objects generated by AI. Sound recordings can be protected as phonograms, audio-visual recordings may qualify for protection under the film producer's right, and broadcasts may find protection under the related rights of broadcasters.[69] This suggestion fails to consider that only some AI-generated objects fall into the category of traditional objects of related (neighbouring) rights. These are, in particular, texts and paintings, and if in the future AI begins to generate architectural projects or computer programs, the issue of their legal protection will remain unresolved.

36 The second idea is to create a category of new related (neighbouring) rights that would apply to all AI-generated objects. Within this approach, it is proposed "requiring substantial investment as a pre-condition"[70] while "the duration can be shorter and the exclusive rights granted can be lesser when compared with copyrighted works."[71] In this way, it is possible to solve the issue of protection of texts, pictures, and other creations that differ from traditional objects of related rights. However, on the other hand, there may be a problem in distinguishing between "ordinary" and "special" related (neighbouring) rights; it will be unclear which object is created by humans and which is generated by AI. There are also doubts about the proposed criterion for granting protection, namely, the substantial investment. Evaluation of such investments can be quite problematic, as there is no generally accepted understanding of what amount of investment in the creation and operation of AI is considered significant enough. In addition, investors may not wish to disclose such information, they will refuse to evaluate the investment and, accordingly, to obtain legal protection. This calls into question whether the application of such a criterion could be useful.

37 New related (neighbouring) rights are actually a special regime of legal protection that has a common name but a completely different content compared to related (neighbouring) rights protected in Europe. Taking into account that there are other proposals to apply a special regime to AI-generated objects, it is advisable to consider these proposals separately and in more detail.

III. A special regime

38 In the field of intellectual property, a special regime is usually associated with sui generis right. It can be defined as a special kind of right that operates within a certain regime and defines particular aspects of legal regulation that apply in individual cases. European legislation establishes such a right for one object, namely, databases. According to the provisions of Directive 96/9/EC on the legal protection of databases, the sui generis right is granted to ensure the protection of substantial investment that may consist in the deployment of financial resources and/or the expending of time, effort, and energy. The objective of this sui generis right is to give the maker of a database the option of preventing the unauthorized extraction and/or re-utilization of all or a substantial part of the contents of that database.[72]

68 Martin Senftleben and Laurens Buijtelaar, (n 32).

69 Christian Hartmann et al., (n 28) 117.

70 Anke Moerland, 'Artificial Intelligence and Intellectual Property Law' (2022) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4203360> accessed 15 November 2022.

71 Tianxiang He, 'The Sentimental Fools and the Fictitious Authors: Rethinking the Copyright Issues of AI-Generated Contents in China' (2019) 27(2) Asia Pacific Law Review 218, 235.

72 Para 40, 41 of the Preamble, Art. 7(1) of the Directive 96/9/EC (n 58).

39 In 2018, the European Commission evaluated the effectiveness of this Directive and noted that a sui generis right has overall policy potential and the limited range of problems it currently generates for stakeholders. At the same time, despite providing some benefits at the stakeholder level, the sui generis right continues to have no proven impact on the overall production of databases in Europe, nor on the competitiveness of the EU database industry.[73] There are doubts about the effectiveness of this special regime since its economic impact "was unproven, and that it comes perilously close to an undesirable property right in data as such".[74] Nevertheless, the idea that objects generated by AI without direct human participation can be protected by a sui generis right has become quite widespread. Some studies consider the possibility of applying the provisions of Directive 96/9/EC to AI-generated databases.[75] Meanwhile, there are justifications for the development of a separate special regime for the protection of autonomous computer creations—that is, a new sui generis right.

40 The advantages of a sui generis right can be explained by the fact that this regime will provide only certain limited protection that will allow investors to influence the possibility of using AI-generated objects, and at the same time will not create risks of devaluation of human creativity. As the supporters of this approach justify, this "could reinforce investment without pressuring and deconstructing concepts such as originality and creativity",[76] "would allow for more flexibility and prevent the mass production of work that would create a reverse merger situation."[77] Indeed, the development of special legislative provisions that do not interfere with the intellectual property paradigm and do not create conflicts with the regime of the legal protection of works may be the most appropriate solution to protect the results of the autonomous functioning of a computer. At the same time, the summary of existing scientific developments suggests that in general there is no clear concept of a special regime for AI-generated objects but there are a number of questions that need to be answered.

41 First, it is necessary to determine which objects may be subject to legal protection. If we are referring to all objects that can be created by AI, this could potentially include those that should not be protected at all by any regime that provides a monopoly on their use. In particular, reports of current events in the form of ordinary press information are excluded from the scope of copyright due to lack of originality, but if such reports made by AI fall under a sui generis right, this will prevent the free dissemination of information. Therefore, it is important to provide a list of AI-generated objects that will not be protected by sui generis right.

42 Second, there is still no consensus on whether any criteria should be applied for the protection of these objects. There are opinions that for attracting the sui generis protection, "an originality test as assessed and interpreted objectively and contextually would be appropriate";[78] to be eligible for the sui generis protection, AI-generated works "should be independently created by an AI system with contributions from the system's developer and possess a minimal degree of creativity" in the meaning that "it cannot consist solely of designs that are staple, commonplace, or familiar in the semiconductor industry, or variations of such designs, combined in a way that, considered as a whole, is not original."[79] These proposals contradict the general idea of establishing a separate legal protection regime that should not apply the categories of authorship, creativity, and originality. Given that a computer is not capable of making a creative choice, it is difficult to justify what exactly should be the basis for assessing the presence of a minimum degree of creativity. Therefore, an attempt to adapt the copyright criterion of originality to computer creations does not seem to be the best idea. Another potential condition that could determine the protectability of AI-generated objects is a substantial investment, as provided by Directive

73 European Commission, Commission Staff Working Document: Executive Summary of the Evaluation of Directive 96/9/EC on the Legal Protection of Databases, SWD (2018) 147 final (Apr. 25, 2018) <https://digital-strategy.ec.europa.eu/en/library/staff-working-document-and-executive-summary-evaluation-directive-969ec-legal-protection-databases> accessed 15 November 2022.

74 Mireille van Eechoud, 'Please share nicely – From Database directive to Data (governance) acts' (2021) Kluwer Copyright Blog <http://copyrightblog.kluweriplaw.com/2021/08/18/please-share-nicely-from-database-directive-to-data-governance-acts/> accessed 15 November 2022.

75 Guido Noto La Diega, 'Comments on WIPO's 'Draft Issues Paper on Intellectual Property and Artificial Intelligence' (WIPO/IP/AI/2/GE/20/1)' (Apr. 3, 2020) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3551908> accessed 15 November 2022.

76 Anthoula Papadopoulou, (n 33) para 22.

77 Vicenç Feliú, 'Our Brains Beguil'd: Copyright Protection for AI Created Works' (2021) 25(2) Intellectual Property and Technology Law Journal 105, 124.

78 Enrico Bonadio and Luke McDonagh, (n 34).

79 Haochen Sun, 'Redesigning Copyright Protection in the Era of Artificial Intelligence' (2022) 107(3) Iowa Law Review 1213, 1244.

96/9/EC on databases.[80] However, as noted above, the need to prove a significant amount of investment may discourage potential rightsholders from obtaining legal protection. Thus, the only reasonable criterion for the application of a sui generis right so far remains that the object is generated by a computer without direct human intervention.

43 Third, the question of who exactly should acquire a sui generis right to the results of the autonomous functioning of the computer remains debatable. Different points of view have been expressed on this issue. In particular, it was concluded that a sui generis right should "encourage the creation of these technologies (through the offer of exclusive rights)",[81] that is, it should be guaranteed to AI developers. Also, the possibility of joint ownership between developers and users was considered.[82] There is also an opinion that the acquisition of the right should be carried out "in a combination of the user of the system, programmer of the learning algorithm of the creative agent and/or the creative agent itself can become a reality in a sui generis system".[83] By analogy with the regime of works made for hire, it is proposed to consider the user as a person who may have a sui generis right, but since the user is usually an employee of the company that owns the AI system, this company will acquire the rights on generated objects.[84] Another idea is that "economic rights derived from the AI protection should be conferred to the employer, investor or another person for whom the work was prepared or by whom the arrangements necessary for the creation are undertaken."[85]

44 In my view, a sui generis right should be guaranteed to the AI owner analously to that of a broadcasting organisation, which acquires related rights to the broadcast directly and not as a result of their transfer from employees. If legal protection of AI-generated objects is justified, it seems that it will be largely grounded in the need to protect economic investments. The owner of the AI usually finances the creation of AI (or buys it) and solves financial and organisational issues related to the functioning of AI. While the input of developers is crucial to the emergence of AI, without financial and organisational support, the efforts of developers could hardly have resulted in the emergence of the amount of AI that is currently seen. In addition, developers and end users receive remuneration for their work as company employees or independent specialists engaged in the contracts while the AI owner invests large resources without receiving remuneration for it. Therefore, it is quite difficult to find an explanation for why economic benefits from the use of a computer creation should be granted to employees, and not to the person who provided the economic preconditions for these benefits to appear at all.

45 Fourth, the scope of rights that can be granted in relation to an AI-generated object needs to be clarified. Images, texts, sound recordings, and other results of AI activity can be used in the same way as works or objects of related rights with the same form of expression; that is, the relevant ways of using works and objects of related rights can be applied to AI-generated objects. However, the question remains whether the sui generis regime should grant the rightsholder a monopoly on the modification of computer creations by analogy with copyright. Thus, the concept of a sui generis right can be formed in one of two ways: the right holder receives the whole range of economic rights, including the right to allow the reworking of a computer creation, or the right holder receives protection only against literal copying, while the reworking of the protected object can be freely carried out by the public. Now there is no decision on which approach will be the most reasonable and appropriate. In addition, the researchers mostly do not mention whether sui generis right can be subject to exceptions and limitations by analogy with copyright and related rights. It seems that there are no obstacles to citing AI-generated objects, reporting them in the news, using them for educational purposes, and even parodying them but this aspect also needs to be clarified.

46 Fifth, it is necessary to decide what should be the term of validity of the sui generis right so that it could satisfy the economic interests of the right holder. This issue is extremely important since the duration of protection may determine whether it makes sense to provide such protection at all. In the doctrine, it is proposed that the right to AI-generated objects

80 Art. 7(1) of the Directive 96/9/EC (n 58).

81 Enrico Bonadio and Luke McDonagh, (n 34).

82 Celine Melanie A. Dee, 'Examining Copyright Protection of AI-Generated Art' (2018) 1 Delphi 31, 37.

83 Madeleine de Cock Buning, 'Artificial intelligence and the creative industry: new challenges for the EU paradigm for art and technology by autonomous creation' in Barfield and Pagallo (eds.) *Research Handbook on the Law of Artificial Intelligence* (Edward Elgar: 2018) 511, 532.

84 Anthoula Papadopoulou, (n 33) para 32.

85 Javiera Cáceres B. and Felipe Muñoz N., 'Artificial Intelligence, A new frontier for intellectual property policymaking' (2020) 9(2) Journal of Intellectual Property Law and Management 108, 126.

should be granted for two years,[86] three years,[87] ten years[88] or fifteen years.[89] It is also possible to take as a basis the twenty-five-year term defined in Article 4 of Directive 93/98/EEC on the protection of rights to a work that is first published after the expiry of its copyright protection.[90] Researchers express solidarity that this period should be relatively short[91] "in line with rapid technological advancements in the field."[92] At the same time, the question arises whether the legal regime lasting several years will be attractive for rightsholders.

47 If the sui generis right will provide protection only against literal copying for a period of two years while the rightsholders will be liable for violations committed by the computer in the content of the object, it is very doubtful that they will be interested in such protection at all. At the same time, a term of legal protection of twenty-five years may seem too long given the rapid development of technologies. On the other hand, if a certain AI-generated object has commercial potential and remains interesting for the audience after several years, the rightsholder may wish to keep the rights to this object longer than the rights to an object that has not shown commercial potential. Therefore, it may be more appropriate to adopt an approach similar to trademark rights, where initial protection is granted for a short period, e.g., five years, but can be renewed by the right holder for a further five years. Perhaps, in this case, it will be necessary to limit the total term of validity of the sui generis right not to exceed twenty-five years or another term justified by the interests of society. Although this will require registration of rights to each object and development of the procedure for such registration, in my opinion, this approach may deserve attention. It will allow the rightsholders to decide independently whether they want to have legal protection of computer creations and bear the risks associated with it.

48 Hence, although a special regime for the legal protection of autonomous computer creations is being actively discussed, it is still very far from having a clear concept. While the above considerations may to some extent contribute to the improvement of this concept, it should be recognised that the theoretical developments in this area are still very different and too controversial to be used as a basis for the adoption of relevant legislation if such a need is confirmed.

E. Concluding remarks

49 AI has changed the world and continues changing it. Images, music, drawings, and other similar objects generated by AI without human intervention have become a great challenge for the legal systems of the world as they do not fit into the existing paradigms of legal protection. It is not yet confirmed whether protection of such AI-generated objects is really needed or they should remain in the public domain. Data on AI investments show that this sector is developing rapidly and successfully regardless of the fact that investors cannot influence the use of objects autonomously generated by their wards computers. Assumptions about potential risks to the market and threats to normal competition that may arise as a result of the lack of legal protection of these objects are not yet supported by studies that would indicate the reality of such risks and threats. Other arguments in favour of granting legal protection to computer creations also raise doubts.

50 Despite a large number of scientific proposals, the optimal legal model that will satisfy both the interests of investors and society has not yet been developed. This article puts forward that the implementation of the protection of objects generated by AI without human intervention requires the development of a special legal regime and considers its main elements. At the same time, almost all key questions concerning this regime have ambiguous answers so in general we are not yet ready to implement such protection.

86 Anke Moerland, (n 70).

87 Enrico Bonadio and Luke McDonagh, (n 34).

88 Haochen Sun, (n 79) 1245.

89 Javiera Cáceres B. and Felipe Muñoz N., (n 85) 125.

90 Council Directive 93/98/EEC (n 57).

91 Anthoula Papadopoulou, (n 33) para 22.

92 Celine Melanie A. Dee, (n 83) 37.

All Agents Created Equal?

The Law's Technical Neutrality on AI Knowledge Representation

by **Philipp Lerch***

Abstract: The term "Artificial Intelligence" comprises different approaches. They can be roughly divided into rule-based approaches and approximative machine learning. The author discusses the legal implications of this technological choice on the background of Product Liability law. It stands to reason that using rule-based approaches may be prone to stricter safety standards than approximative implementations.

Keywords: Product Liability; Product Security; Artifical Intelligence

Recommended citation: Philipp Lerch, All Agents Created Equal? The Law's Technical Neutrality on AI Knowledge Representation, 14 (2023) JIPITEC 108 para 1.

A. Introduction

1 A recent EU Commission's proposal aims at amending the legal framework on Product Liability with specific adaptations for products employing Artificial Intelligence technologies.[1] It is part of a major strategy of the European Union embracing the fields of Product Security, Technology Regulation and Contractual Liability, *inter alia*. The proposed directive adapts "non-contractual fault-based civil liability rules to artificial intelligence".[2] The most eye-catching though unspectacular novelty is—not surprisingly—the codification of the widely accepted notion that software is indeed a product (Article 4, para 1 of the Directive). The changes made appear to be rather subtle (which is, simply put, a smart decision disregarding those hyped voices who cannot wait to introduce AI Law early enough as a fourth major area of law). Interestingly the two major concerns of what forms a *defect* (as the most central term of Product Liability Law), and what justifies *exculpation* are not extended by a fundamentally new approach. Article 6, para 1 of the Directive amends certain circumstances to take into account when a defect is being ascertained:

2 "The effect on the product of any ability to continue to learn after deployment" (lit. c) refers to what is known as "development risks" of AI systems in the debate. The effect on the product of other products that can reasonably be expected to be used together with the product" (lit. d) can be described as interoperability which has already been set for the

* Philipp Lerch, Formerly Institute for Legal Informatics, Saarland University.

1 COM(2022) 495 - Proposal for a directive of the European Parliament and of the Council on liability for defective products.

2 COM(2022) 495, Explanatory Memorandum 1.2.

term of contractual defect.[3] With lit. e the aspect is taken into account that products may be kept under control of the manufacturer via network connection.[4] Lit f) and g) state that product safety requirements including cybersecurity, as well as "specific expectations of the end-users for whom the product is intended" are to be taken into account which is nothing revolutionarily new to the doctrine of Product Liability.

3 On the *exculpation* side the relevant Article 10, para 1 provides even less deviations from the current law. The exemption ground of lit. e) is still central, which allows exculpation if the defect could not have been discovered due to the objective state of scientific and technical knowledge at the time when the product was put on the market.

4 One problem identified in the field of AI law is whether self-learning systems, whose behaviours change over time, are subject to liability also for the adaptions that occur after the user has put the product into operation.[5] The novel directive surely aims at solving this issue. However, it assumes that most systems' algorithms do not evolve in the hand of the user. In principle, a computer software can (somewhat) solve *any* problem *either* by coding it to explicitly implement algorithms *or* by "training" how to solve it. This touches even more fundamental issues that are not tackled by the Directive at all. It goes to the heart of a Product Liability legal regime and touches specifically technical concerns: What *constitutes* a defect? Was it *avoidable*? And if it was, was it also *discoverable*?

5 A manufacturer may make use of machine learning techniques instead of coding the system's behaviour explicitly. The most illustrating examples for this can be found in the field of autonomous vehicles. There is ongoing research regarding so-called "end-to-end" approaches for autonomous vehicle control.[6] Instead of classical modular development of the vehicle, a single machine learning model is trained on the entire driving functionality like steering, object and lane detection, path planning, and control.[7] In such a framework information about the outer world ("knowledge"), particularly the way a vehicle ought to behave, is not being provided explicitly to the vehicle. Instead, it is being implicitly induced by the training data, that could be obtained by a human driver in operation.

6 The classical way autonomous vehicles are being constructed is different: expert and world knowledge, particularly traffic rules are being explicitly coded.[8] They serve as explicit constraints over other modules that make use of machine learning algorithms.

7 I will call the latter approach "explicit rule based". World knowledge leading to an agent's behaviour is being explicitly represented and the system operates directly on it. The former approach is the "implicit" machine learning approach. The agent's behaviour results from the induction of rules (implicitly represented in the system) from a given set of data. The choice of whether to use either of the methods also affects the widely-known postulate of transparency (problem of opacity): many machine learning techniques suffer from poor interpretability, known as the *black box* problem.

8 Unfortunately, there has not been active research on the legal consequences of this choice. Is the law technically neutral on this question? Another EU proposal, the famous AI Act[9], has been overtly called "technically neutral".[10] Technical neutrality means that the law is not per se preferring one technical approach to another in a specific domain, neither it is imposing a specific regime on any technical solution. Recent legislation is being called "technically neutral" as the regulators may have explicitly enumerated the (almost) entire set of

3 Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC, OJ L 166 0f 22 May 2019 ("SGD"), Art 2(5)(b).

4 "The moment in time when the product was placed on the market or put into service or, where the manufacturer retains control over the product after that."

5 Ebers, „Autonomes Fahren: Produkt- und Produzentenhaftung", in: Oppermann and Stender-Vorwachs, *Autonomes Fahren. Rechtsfolgen, Rechtsprobleme, technische Grundlagen*, p 34 ff.

6 For instance, see Rausch et al, "Learning a Deep Neural Net Policy for End-to-End Control of Autonomous Vehicles", 2017 American Control Conference (ACC) (24-26 May 2017).

7 Rausch et al, "Learning a Deep Neural Net Policy for End-to-End Control of Autonomous Vehicles", 2017 American Control Conference (ACC) (24-26 May 2017).

8 See for instance the implementation of the autonomous vehicle "Bertha": Ziegler et al, "Making Bertha Drive - An Autonomous Journey on a Historic Route", IEEE Intelligent Transportation Systems Magazine, 6 (2), pp. 8-20, 2014.

9 Proposal for a Regulation Of The European Parliament And Of The Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts (COM/2021/206 final) (AI Act)

10 Memorandum to the AI Act, p. 8; Geminn, "Die Regulierung künstlicher Intelligenz", ZD 2021, 354.

possible technical approaches. The AI Act explicitly names both machine learning, logic, and knowledge-based approaches; statistical ones have also been mentioned as forms of artificial intelligence.[11]

9 These explicit regulatory considerations are at the front of recent technological developments. General German Private Law relies on statutes given in the German Civil Code. It had been enacted in 1900. It provides the fundamental rules of private law, which means particularly contracts and liability rules (e.g. torts). One may claim that—given the technological developments in the last 100+x years—the German Civil Code is technology neutral by design: it does not pose any explicit restriction on technologies to be used—particularly not on Artificial Intelligence.

10 However, the general structure of legal doctrines may affect different technical approaches in a different manner. Law and Economics scholarship has studied the effects that legal doctrine can have on society, in particular by providing a framework to enforce contracts and property rights effectively. Similarly, Law and Technology as well as Law and Innovation studies extended this approach to study the interaction between these fields.

11 Building on a Law and Technology approach, we study the effects of the liability regime on the choice between adopting a smart product on explicit rule representations and making use of machine learning methods.

12 We show that *correctness* as a desiderate of software engineering and the 'defect' in the legal sense are distinct. However, when safety-relevant features of a product are concerned, correctness of a software system is *de facto* the obliged outcome. If instead the manufacturer chooses to use Machine Learning technologies, thus merely approximating the desired outcome, the law may yield certain degree of inaccuracies. Finally, the question arises whether the law may dictate the use of explicit rule representations in cases where a certain output or behaviour is asserted or minimal guarantees hold.

11 In detail Geminn, "Die Regulierung künstlicher Intelligenz", ZD 2021,354. This commission states that these provisions are technology neutral: COM(2021) 206 final, 12: „as technology neutral and future proof as possible".

I. Two Tier-Perspective on Autonomous Agents

13 There are two perspectives on Artificial Intelligence as identified by Russell and Norvig: (1) the *behaviour* of the agent and (2) the *thought processes* or *reasonin*.[12]

1. Behaviour

14 The behaviour of an agent can be simply defined as the relationship between a certain input and the output. By 'output' it is meant any result of calculation that constitutes the agent's functionality. The 'behaviour' of an agent is usually what is of directly relvant to legal liability as the behaviour determines how the agent interacts with the environment and thus may be source of damage.

2. Reasoning

15 The *reasoning* corresponds with *how* a certain conclusion is being drawn.[13] It determines the steps the agent performs in order to ascertain the output. Any computer programme may be seen as a conditioned sequence of intermediate system states, and a concrete run of a system as an unconditioned sequence of system states. They can be invisible to the user.

16 By "intermediate states", I mean the sequence of states in between the output and input states. By evaluating the single steps taken by the agent, results might be traced and thus proven and explained.[14] This is invariant of the technology used. In classical algorithms, a sequence of system states is defined by the program flow. This is no different when machine learning comes into play. In neural networks, the *latent space* matches the single intermediate steps in the computation; in each layer there is some different representation of the input data which one may call a kind of interim result.[15]

12 Russell and Norvig, *Artificial Intelligence. A modern approach* (3rd Edition 2016), pp 1-2.

13 In logic, reasoning is being done by *inference:* propositions are being inferred according inference rules from a certain knowledge base: Russel and Norvig (fn 11), p 235.

14 For instance, the Hoare logic offers a formal-mathematical tool to prove an output (a postcondition) given a certain input (a precondition): Hoare, "An Axiomatic Basis for Computer Programming", 12 (10) Communications of the ACM, 576.

15 Cf. Lassance et al, "Representing Deep Neural Networks

17 These two conceptual tiers correspond with the terms of "specification" and "implementation". The specification of a system determines the outer behaviour given a certain input. The implementation determines the exact way a certain specification is being realized.

II. The Term Correctness of a Computer System

18 In Computer Science and Software Development, the term "correctness" refers to a behaviour of a computer programme. A computer system is correct if—given a certain input and certain preconditions in the state space—the *specified* preconditions hold, particularly the expected outcome.[16] The *specification* is a formal or informal description of what behaviour a computer programme is supposed to have.[17] Usually the term "specification" refers to both the requirements specification and the design specification. The first comprises the description of product behaviour in regard to the customer's *needs*. The latter is a more fine-granular description of the different components, modules, and interfaces (subsystems) of the system. Both are not representing the way *how* to achieve things, but *what* to achieve.

19 Functional requirements and non-functional requirements are still being distinguished on the specification side.[18] The functional requirements encompass that relation between input and output, respectively preconditions and postconditions. They describe the main functionality of the software. On the other hand, the non-functional requirements concern side-conditions, such as certain security standards, performance, etc.[19]

20 The implementation is the actual realization of the system, i.e., the concrete computer programme. The computer programme determines not only *what* behaviour a system may have (prescribed by the specification), but also it consists of concrete instructions to the system environment about *how* this behaviour shall be accomplished.[20]

21 Thus, on the one hand, from a Software Engineering internal perspective, the *correctness* is being assessed just by matching the implementation with the specification. From an *external* perspective on the other hand, a software product may be considered "sensible", "proper", etc. in regards to customer needs.

22 As described above, the specification describes the *behaviour* of an agent to its environment. The implementation is what constitutes the *reasoning* process, thus behaviour is reached by a specific sequence of instructions forming a certain sequence of states.

III. Implementation Approaches

23 Generally, there are two types of Artificial Intelligence approaches distinguished: Rule-based systems and Machine Learning methods.

1. Rule-based systems

24 Rule based systems belong to the group of "symbolic" AI methods. Symbolic AI relies on the use of logic and "ontologies" to represent knowledge.[21] The way behaviour is defined directly corresponds with the concepts of the problem domain. Thus, a rule "If A then B" can be directly represented using a certain *syntax*, e.g. "A → B", "IF A: B" etc. Ontologies can refine concepts as "A consists of 1 and 2", and semantic web methods may represent complex webs of relations between concepts.[22] For instance, one could represent legal rules symbolically by using

Latent Space Geometries with Graphs" <https://arxiv.org/abs/2011.07343>

16 Cf. Dennis, "The design and construction of software systems" in Bauer et al (eds.), *Software Engineering. An Advanced Course*, p. 22 "correctness of its description with respect to the objective of the software system as specified by the semantic description of the linguistic level it defines" The "description" in this sense is the code that describes the computer behaviour. The "objective" is what one can understand as the core of specification.

17 Schmidt, *Software Engineering. Architecture-driven Software Development* (2013), pp 93-111. *Bauer* et al, Software Engineering. An Advanced Course.

18 Cf Dick et al, *Requirements Engineering*, p. 172.

19 Critical discussion on this term in Glinz, *On Non-Functional Requirements, 15th IEEE International Requirements Engineering Conference* (RE 2007) DOI 10.1109/RE.2007.45.

20 Imagine a programme that shall sort numbers in descending order. In first year computer science classes students learn that there exist many different sorting algorithms (Bubblesort, Quicksort, Mergesort etc.). All of them are different implementations of the same.

21 These are called „knowledge-based agents" in AI research. Russell/Norvig, *Artificial Intelligence*, p 234.

22 For Semantic Web technologies used in the legal domain, see Benjamins et al, "Law and the Semantic Web, an Introduction", in: Benjamin et al (eds), *Law and the Semantic Web. Legal Ontologies, Methodologies, Legal Information Retrieval, and Applications*, pp. 1 – 17.

a deontic logic, e.g. stating that somebody who murders another human being ought to be punished:

Murderer(x) → O(Punished(x))

25 If x is a murderer, he ought to be punished. It is clear to see that this representation of legal domain knowledge somewhat maps with the real life concepts behind it. In a rule-based system, therefore, behaviour of a computer system is being described *explicitly*. The language in which rules are being described *matches* the concepts of the problem domain; the domain-level concepts are being translated directly into logic-level names as predicates, functions, and constants.[23] The semantic *model* of the logic involved determines the truth of an individual sentence (rule) described.[24] The *model* thus maps the logical formalism (syntax) to the real-world concepts and the truth of sentences in the real domain.[25]

26 For *correctness* of such approach twofold conditions need to be satisfied. Firstly, the rule engine, i.e. the component that translates the rules into executable instructions, needs to be correct.[26] This encompasses both syntactic and semantic correctness; particularly the rules must be consistently interpretable.[27]

27 Secondly, the rule definitions themselves must be correct, thus leading to the correct behaviour of a system, given the rule translator works *correctly*. This means that rules shall conceptually map the problem domain the system is meant to represent.

28 However, there is non-determinism posing a problem because of the input/output operations of the autonomous system: the correctness property just implies that the programme meets certain post-conditions given a certain input meeting the pre-conditions. Neither it can be in any way logically proven that a person interacting with the agent meets the precondition of the system with their input, nor is it any possible to prove this for other input/output periphery as sensors. Reliability cannot be ensured in unreliable host environments.[28] Arbitrary changes in the circuits may inevitably happen and thus can lead to an error occurring.[29]

2. Machine Learning

29 Machine Learning relies on the idea that a certain model structure is parametrized and these parameters are being induced by a learning process.[30] The most common structure in modern machine learning is Artificial Neural Networks (ANNs). They are a layered architecture consisting of several computational layers, in which each layer is a linear combination of the previous layers, with some non-linear activation function applied on each output of the respective layer.[31] Whilst any neural network of the same architecture practically does similar steps, what constitutes the network solving a specific problem are the parameters (often referred to as 'weights'): in a simple ANN they are the real numbers that—simply spoken—determine the flow ratio of neurons of the previous layer to each of the neurons in the next layer.

30 This is a highly general and abstract way to solve a problem: the same general architecture can be trained to a theoretically infinitely high set of

23 For first-order logic rule representation Russell and Norvig, *Artificial Intelligence*, p 290.

24 Russell and Norvig, *Artificial Intelligence*, p 232.

25 The theoretical term *model* originates from logic to theorize the idea of semantic within formal systems. In Artificial Intelligence and Machine Learning, a *model* is something different: It is closer to the colloquial meaning of a *model* as an approximation of reality. However, they are related in the way that also a logical *model* is mapping reality semantics onto the finite syntax.

26 This maps what Dennis (fn. 15), p. 24 demands that for "host level descriptions [...] that are the result of automatically translating the designer's description, proving the correctness of the translator suffices."

27 See Morscher, *Normenlogik* (Paderborn 2012), p 117 ss for consistency in model theory.

28 *Dennis* (p. 24) calls this aspect 'reliability' in contrast to the correctness: A system is reliable if it may perform its functions in spite of any host system failure. A system cannot be entirely reliable if the host system may be fallible (p. 25).

29 It is suspected that cosmic rays may sometimes affect circuitboards and can randomly change the state of computer systems, see e.g. *Ziegler*, "Effect of Cosmic Rays on Computer Memories", [1979] 206 Science 776-788. It stands to reason that a certain degree of unreliability of computer systems is inevitable.

30 When talking about Machine Learning, a model is a combination of a certain shape of a network and their parameters. An architecture describes the principal ideas the model structure follows: For instance, sequences of input can be processed by Recurrent Neural Nets (*RNN*s), where the output of a model is 'plugged' back as a model input itself.

31 A linear combination is simply a somehow weighted combination (1,1,1) as can be calculated as linear combination with the weights (5,2,1) to (1*5+2*1+1*1)=5+2+1=8. Applied to n different weight vectors, one can create n different new values, which are output of the next layer.

problems, if enough training data is available. It can be proven that ANNs are universal approximators.[32]

31 However, the major shortcoming in practical use is, that it is difficult to explain what is exactly going on in the middle of this network, the so-called latent layers (as they are 'hidden' in the middle of the network). Nor can one prove properties of a neural network in general. This is often referred to as the "black box problem" of neural networks: whilst certain behaviour can be validated by testing, latent states (representing the reasoning process steps) are difficult to impossible to interpret.[33] The issue of "Explainable AI" is a current research issue, where these restrictions are aimed to be diminished.[34]

32 The most important property of these techniques is that they are merely approximative.[35] They will not be *correct* in the sense that they would always meet the right result given an input, if not all possible inputs have been tested. Testing every possible input will not be possible in most domains. Just imagine an autonomous vehicle that may be confronted with a sheer vast amount of possible traffic situations and their combinations.

3. Neuro-symbolic Integration

33 Several hybrid methods are aiming at combining both approaches to each other. They are known under the name "neural-symbolic integration". Essentially, networks may be used for for reasoning tasks and context understanding. Symbolic knowledge representations may be fed into a network, upholding certain properties of syntactic equivalence of the input logic.[36] However, if these architectures remain approximative approaches, they are neither provable nor totally correct.

B. Normative Knowledge vs. World Knowledge from a Legal Perspective

34 Before assessing the issue in more fine granular detail, we want to shortly discuss the importance of different types of knowledge that are to be represented in a system.

I. Knowledge Types

35 When talking about *knowledge* in context of AI systems, a rough distinction may be made between *world knowledge* and *normative knowledge*.[37] World knowledge is the set of propositions about the *being*, thus any states of or actions in the world. Normative knowledge is the knowledge about how the world *ought* to be; it can represent ethical or legal postulates.

36 From a mere information representation perspective, this distinction does not make a difference per se.[38] This is different in law itself. In criminal law, an important distinction between world knowledge and normative knowledge can be made. Whilst most criminal offences require an *intention* or *knowledge* of the factual circumstances that constitute the offence ("Vorsatz", mens rea), there is the principle "*ignorantia juris neminem excusat*".[39] According to the German Criminal Code, ignorance of the unlawfulness of an offence committed may only exculpate a defendant *not guilty* if the ignorance was *not avoidable*.[40] Regularly, there is everybody's obligation to obtain legal advice on acts whose legality is doubtful.

37 On the other hand, in private law (contracts and torts) an intention or knowledge of a wrongdoing is—according to legal scholarship as well as jurisdic-

32 Alpaydin, *Introduction to Machine Learning.* (4th edn, 2016), p 99.

33 Cf. Alpaydin (fn. 32), p 155.

34 *Gunning et al*, ORCID: 0000-0001-6482- 1973,. XAI-Explainable artificial intelligence. Science Robotics, 4(37). DOI: 10.1126/scirobotics.aay7120.

35 Cf. the 'probability risk' of artificial intelligence identified by Zech, "Liability for autonomous systems: Tackling specific risks of modern IT", in Lohsse et al., *Liability for Robotics and in the Internet of Things.*

36 E.g. Lamb et al., "Graph Neural Networks Meet Neural-Symbolic Computing: A Survey and Perspective" <https://arxiv.org/abs/2003.00330>.

37 A finer distinction is made in Valente, "Use and Reuse of Legal Ontologies in Knowledge Engineering and Information Management" in Benjamins et al., *Law and the Semantic Web. Legal Ontologies, Methodologies, Legal Information Retrieval, and Applications*, p. 71: They distinguish between different knowledge on the legal side. However, for the purpose at hand the more rough distinction will suffice.

38 However, Deontic (normative) Logic languages pose different issues on Computer Science than other logical systems. They do not touch the ways of representing, but of operating on them.

39 Ignorance of the law does not pose a defence; see Jackson, *Latin for Lawyers II*, (2014), p 166.

40 Section 117 German Criminal Code.

tion—considered to encompass both the knowledge of the circumstances that constitute the wrongdoing and its unlawfulness.[41] This difference to criminal law may be explained by the higher complexity of private law obligations; however it also stands out that in private law, most legal norms do not even require intention or knowledge of the unlawful act, but also let mere negligence suffice.[42] So the distinction is of less importance in private law.

38 For criminal law, the normative order imposes a dense obligation on everyone to inform themselves about the state of law. However, this becomes only relevant if one behaves against the law. Whilst the imagination of *factual circumstances* that fulfil the requirements of a criminal offense can cause liability for criminal attempt, the imagination of illegality of a behaviour that is not criminal, does not.[43]

39 Normative knowledge thus can have different legal implications than world knowledge. Put shortly, the law assumes that everyone must know about right and wrong, and failure to do so will not provide a defence against liability for malice.

II. Implications for Technical Systems

40 In current legal orders, there is no liability of technical systems themselves; any knowledge that is required for liability needs to be present in the human actors involved. For this constellation to occur, an analogy to § 166 German Civil Code is proposed:[44] If an autonomous agent took a decision "knowing" a certain fact (whatever this means for a computer system), then the human the agent connected to it cannot raise a defence of ignorance. This however is not widely accepted.[45]

41 Cf. Müko-BGB/*Grundmann* § 276 Rn. 158 ff.

42 § 826 German Civil Code is one of the rare examples where the law explicitly requires the intention or knowledge of the unlawful harm that triggers liability.

43 A maniac offense ("Wahndelikt") where the defendant just imagined that his behaviour was criminal does not form a criminal attempt and thus is not punishable. *Joecks/Kulhanek*, MükoBGB-StGB § 17 Rn. 38.

44 Recently Linke, „Die elektronische Person. Erforderlichkeit einer Rechtspersönlichkeit für autonome Systeme?, MMR 2021", 200 (with further references).

45 Against this, see only Cornelius, „Vertragsabschluss durch autonome elektronische Agenten", MMR 2002, 353 (355); Grapentin, *Vertragsschluss und vertragliches Verschulden beim Einsatz von Künstlicher Intelligenz und Softwareagenten*, 2018, S. 97.

41 For a machine there is no difference between "knowing" about the world and knowing about normative facts. It just behaves in the way it has been programmed. Thus, if active normative knowledge of a machine would matter, e.g. if there would exist a concept of malice done by a machine, there would not be any incentive of a programmer or operator to feed a machine with the normative knowledge (as then this would bar the responsible person from the defence of ignorance). The distinction between the knowledge of right and wrong and other kinds of knowledge should not be continued when considering autonomous agents from the legal perspective.

42 Generally speaking, the latent states of a machine (see above) are of no importance when considering the liability for a system. Only the behaviour matters. It does not matter *why* a machine takes a decision; both knowledge of fact and knowledge of norms only touch the question of personal responsibility of a human being. As long as computer systems themselves cannot be held accountable there is no need to distinguish between normative knowledge and world knowledge in autonomous agents *by law*. This does not mean that this distinction does not pose engineering problems when attempting to operate on formalized normative knowledge, i.e. by use of deontic logic.

C. Technical Correctness and Normative Standards

I. "Defect" in Product Liability

43 In the heart of the Product Liability Law regime lies the term "defect". Eliciting the scope of the term constitutes the remaining assessment of the problem.

1. Different "Flavours" of Defects

44 The EU Product Liability Directive establishes a liability for producers "caused by a defect in his product".[46] According to the definition given in the Directive, a product is defective, "when it does not provide the safety which a person is entitled to expect", taking into account the presentation of the product, the

46 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 (Short: Product Liability Directive), Art. 1.

expected use of the product, the time the product was put into circulation.[47]

45 It is acknowledged that this standard ought to be objective.[48] In the respective recital of the German implementation of the Directive, it is explicitly stated that it relies on the "expectations of the public"[49], which is to be concretised as the usual circle of ideal users.[50] This means it relies on the expectation of the product's target group. However, some call the wording "expected safety standard" an empty formula, as it did not make it any easier for courts to ascertain the standard of safety.[51]

46 Jurisprudence has delivered more concrete formulas. For instance, the level of the product's safety standard to be expected is ascertained by an "exhaustive consideration", taking into account the size and scope of the dangers, the cost of safety measures as well as further circumstances as the detectability and avoidability of dangers.[52] Generally, the manufacturer was only liable for security measures whose cost was reasonably proportionate to their utility.[53] This "risk-utility-test" is also the formula to determine the safety standard under U.S. law.[54]

47 For the separate types of defects, doctrine distinguishes between those of design, manufacture, and instruction. When considering software systems, on which it is at least partially acknowledged that product liability law is applicable,[55] it also considers how the safety standards connect with the term "correctness".

47 Product Liability Directive, Art. 6.

48 BeckOGK/*Goehl*, § 3 ProdHaftG Rn. 14.

49 BT-Drs. 11/2447, 18.

50 BeckOGK/Goehl, § 3 ProdHaftG Rn. 15.

51 MükoBGB/Wagner, § 3 ProdHaftG Rn. 7.

52 BeckOK-IT-Recht/*Borges*, § 3 ProdHaftG, Rn.8.

53 MükoBGB/Wagner, § 3 ProdHaftG Rn. 7; BGHZ 181, 253 Rn. 23.

54 Geistfeld, "A Roadmap for Autonomous Vehicles. A Roadmap for Autonomous Vehicles: State Tort Liability, Automobile Insurance, and Federal Safety Regulation" (2017) 105 California Law Review 1611.

55 At least for embedded systems (software that has been integrated into a physical good) this is acknowledged: MükoBGB/Wagner, § 2 ProdHaftG Rn. 6. However, this should not be discussed another time in this paper.

48 First, it is obvious that these terms are of different meaning. By definition, a software is correct if it matches the specification.[56] Now, given the specification also matches with the safety standards demanded by law (including the safety standard demanded by a reasonable and ideal user), a *correct* software also fulfils the safety standards demanded by law. In this case, one can state the presumption that *correctness* is a prima facie condition for a software to fulfil these safety requirements.

49 However, neither an incorrectness implies a defect necessarily, nor follows from a defect in the legal sense that the software is technically incorrect. Literature restricts the term "defect" to features that are "safety relevant".[57] This can be explained by the purpose of Product Liability Law: there shall not be an obligation to deliver an optimal product.[58] Product Liability is about safety only. Therefore, naturally not every incorrectness poses a defect.

50 On the other hand, a software may be completely correct, but still not meeting the product safety requirements. The flaw is therefore to be found in the specification. It might be that the requirements are itself "incorrect" or "flawed". This only applies to the "external" safety expectations that cannot be systematically captured within the "internal" development sphere that is only concerned with matching the implementation with the specification. Whereas, the flaw can be that *needs* have not been sufficiently put into *specification*, which means that the product does not fit the customer *needs*.[59] From an engineering perspective, it is to be said that all customer needs are required to be taken into account when eliciting requirements; they come in vague statements from the persons in charge of eliciting the needs.[60] This will entail observing the market and also the legal framework around this market, particularly safety standards.

2. Is always correct software expected?

51 Imagine a judge examining a case of a potentially flawed feature that is safety-relevant. Without doubt, this leads to an application of the product li-

56 See above, p 5.

57 MükoBGB/*Wagner*, § 3 ProdHaftG Rn. 2.

58 BeckOK-IT-Recht/*Borges*, § 3 ProdHaftG Rn. 21.

59 In any requirements elicitation process the (abstract) *needs* serve as "input requirements" to the next level of requirements elicitation. Dick et al (fn. 17), p. 33 ss.

60 Dick et al (fn. 17), p. 33 ss.

ability regime. The question then is whether every incorrect implementation of a safety-relevant feature triggers liability. By the term *incorrect* I mean that the specification of the feature is flawless; the engineers in such a case correctly considered a feature that falls into the scope of the public safety expectation. The defect to be considered merely lies in the wrongful implementation.

52 It is highly doubtable whether the public expectation always demands software to be *correct* in the terms stated above.[61] Obviously, this cannot be determined generally and depends highly on the requirements of the domain. From an algorithmic perspective, there are some problems that are so-called NP-hard: a *correct* solution needs—from what theoretical computer science's complexity theory is at least presuming—exponential runtime complexity.[62] Thus, they cannot be practically solved correctly as the runtime would be too high.[63] An example is the Traveling Salesman Problem (TSP), where the shortest path in a graph is searched, that traverses all nodes and finishes at the starting point.[64] It cannot be solved efficiently (which means in polynomial / non-exponential time) whilst being correct. However there exist heuristics, that do not guarantee an optimal solution, but a reasonable runtime.[65]

53 Therefore, the public safety expectation (and this is only what matters)[66] cannot be an always correct software, even in safety-relevant matters; if complex problems are solved that can only be solved by approximating algorithms, there cannot be claimed a reasonable expectation of a correct software. Then, however, testing needs to be done to a reasonable extent.

54 However, a manufacturer cannot always claim the impossibility of a correct implementation. There are cases where a product cannot be safely brought to market, and thus shall not be issued at all.[67]

55 In parallel to this test, side-constraints posed by legal rules and standards must also be taken into account.[68] For autonomous vehicles, the German Traffic Code (*Straßenverkehrsgesetz*) imposes a regime for the technical admission requirements. Thus, the law specifies that any autonomous vehicle ought to ensure the behaviour of a "risk-minimal" state: A vehicle ought to set itself to a safe idle mode in a safe position (§ 1 d para 4 StVG, § 1 e para 2 no 3), or otherwise an infringement of traffic rules would occur. This is an explicit *minimal guarantee* of the product safety standard by law.[69] It is to be further discussed whether these *minimal guarantees* demand a correct implementation or can be implemented by approximation methods.[70]

3. Software Defects as Defects of Design only?

56 From an engineering perspective, a system may be either incorrect (i.e. its implementation does not meet the specification) or suffer of poor specification and thus the requirements are badly elucidated and do not meet the customer needs. Generally, one could speak of a *defective product* in this sense.

57 An issue however is to decide whether a defect is legally a design or manufacturing defect. This distinction is necessary as it determines the well-known *safety standard test*: defects of design are determined by actually applying the *risk-utility test* while defects of manufacture on the other hand can be proven by showing that the individual exemplar suffers of a disadvantageous deviation from the design plans.[71] This is because the public may rely on the specific properties of a product series.[72] The blueprints of a product thus pose a self-inflicted

61 Cf. BeckOK-IT-Recht/*Borges*, § 3 ProdHaftG Rn. 21; Taeger, „Produkt- und Produzentenhaftung bei Schäden durch fehlerhafte Computerprogramme" 1995 Computer und Recht 257, who stress that flawed software does not pose a defect necessarily.

62 The "P=NP-Problem" is actually a Millennium Problem for which the Turing Society offers a prize of One Million Dollars. Solving this problem would go beyond the scope of this essay. It may be solved in a further paper by the author. See Goldreich, *P, NP, and NP-Completeness. The Basics of Computational Complexity*, p. 48 ff.

63 Goldreich (fn 61), p. 50.

64 Lin and Kernighan, "An Effective Heuristic Algorithm for the Traveling-Salesman Problem" [1973] 21 (2) Operations Research p 498-516.

65 Lin and Kernighan (fn 61).

66 BeckOK-IT-Recht, § 3 Rn. 21.

67 BGH NJW 2009, 2952; BeckOGK/Goehl, § 3 ProdHaftG Rn. 15; MükoBGB/Wagner, § 3 ProdHaftG Rn. 45.

68 MükoBGB/Wagner, § 3 Rn. 27 ff.

69 The term "minimal guarantee" refers to software specification, in which the expected behaviour of a system or subsystem is stated, disregarding of a successful or non-successful execution of the component. See fn 101.

70 See below, p 19.

71 Wagner, AcP 217 2017, 707 (725 s).

72 BeckOGK/*Goehl* § 3 ProdHaftG Rn. 70.

safety standard that may be stricter than the objective standard matching the public expectation applying in the case of a design defect.

58 A manufacturing defect is a disadvantageous deviation of the product from the safety standard imposed by the producer themself.[73] In literature, Wagner claims that manufacturing defects of software only comprise wrongful *delivery* of software to individual specimens of the product, mainly relating to embedded systems.[74] One can reasonably doubt whether this perspective is entirely correct. Wagner further claims that a software not meeting the respective safety requirements was "*per definitionem*" suffering of a production defect, as every specimen of the product was affected.[75] However, public expectations may also arise from certain specifications that represent standards shared by several producers of software (*interfaces*). This comes into play particularly when components are delivered for end-user software products. Therefore, unlike Wagner's claims, incorrect software may pose a production defect rather than a design defect if one considers the coding as part of fabricating an end product rather than just constructing it.

59 In the analog world, a defect of design may be considered as wrong *blueprints*. They can be regarded as what specifications are for the manufacture of software. If a software is *incorrect* as it was not matching the specification, it is comparable to an item that has not been produced according to the blueprints. It is—from this perspective—a defect of manufacture. On the other hand, a wrongful specification resembles a defective blueprint. It stands to reason that—if the manufacturing defect's *differentia specifica* is the deviation from the *intended design*[76]—incorrect software deviating from the specification would have to be regarded as suffering from a manufacturing defect.

60 This is particularly important when software components are being delivered. The specification fulfils a special task in multi-component software systems. It defines the *interfaces* with which other components may communicate with the respective sub-system or component.[77] A component of a software may be a product itself in the sense of Product Liability Law.[78] Now if a component promises *by specification* to deliver service to another host environment this specification serves as much as a self-inflicted standard as a blueprint in a series of fabricated goods does. Public expectations are then subjectively formed by the intended design.

61 I do not want to argue out this issue; there may be good arguments for not considering incorrectness of software as defect of manufacture, certainly. It is not just as simple as to refer to the argument of a *per definitionem* nature of the implementation process. It highly depends on the mapping of analogies from the digital to the analogue. In literature it has therefore been proposed—with similar arguments—a new type of defect, the "generic manufacturing defect".[79]

62 Finally, it cannot be predicted today that the prevailing opinion on the nature of a bug will be seen correctly as a manufacture defect, if the defect relies on a deviation from publicly available interface specification. I will thus assume for the purpose of this study that incorrectness will lead to a defect of design rather than manufacture.

4. Proving versus Testing

63 To ascertain the quality of a software product, the two main ways are *proof* and *testing*. A proof is a mathematical (or other formal) procedure in which the logical necessity is induced, that a software or an algorithm returns the correct output (or sets the machine into the specified state) given a certain input.[80] For this it is necessary to observe the software's code. Formal proving is considered more of

73 Cf. MükoBGB/*Goehl* § 3 ProdHaftG Rn. 70; discussed by *Hubbard*, Sophisticated Robots: Balancing Liability, Regulation, and Innovation, [2015] 66 Fla. L. Rev. 1803 (1854 ss).

74 Wagner, *Produkthaftung für autonome Systeme*, AcP 217 (2017), 707 (725 s).

75 Wagner (fn. 74), AcP 217 (2017), 707 (725 s).

76 Turner and Richardson, "Software defect classes and no-fault liability." UC Irvine. ICS Technical Reports. Published 1999-04-05 p 16 <https://escholarship.org/uc/item/11v8f8tc>.

77 Foster and Towle, *Software Engineering. A Methodical Appoach* (2nd Edition 2022), p 194.

78 § 2 Produkthaftungsgesetz regards as product also the items that are part of another product. This relies on Art. 2 Product Liability Directive. Similarly Art 3 Product Liability Directive considers the manufacturer of a component as producer.

79 Turner and Richardson (fn. 78), p 19 <https://escholarship.org/uc/item/11v8f8tc>.

80 Dennis (fn. 76), pp 22 ff: "To prove correctness of a software system or component, one establishes by logical deduction that some description of the system or component asserted to be correct by the designer is equivalent to the description of the system or component expressed at the host level". The "description of the system or component asserted to be correct" is none less than the *specification*.

a theoretical thing.[81] Particularly, every computer programme entails a sort of non-determinism, as a software usually works in an operating system environment with a very large state space; the programme calls input/output functions indirectly by system calls to the operating system, and usually user inputs are not foreseeable. In short: one cannot make sure that the executing environment satisfies all the preconditions specified.[82]

64 Furthermore, even in a very simple programming language, it can be shown that the so-called Turing-completeness leads to the *undecidability* of certain properties of the code.[83] The well-known Halting Problem states that for no programming language that enables loops or recursions (possibly leading to infinite loops or recursions), there can be a program that decides *for all valid programs* whether this program falls into an infinite loop or recursion. Thus, there will never be any algorithm, software, or Artificial Intelligence that can cross this logical barrier. However, this does not mean that programmes cannot be written in a form that enables a proof on their correctness. This process just cannot be automatized.

65 Machine learning applications cannot be proven so far; we would have to understand what is going on inside of the model. Instead, only statistical margins can be defined, that a machine learning system shows a certain behaviour (given a certain input) with some percentage of probability.[84] This is done by means of testing. The term binary term *correctness* may then be replaced with scalar measure of *performance* of a model. Therefore, a programme is either correct, or it is not, *tertium non datur*, but it can be performing well (by accuracy metrics, e.g.) more or less.

5. Impacts on Product Liability

a) Correct Boundaries of Decisions and Training Procedures

66 Originating from American law, the consumer expectations are being ascertained by a "risk-utility test".[85] A product is thus to be considered defective if it poses risks to the consumer that are not being outweighed by the benefits.[86] Marchant and Lindor argue that this leads to a prohibitive effect of further developments as every advantageous improvement of the algorithms used can thus create liability, as the benefits of implementing such a change (particularly protecting human life, in the example of autonomous driving) would outweigh the cost, at least when highly valuables as life and body are endangered.[87] This would lead to basically any bug imposing liability.

67 Geistfeld correctly objects that this argumentation relies on the assumption that autonomous cars are being explicitly coded by rule definition.[88] Instead, he distinguishes parts that concern "rules that *constrain* or *guide* the machine learning, such as coding that instructs the vehicle to always stop at stop signs"[89] and the parts that make use of machine learning technologies.[90] Only the former was subject to a code-evaluation as proposed by Marchant and Lindor.

68 First of all, it needs to be stated that—given Marchant and Lindor are right with their claim—*correctness* in the sense stated above would be a minimal requirement for autonomous driving in regard to executive driving functions that—from the German perspective—represent safety-relevant features of an autonomous car (given the behaviour demanded by law was flawlessly specified). Thus, to avoid liability a manufacturer has to carefully (mathematically) *prove* both the rules' correctness and correctness of the piece of software that interprets the rules.

81 For instance, first year CS students are being taught the Hoare Logic (fn. 13) to prove that certain conditions hold given a certain preconditions by analysing the source code of a programme.

82 This is being called a problem of "reliability" of a software system: *Dennis* (fn. 15), pp 24 ss.

83 Enderton, *Computability Theory* (2011), pp 79-102.

84 Leupold et al., *Münchener Anwaltshandbuch IT-Recht* (4th edn 2021), 9.1 Rn. 12.

85 Geistfeld (fn. 85), pp 1642 s. In German law the *Bundesgerichtshof* has accepted this notion for their own adjudication.

86 Geistfeld (fn. 85), pp. 1642 s.

87 Marchant and Lindor, "The Coming Collision Between Autonomous Vehicles and the Liability System"(2012) 52 (4) Santa Clara Law Review 1321, pp 1334

88 Geistfeld (fn. 85), p. 1644.

89 Geistfeld (fn. 85), p. 1645.

90 Geistfeld (fn. 85), p. 35.

69 If this is being restricted to the explicit "rules that constrain or guide" the machine learning (as Geistfeld claims), it remains that both correctness of the machine learning routines themselves (training algorithms) as well as subroutines enforcing certain behaviour as layer on top of the learned behaviour ought to be *correct* for evaluating the product as defect-free.

70 Geistfeld does not go into the existence of methods that are in-between both approaches. They already have been introduced as "neuro-symbolic integration".[91] Roughly, rule representations are being used to influence the training to converge into a certain direction.[92] The system itself remains however approximative.[93] Therefore neuro-symbolic integration is not *correct* in the sense defined above. If a manufacturer makes use of these approaches, it is to claim that *at least* the rules injected into the machine learning model need to be *correct*, thus being a valid representation of the specified behaviour. This notion of *correctness* entails a very isolated, narrow view on the "linguistic level"[94] of the rule definition language, and not the behaviour of the entire system. In this case also, sufficient pre-market testing is the only means to decrease the risk of liability when using still-approximative "neuro-symbolic integration".

b) Escape to Approximations

71 Basically, developers of autonomous cars are free to decide which technical approach is to be used. However, when making use of machine learning technology, this means that a manufacturer would in fact *opt out* the explicit code evaluation done with the liability test. Instead, they would opt for merely ensuring sufficient pre-market testing rather than a mathematical proof of correctness. However, this may lower standards, as correctness of a software will not be necessary. There could be a race to the bottom of quality standards by an escape of developers to mere approximations.

72 Thus, it is problematic that there can be an arbitrary choice between the approaches. Approximative solutions may only be acceptable if the risk-utility test allows a system to be merely approximative—in the case that a correct solution would be either too expensive to obtain or computationally intractable. If the manufacturer opts for approximative solutions, it is to make sure that the system had been sufficiently tested, with regard to the risks it poses.[95]

73 If the manufacturer uses the explicit rule representation approach, the question is whether any coding error (bug) would pose a defect that the manufacturer is liable for. This is being argued by Marchant and Lindor who claim that given the risk-utility test, in risky domains *any* bug would impose less cost to remove than the risks to be expected if the bug would remain in the system.[96] This again would carry a legal obligation for the manufacturer to ensure *correctness* of the explicit rule implementation, regarding safety-relevant features. If certain behaviour is steadily specified, mere approximations to achieve this behaviour will not suffice.

74 Moreover, the largest burden of debugging lies in the *identification* of bugs. However that identification costs are part of the trade-off between risk and utility in the respective test to ascertain a defect is doubtable: In the Directive[97] there is a distinction made between the *identifiability* of a defect and the *implementability* of safety standards. Whilst the question of implementation cost touches the question of an expected safety standard,[98] the non-recognisability of a given defect is merely a defense as provided by § 1 Abs. 2 Nr. 5 ProdHaftG.[99] The prerequisites of the defense of non-recognizability of a defect are much stricter and do not admit a risk-utility-test. It stands to reason that courts will never consider a bug as not identifiable. According to the "state of science and technology" a bug could always be considered identifiable. And if a bug has been identified, the effort it costs to solve it is marginal most of the time. The risk always outweighs the burden.

75 This leads to the proposition that, when using rule-based approaches, it is possible that—due to the strictness of the risk-utility test —making use of explicit rule definitions may lead to higher liability risk. The disproportionate cost to review code for bugs may not help the manufacturer to argue a case

91 See above, p 8.

92 See above, p 8.

93 See above, p 8.

94 This is how Dennis defines a logical level of a software, on which correctness applies: *Dennis* (fn. 15), p 14.

95 This is stressed by Geistfeld (fn. 85), p 1646.

96 Marchant and Lindor (fn. 87), p 1334.

97 See 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, Art 7.

98 And thus is a question of § 3 ProdHaftG resp. Art. 7 lit e of the Directive.

99 Cf. MükoBGB/Wagner, § 1 ProdHaftG, Rn. 52

for themselves in the course of the risk-utility test. Therefore, when using explicit rule-based methods to implement a software, the law will *de facto* require *correctness* of this system, if they potentially affect safety-relevant features. In particularly safety-critical domains, most features are safety-relevant indeed.

76 On the other hand, whether the cost of *testing*, when using approximative machine learning approaches, belongs to the cost of identification of a defect and not the cost of implementation is doubtful. In any case, the obliged scale of testing would depend on the "state of science of technology" in the way that the testing procedures need to be in accordance with the state of the art of computer science, and the scale of testing sufficient to ensure a reasonable safety standard. This also depends on available computational power.[100] Testing therefore will always remain imperfect, and no "perfectly" tested system can be demanded by law (which would mostly not be even possible). The latter case means a necessary trade-off between the cost and benefit of safety measures; this is a strong argument to position the question of scale of testing (particularly how many test runs and how much test data is needed) to the less strict question of expected safety standard.

77 It seems therefore that by using machine learning techniques, the manufacturers can avoid their liability for correctness of a system; the law may tolerate system failures for machine learning systems more than if explicit rules have been used. This appears to be an adverse effect as it might lead manufacturers to escape strict code evaluation by opting for approximative approaches!

c) Minimal guarantees and safeguards

78 An exception to the principle of free technical choice may arise if the law demands that certain behaviour should occur in any case, thus with a probability of 100 percent. For instance, Leupold and Wiesner assert that the absence of "decision boundaries" may lead to product liability.[101] Geistfeld similarly recognizes that in autonomous driving environments, there would—at least—exist explicit "rules that *constrain* or *guide* the machine learning, such as coding that instructs the vehicle to always stop at stop signs"[102]

79 With "decision boundaries" it is meant a fixed range in which a system can autonomously decide but may never go beyond these boundaries. An autonomous car may be coded in the way that e.g. the *Acceleration module* may not exceed a certain velocity. By our nomenclature, this is rule-based coding rather than machine learning as the behaviour will be explicitly defined, and the cap of velocity not just be induced by prior training data. Such boundaries may be imposed by law or by technical standards, or just arise from technical necessity. As rule representations, these boundaries ought to be correct as well if they concern safety relevant features.

80 Aside from that, there may be *minimal guarantees* to be expected. This is behaviour that should in any case hold and should be guaranteed by a system even in case of operation failure.[103] The German regulations give an example of the admission of autonomous vehicles. The law explicitly demands that a system should

> [...] set itself into a risk minimal state, if the driving may only be continued with an infringement of traffic rules.[104]

81 This kind of provision will also oblige the manufacturer to implement such a safeguard functionality; legal safety requirements can be expected to be satisfied by the public. Now the question would arise whether the manufacturer could merely implement this behaviour by training the system to behave this way (which would mean as last resort before an infringement of traffic rules, drive to the right and stop!). Against this it can be argued that the law requires such behaviour to be implemented correctly, so that a mere approximation by machine learning techniques would not suffice.

82 One may argue that the existence of a minimal guarantee does lead to a legal obligation to ensure that the asserted behaviour shall be triggered in any case possible, thus with a probability of 100 percent given certain prerequisites. This could only be achieved by explicit rule representation,[105] as this

100 Moore's law states the monotonic, exponential growth of transistor size and thus computational power (cf. Kurzweil, *The law of accelerating returns*, <https://www.kurzweilai.net/the-law-of-accelerating-returns>). Thus, the technical developments will also shift the standards for the adequate scale of testing to more intense testing.

101 Leupold/Wiesner, 9.6.4, Rn. 26.

102 Geistfeld (fn. 85), p. 1644.

103 This is a term used by to set such behaviour of a computer system within a Use Case; thus it originates from the requirements elicitation phase: Cockburn, *Writing Effective Use Cases*, p. 83.

104 § 1e II Nr. 3 StVG.

105 Of course, this 100 percent would be anyway conditioned on full reliability of the host system.

behaviour merely being induced by training data would never be an optimal solution. However, whilst it is possible to ensure correctness, reliability affects the product behaviour as well. Reliability means a stable system behaviour despite any hardware or subsystem error. It stands to reason that an autonomous driving system will always be prone to hardware errors and thus the perfectly reliable system does not exist.

83 One may say: At least, if there is no 100 percent safety, one should at least expect optimal safety. This would mean that a *correct* implementation of the feature can be expected, and this would bar the manufacturer from using approximative methods for the feature.

84 Against this, it may be argued that such strict standards do not apply to other, non-digital products. For a conventional car, one would assert that its brakes should be effective. Obviously, there is always a probability that the brake fails, there cannot be 100 percent safety. Unlike computer code that works in a *conceptually* perfect environment (correctness assumes that the computer does what it is being told to do), mechanical parts are not considered to work in such a formal machine environment. Why would a prerequisite of *correctness* be made for certain features in a digital system, but not in other, analogous system? The doctrine of risk-utility test gives the answer to this question: because *it is usually feasible* at proportionate cost. If the minimal guarantee cannot be implemented effectively, the system would be usually too risky to be published, or an approximative solution would suffice.

85 This depends on the individual case matter. As a rule of thumb one can state:

> Features that are mandated by law to exist shall be explicitly coded (by a rule).

86 Therefore, a manufacturer may not lawfully refrain from explicitly representing *guaranteed* behaviour; an arbitrary escape to approximative solutions is not possible here. However, it is an individual question of legal statute interpretation of the safety standards demanded by law whether it imposes an actual minimal guarantee on the manufacturer, or just aims at ensuring a very careful consideration of a certain safety aspect.

D. Regulatory Impact of the AI Act

87 Interestingly, one cannot find the term "correctness" in the "AI Act" proposal. Instead the term "accuracy" is used for postulating in Article 15, para 1 that systems ought to achieve an "appropriate level of accuracy" (cf. Rec. 38, 47, 49). This wording appears to imply that the regulator acknowledges the fact that machine learning will only be accurate to a certain degree, thus is restrained to approximations. What is an appropriate degree of approximation, remains unclear and will depend on the single case as intended.

88 However, the transparency requirements of Article 13 para 1 of the proposed AI Act may impose a stricter constraint on the design choice:

> "High-risk AI systems shall be designed and developed in such a way to ensure that their operation is sufficiently transparent to enable users to interpret the system's output and use it appropriately. An appropriate type and degree of transparency shall be ensured, with a view to achieving compliance with the relevant obligations of the user and of the provider set out in Chapter 3 of this Title."

89 "Sufficiently transparent" sounds rigorous given that interpretability of the state-of-the-art machine learning technologies is still in its infancy. For certain high-risk systems this might mean that only explicit rules may be used so that the system can output a reasonable explanation.

90 The manifest itself is even more generous in its understanding of transparency:

> "Users should be able to interpret the system output and use it appropriately. High-risk AI systems should therefore be accompanied by relevant documentation and instructions of use and include concise and clear information, including in relation to possible risks to fundamental rights and discrimination, where appropriate"[106]

91 It does not state that the user shall be allowed to interpret from the latent space of the machine learning model what *explainability* is about from the technical perspective. The manifest appears to let documenting the caveats of a system suffice, particularly its approximative nature. This is the key information that is needed in order to interpret an approximative system's output and to estimate its significance. Whether this is enough to achieve their intended goal remains questionable. Society might still rely on non-transparent models while being aware of the mere correlation-based stochastical nature. The general idea of a mere disclosure or information-based approach rather than substantive regulation would generally be welcome. But then the Commission could not evade the question of why it opted for the rather substantive regulatory approach for the rest.

106 Manifest of the AI Act rec. 47.

E. Contract Law – The Digital Content Directive

92 Similar conclusions as for the product liability may be made for the field of contract law. According to the Directive, digital content providers are obliged to fit the contractual requirements (subjective requirements) as to functionality, compatibility, interoperability, and other features.[107] It demands that beneath these subjective requirements the product should be fit for the purposes for which digital content or digital services of the same type would normally be used, taking into account, where applicable, any existing Union and national law, technical standards or, in the absence of such technical standards, applicable sector-specific industry codes of conduct.[108]

93 It is important to stress that these requirements are not restricted to safety requirements as the product liability regime is. It goes beyond them and also comprises any reasonable expectation of the customer to get a fully functional product. To be free of system failures is also a question of whether the system is secure.[109] In Information Technology, a secure system needs to be reliant and available; unreliance and unavailability may originate from both software bugs as well as human manipulation.

94 Any code incorrectness that leads to system failure in this sense may form a breach of contract. However, there is no equivalent to defective production as the measure is either by contract or inflicted by the industry average. It is yet to ascertain whether a risk-utility test will be applied.

F. Conclusions

95 Manufacturers should be aware that if they use rules to represent knowledge and behaviour, they ought to be correct! By making use of machine learning techniques manufacturers may partially avoid code assessment in the course of a dispute and thus may diverge from a strict correctness prerequisite. Then they simply need to provide evidence for sufficient testing before the product had been put on the market. However, a caveat is formed by minimal guarantees to be implemented—they ought to be implemented explicitly. If they are not computationally tractable or just way too costly to implement this can bar the manufacturer from putting a product on the market. It seems that under current liability law not all smart agents are created equal; approximative solutions are not required to be assessed as harshly as when explicit algorithms are used.

G. Acknowledgment

96 The research leading to these results is funded by the German Federal Ministry for Economic Affairs and Energy within the project "KI Wissen – Automotive AI powered by Knowledge". The author would like to thank the consortium for the successful co-operation.

107 Article 7 lit a. Digital Content Directive.

108 Article 8 para 1 lit a Digital Content Directive.

109 Compare Recital 42 of the Digital Content Directive.

Prior filtering obligations after Case C-401/19: balancing the content moderation triangle

A comparative analysis of the legal implications of Case C-401/19 for filtering obligations ex ante and the freedom of expression in Europe

by **Willemijn Kornelius***

Abstract: On 26 April 2022, the CJEU finally delivered its judgment (Case C-401/19 Poland v. Parliament and Council) on the compatibility of Article 17 DSM-directive with the freedom of expression (Article 11 Charter). Article 17 DSM-directive introduces an obligation for online content-sharing platforms to proactively prevent uploads of copyright infringing material. This *de facto* requires them to resort to automatic filtering technologies with a potential of over-blocking. The CJEU concluded that such prior filtering restricts an important means of disseminating online content and therefore constitutes a limitation of Article 11 of the EU Charter. The CJEU nevertheless upheld Article 17, finding a justification for this limitation. Several scholars have suggested that the CJEU's conclusions have implications outside the copyright realm on obligations for platforms to detect illegal content. Although this linkage is suggested, it has up to now not been looked into exhaustively. This article aims to answer the question what the legal implications of Case C-401/19 are for the regime of *de facto* obligations on online content-sharing platforms under EU law to act against illegal content ex ante more generally. It distils other *de facto* obligations on online content-sharing platforms to carry out a prior review of content. These obligations are all governed by the prohibition of general monitoring obligations (e.g. Article 8 DSA). The CJEU treats this prohibition as a safeguard to the freedom of expression. Consequently, online content-sharing platforms should only block content that is clearly illegal. This article shows that the fundamental importance of the freedom of expression and information of the users of the internet needs to play a key role in designing obligations to act against illegal content both inside and outside the area of copyright law.

Keywords: content moderation; online platforms; illegal content; freedom of expression; general monitoring obligation

Recommended citation: Willemijn Kornelius, Prior filtering obligations after Case C-401/19: balancing the content moderation triangle, 14 (2023) JIPITEC 123 para 1.

A. Introduction

1 People increasingly share and access information and works ("content") on the available services on the Internet such as online content-sharing platforms.[1] Online content-sharing platforms, like Facebook and Twitter, provide their users with the possibility to

* Legal Research master student at Utrecht University and Civil Law (Intellectual Property) graduate from Leiden University. The author would like to thank Dr. Vicky Breemen, Assistant Professor at Utrecht University for her helpful guidance in the course of this work and comments on earlier versions of this article and the researchers of the Centre of Private Governance (CEPRI) of the University of Copenhagen for offering the possibility to visit their centre as a visiting researcher and the fruitful discussions that contributed to this article.

1 E.g. S Kulk, 'Internet Intermediaries and Copyright Law. Towards a Future-proof EU Legal Framework' (PhD-thesis, Utrecht University 2018) 56; K Erickson and M Kretschmer, 'Empirical approaches to Intermediary Liability' in: G Frosio (ed), *The Oxford Handbook of Intermediary Liability Online* (OUP 2020), also accessible < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3400230> accessed 5 February 2023, 2.

express themselves with a potential global reach and to participate in ongoing discussions. The European Court of Human Rights ("ECtHR") repeated in *Vladimir Kharitonov v. Russia* that the Internet has become one of the most important means for individuals to exercise their right to freedom of expression and information.[2]

2 However, illegal content is an immediate concern of the European legislature. "Illegal content" comprises information or works uploaded by internet users (related to an activity that is) not in compliance with the law.[3] For example, such content could be the spreading of information concerning child sexual abuse, large scale copyright infringements or incitements to violence.[4] Initially, the European legislature considered it disproportional to hold online platforms liable for illegal activities of their users (such as copyright infringement or hate speech).[5] The European E-Commerce Directive 2000/31/EC ("E-Commerce Directive") contains liability exemptions for online intermediaries ("safe harbours"). In these situations an online platform is—in short—not liable if they do not have actual knowledge of the illegal content or act expeditiously to remove it. As the digital environment changed, so did this policy focus.[6] The wish to control and tackle online harm and illegal content online, has resulted in stronger regulation and stronger liability rules for online platforms.[7] These online platforms are considered to be best placed to bring infringing activities to an end.[8]

3 In the area of copyright law, the liability of intermediaries, such as online content-sharing platforms, has evolved quite progressively. The CJEU construed this type of liability in its case law.[9] In light of the new challenges posed by the increasing digitalisation, the EU adopted the Directive on Copyright in the Digital Single Market ("DSM-directive") in 2019.[10] The coming into being of this directive was not an easy road. Especially the introduction of a liability framework with a "staydown"-obligation for online content-sharing service providers ("OCSSPs"), e.g., Article 2(6) DSM) in Article 17 was controversial.[11] It requires these OCSSPs to proactively take measures *ex ante*. *Ex ante* here means: "before content is uploaded".[12]

---

2 *Vladimir Kharitonov v. Russia* App no. 10795/14 (ECtHR, 23 June 2020) [33], as laid down in Article 10 ECHR.

3 Definition partly derived from the definition given in the Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market For Digital Services and Amending Directive 2000/31/EC (Digital Services Act) ("DSA") article 3 (h).

4 Commission, 'Recommendation on measures to effectively tackle illegal content online', C(2018) 1177 final 1.

5 The European legislature wanted to create a technology-neutral regulatory environment: Commission, 'Online Platforms and the Digital Single Market. Opportunities and Challenges for Europe (Communication)' COM (2016) 288 final, 7-8; MRF Senftleben and C Angelopoulos, 'The Odyssey of the Prohibition on General Monitoring Obligations on the Way to the Digital Services Act: Between Article 15 of the E-Commerce Directive and Article 17 of the Directive on Copyright in the Digital Single Market' (Study for IViR & CIPIL 2020) 2.

6 M Husovec, '(Ir)Responsible Legislature? Speech Risks under the EU's Rules on Delegated Digital Enforcement' available at https://ssrn.com/abstract=3784149 accessed on 5 February 2023, 7.

7 Erickson and Kretschmer (n 1) 2; JP Quintais and SF Schwemer, 'The Interplay between the Digital Services Act and Sector Regulation: How Special Is Copyright?' (2022) 13 European Journal of Risk Regulation 191, 192.

8 See already in recital 59 of Directive 2001/29/EC of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society [2001] OJ L 167/10 ("Copyright Directive"); Commission, 'Recommendation on measures to effectively tackle illegal content online', C(2018) 1177 final [2] and [3].

9 E.g.: Case C-314/12 *UPC Telekabel Wien* [2014] ECLI:EU:C:2014:192; Case C-70/10 *Scarlet Extended / SABAM* [2011] ECLI:EU:C:2011:771.

10 Directive (EU) 2019/790 of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC OJ L 130/92 ("DSM-Directive").

11 During the adoption procedure, the article was known as the "meme ban". See for example: M. Reynolds, 'What is article 13? The EU's divisive new copyright plan explained', WIRED 24 mei 2019, <wired.co.uk/article/what-is-article-13-article-11-european-directive-on-copyright-explainedmeme-ban> accessed on 21 June 2022. And see further on this controversial article: A Metzger and M Senftleben, 'Selected Aspects of Implementing Article 17 of the Directive on Copyright in the Digital Single Market into National Law – Comment of the European Copyright Society' (2020) 2 JIPITEC 115, 115; JP Quintais ea, 'Safeguarding User Freedoms in Implementing Article 17 of the Copyright in the Digital Single Market Directive: Recommendations from European Academics' (2019) 3 JIPITEC 277, 277; Husovec, '(Ir)Responsible Legislature? Speech Risks under the EU's Rules on Delegated Digital Enforcement' (n 6) 6-7.

12 It can also refer to *ex ante* safeguards: meaning that safeguards have to be implemented before content is uploaded.

4 The problem with obligations to *ex ante* ensure "stay-down" of illegal content are the filtering technologies platforms put in place. These technologies tend to excessively block information: "over-blocking".[13] Over-blocking means that not only illegal, but also *legal* content is blocked. Removal of legal content would constitute an infringement of users' freedom of expression.[14] This fear led Poland to issue an annulment procedure against (parts of) Article 17 DSM-directive. On 26 April 2022, the CJEU finally published its ruling (*Poland v. Parliament and Council* ("C-401/19")). The CJEU admits that the use of automatic filtering technologies is inevitable.[15] This constitutes a *de facto* obligation to carry out a prior review of content users wish to upload. In this sense, and in the rest of this article, a *de facto* obligation is understood as an obligation that is not prescribed by the law itself in that way, but there is in fact no alternative way to comply with the legal obligation. Despite this observation, the CJEU chooses to uphold Article 17 DSM-directive.[16]

5 Obligations on online content-sharing platforms to proactively act *ex ante* against illegal content, requiring the implementation of automatic filtering technologies will exist under the wings of the Digital Services Act ("DSA").[17] Moreover, additional sector-specific regulations of different types of content strengthen the responsibilities of online content-sharing platforms to act. C-401/19 is embedded in the prohibition of a general monitoring obligation (Article 17(8) DSM-directive and Article 15 e-Commerce Directive), which is also in the DSA (Article 8). Several scholars have suggested that the CJEU's conclusions have implications outside the copyright realm on obligations in the European Union for platforms to detect illegal content.[18]

6 Although this linkage is suggested, it has not been looked into exhaustively. Scholars focus on the impact of the DSA on copyright content moderation in the EU.[19] They describe the interplay between the DSA and Article 17 and their *lex specialis-lex generalis* relationship.[20] In this article, I therefore aim to answer the following question "what are the legal implications of the CJEU's ruling in C-401/19 on Article 17 DSM-directive for the regime of *de facto* obligations on online content-sharing platforms under EU law to act against illegal content *ex ante* more generally?"

7 I focus on the EU legal framework that applies to online content-sharing platforms of which users post illegal content. These platforms are information society service providers with the aim to store and give the public access to a large amount of works or information uploaded by their users ("content"), which they organise and promote for profit-making purposes.[21] This definition is partly derived from Article 2(6) DSM-directive, but broadens the concept because it does not solely focus on copyright-

13 Case C-401/19 *Poland v Parliament and Council* [2022], Opinion of AG Saugmandsgaard Øe, ECLI:EU:C:2021:613, para 142; L Fiala and M Husovec, 'Using experimental evidence to improve delegated enforcement' (2022) 71 International Review of Law & Economics, 1; C Geiger and BJ Jütte, 'Platform liability under Article 17 of the Copyright in the Digital Single Market Directive, Automated Filtering and Fundamental Rights: An Impossible Match' (2021) 70 GRUR International 517, 546.

14 This freedom is protected by Article 10 ECHR and Article 11 Charter of Fundamental Rights of the European Union 2012/C 362/02 ("Charter").

15 Case C-401/19 *Poland v Parliament and Council* [2022] ECLI:EU:C:2022:297, para 54.

16 Case C-401/19 *Poland v Parliament and Council* [2022] ECLI:EU:C:2022:297, paras 85-86, 90-92.

17 Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market For Digital Services and Amending Directive 2000/31/EC (Digital Services Act) ("DSA").

18 F Reda, 'Wieviel Automatisierung verträgt die Meinungsfreiheit?' 2 May 2022, https://verfassungsblog.de/wieviel-automatisierung-vertragt-die-meinungsfreiheit/ accessed 5 February 2023; A Peukert ea, 'European Copyright Society – Comment on Copyright and the Digital Services Act Proposal' (2022) 53 IIC 370; JP Quintais, 'Between filters and fundamental rights. How the Court of Justice saved Article 17 in C-401/19 – Poland v. Parliament' 16 May 2022, <'https://verfassungsblog.de/filters-poland/'> accessed 5 February 2023; JP Quintais ea, 'Copyright Content Moderation in the EU: An Interdisciplinary Mapping Analysis' (ReCreating Europe 2022) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4210278 accessed 31 January 202331 January 2023, 126.

19 JP Quintais ea, 'Copyright Content Moderation in the EU: An Interdisciplinary Mapping Analysis' (ReCreating Europe 2022) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4210278 accessed 31 January 2023, 126.

20 JP Quintais ea, 'Copyright Content Moderation in the EU: An Interdisciplinary Mapping Analysis' (ReCreating Europe 2022) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4210278 accessed 31 January 2023, 126ff; Peukert ea (n 18) 358. See also recitals 9-11 DSA.

21 The definition "information society service providers" was already introduced in Directive 98/34/EC and Directive 98/84/EC (Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("E-Commerce Directive"), recital 17) and repeated in the E-Commerce Directive,recital 17 and Article 2(a) and (b).

protected content. It also aligns with the definition of an "online platform" as laid down in Article 3(i) DSA. The definition in the DSA, however, is broader and does not refer to "profit-making".[22]

8 Before a legal analysis is made of the different regulatory frameworks at play, I give a theoretical background of the context of content moderation in which these frameworks have effect (Section B). I outline the existing EU framework of platform liability to distil what other obligations exist in Section C. I describe the case of platform liability under EU copyright law in more detail to determine the place of Article 17 of the DSM-directive within EU law. I use the applicable EU legislation, relevant case law and academic literature. I supplement this by (legal-)empirical studies on automated content moderation tools to achieve an understanding of the risks of over-blocking for the freedom of expression in practice (Section D). I continue with an analysis of Case C-401/19 (Section E). Finally, I compare the *de facto* obligations to act against illegal content *ex ante* within the EU with Article 17 of the DSM-directive to determine what Case C-401/19 implies for these obligations (Section F).

B. Content moderation of illegal content: a triangle relationship

9 In this section, I describe the context in which the obligations under consideration have effect. This type of regulation is meant to mitigate the effects of illegal content (Section B.I). I demonstrate that obliging online content-sharing platforms to act against illegal content is a form of regulation *of* platforms leading to regulation *by* platforms (Section B.II). We can witness a content moderation triangle relationship between platform, user(s) and affected parties emerging in this area (Section B.III).

I. Illegal content

10 This article covers obligations resulting from EU legislative initiatives to tackle illegal content online. The EU legislature perceives illegal content to be content that comprises information or works (related to an activity that is) not in compliance with the law (Article 3(h) DSA).[23] The "law" could be EU law or the law of a Member State. Illegal could be information relating to terrorism, pictures or videos from child sexual abuse, illegal hate speech, but also posts that infringe copyrights.[24]

11 Illegal content has negative consequences which should be addressed. Content containing copyright protected material infringes the rights of the copyright holder. A post that incites hatred against someone or a group of people, negatively effects these persons, but also negatively impacts the public more generally.[25] The dissemination of radical terrorist content endangers general security.[26] The Commission spells out that the presence of illegal content has serious negative consequences "for users, affected citizens and companies and for society at large".[27] Illegal content interferes with the interests the laws attempt to safeguard. Dealing with the illegal activities underlying illegal content, enforcement of the law and the protection of the interests, is traditionally seen as a public state responsibility.[28] Online content-sharing platforms are taking over parts of this role.

II. Platform governance and regulation "of" and "by" online platforms

12 The wish to tackle illegal content results in regulation *by* platforms following regulation *of* platforms. As described in Section A, the European legislature targets online platforms to act against the illegal content uploaded on their platforms, for example

22 The definition is thus broader than 'content- sharing platforms', it e.g. also comprises 'online marketplaces': see J Barata ea, 'Unravelling the Digital Services Act package' (IRIS Special 2021-1, European Audiovisual Observatory 2021) 32.

23 See also: Commission, 'Recommendation on measures to effectively tackle illegal content online', C(2018) 1177 final [14] and Article 4(b).

24 Commission, 'Recommendation on measures to effectively tackle illegal content online', C(2018) 1177 final [1]-[2]; recital 12 DSA.

25 Code of Conduct on Countering Illegal Hate Speech Online, < https://ec.europa.eu/info/files/code-conduct-countering-illegal-hate-speech-online_en> accessed 5 February 2023, 1.

26 M Rojszcak, 'Online content filtering in EU law – A coherent framework or jigsaw puzzle?' (2022) 47 Computer Law & Review.

27 Commission, 'Recommendation on measures to effectively tackle illegal content online', C(2018) 1177 final [2].

28 E.g. R Gorwa, 'What is platform governance' (2019) 22 Information, Communication & Society 854, 856; CS Petersen, VG Ulfbeck and O Hansen, 'Platforms as Private Governance Systems – The Example of Airbnb' [2018] NJCL 38.

through regulations concerning their liability for this content.[29] In this article, I understand "liability of online platforms" to refer to obligations imposed on these platforms to act against illegal content of their users.[30] It encompasses liability for damages but also, and important in this context, legal obligations to act, such as injunctions, or court orders.[31] To comply with their responsibilities and in order to remain immune from liability, online platforms are required to take action once they obtain knowledge of illegal activities ("notice-and-action") or comply with orders to delete and prevent uploads of illegal content.[32] This type of regulation can be described as regulation *of* platforms.[33]

13 Online content-sharing platforms increasingly act to remove or disable access to illegal content. The platform thereby governs and orders the activity of its users: "platform governance".[34] Platforms set rules (terms and conditions, behavioural guidelines) and install 'notice-and-takedown'-systems and *ex ante* content filtering systems.[35] The platform assesses whether uploaded information is indeed illegal or infringing and decides to act or not.[36] To effectuate all this, platforms need to employ technical measures, such as algorithmic content detection.[37] As underlined in academic research and literature, the management of users' activity that emerges through these technologies is a form of regulation *by* platforms.[38]

III. Content moderation through technologies: removing illegal content

14 The regulation *by* platforms resulting from the EU regulation *of* platforms results in activities these platforms undertake to detect, remove or disable access to illegal content. In this article, I address these activities as "content moderation". I thereby align with the only definition thereof in EU law, found in article 3(t) DSA.[39] The DSA refers to both automated and non-automated activities. In light of the question central to this article, I focus on automated activities.

15 Husovec describes the content moderation practices as "delegated enforcement" because the action taken against illegal practices is left to private actors, in this case, online content service providers ("OCSPs").[40] Here, we can see a triangle relationship. As online platforms are given the responsibility to protect public or private interests protected

29 Husovec, '(Ir)Responsible Legislature? Speech Risks under the EU's Rules on Delegated Digital Enforcement' (n 6) 7. Mechanisms such as: Article 17 DSM-directive, Article 12-15 E-Commerce Directive, the Commission, 'Recommendation on measures to effectively tackle illegal content online', C(2018) 1177 final, DSA; Regulation (EU) 2021/784 of 29 April 2021 on addressing the dissemination of terrorist content online [2021]: Fiala and Husovec (n 13) 12.

30 This definition is partly derived from Kulk's definition of "liability of online intermediaries", Kulk (n 1) 7.

31 See on liability of online platforms: Husovec, '(Ir)Responsible Legislature? Speech Risks under the EU's Rules on Delegated Digital Enforcement' (n 6).

32 A Kuczerawy, 'From 'Notice and Takedown' to 'Notice and Staydown': Risks and Safeguards for Freedom of Expression' in: G Frosio (ed), *Online Intermediary Liability* (OUP 1st edn 2020), 526.

33 JP Quintais ea, 'Copyright Content Moderation in the EU: An Interdisciplinary Mapping Analysis' (ReCreating Europe 2022) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4210278 accessed 31 January 2023, 30.

34 JP Quintais ea, 'Copyright Content Moderation in the EU: An Interdisciplinary Mapping Analysis' (ReCreating Europe 2022) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4210278 accessed 31 January 2023, 29. It refers to R Gorwa, 'The Shifting Definition of Platform Governance' (Centre for International Governance Innovation 23 October 2019) <https://www.cigionline.org/articles/shifting-definition-platform-governance/> accessed 5 February 2023.

35 See e.g. Quintais and Schwemer, (n 7).

36 Kuczerawy (n 32) 524-543; Kulk (n 1) 115.

37 I elaborate on the need to use automatic filtering technologies in section D.

38 JP Quintais ea, 'Copyright Content Moderation in the EU: An Interdisciplinary Mapping Analysis' (ReCreating Europe 2022) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4210278 accessed 31 January 2023, 31; Gorwa, 'What is platform governance' (n 28) 859.

39 Article 3(t) DSA: "'content moderation' means the activities, whether automated or not, undertaken by providers of intermediary services aimed, in particular, at detecting, identifying and addressing illegal content or information incompatible with their terms and conditions, provided by recipients of the service, including measures taken that affect the availability, visibility, and accessibility of that illegal content or that information, such as demotion, demonetisation, disabling of access to, or removal thereof, or the recipients' ability to provide that information, such as the termination or suspension of a recipient's account"

40 Husovec, '(Ir)Responsible Legislature? Speech Risks under the EU's Rules on Delegated Digital Enforcement' (n 6) 3 and 7.

by laws, they embark on activities to remove or disable access to illegal content and interfere with the rights of the users that uploaded this content.[41] Most notably, this concerns the users' right to freedom of expression including the freedom to receive and impart information and ideas in an open democratic society ("freedom of expression") protected by Article 11 of the Charter.[42] In the following figure I display this relationship:

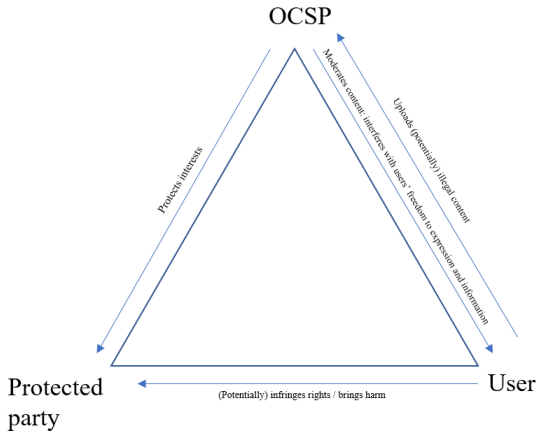

Figure 1: Content moderation triangle where OCSP is the online content-sharing platform

16 For content moderation in the area of copyright law, this relationship can be specified as follows:

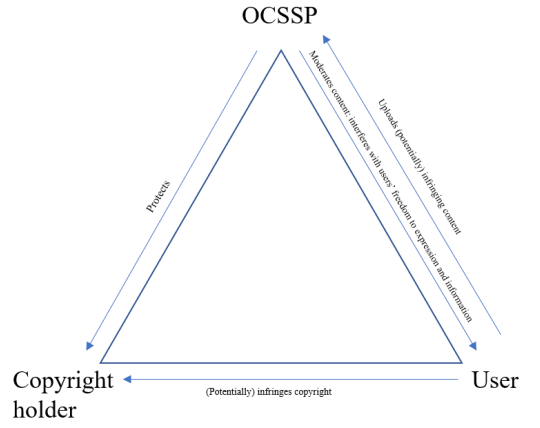

Figure 2: Copyright content moderation triangle where OCSSP is the online content-sharing service provider

41 Fiala and Husovec also recognise the main types of "players": Fiala and Husovec (n 13) 5. About this from a U.S. perspective: K Klonick, 'The New Governors: The People, Rules, and Processes Governing Online Speech', (2018) 131 Harv L Rev 1598, 1662.

42 For the rest of the article, I use "freedom of expression" to refer to the "right to freedom of expression and to receive and impart information and ideas in an open democratic society" of users of online content-sharing platforms. This right is protected by both Article 11 Charter and Article 10 ECHR, but since I focus on the EU law context, Article 11 Charter is mentioned.

17 I focus on content moderation *by* platforms that follows from regulation *of* platforms and its compatibility with the users' freedom of expression. In general, this right is primarily addressed to public institutions.[43] The Charter is addressed to the 'institutions and agencies of the EU and Member States when they implement EU law'.[44] I therefore focus on the importance of the assessment of the CJEU in C-401/19 for obligations on online content-sharing platforms stemming from public institutions. The figures above show that the freedom of expression affects the triangle relationship resulting from these obligations. Content moderation following from voluntary actions by online content-sharing platforms is left outside the scope of this article.[45]

C. European legal framework for platform liability in case of illegal content

18 The obligations of online content-sharing platforms to engage in content moderation in the European Union are governed by a complex puzzle of applicable chunks of legislation and case law.[46] In this section, I provide an overview of this legal framework. I identify *de facto* obligations for online content-sharing platforms to act *ex ante* against illegal content. The general rule of EU platform liability framework is the neutrality of the platform: as long as a platform does not have knowledge of an illegal activity on his platform, they do not have to act (Section C.I). In its Communication on Online Platforms and the Digital Single Market, the Commission chose to upheld the existing liability regime.[47] However, the Commission

43 Article 1 ECHR makes that clear for the rights and freedoms enshrined in the ECHR.

44 Article 51(1) Charter. See on the broad interpretation of 'implementing EU law': J-P Jacqué, 'The Charter of Fundamental Rights and the Court of Justice of the European Union: A First Assessment of the Interpretation of the Charter's Horizontal Provisions' in: LS Rossi and F Casolari (eds), *The EU after Lisbon* (Springer International Publishing 2014) 139.

45 This is done because voluntary content moderation concerns the horizontal relation between platform and its user. There could potentially be importance of the Charter for this relation too, but the scope of this article is too small to cover this too. See on such 'horizontal application' of the Charter: Jacqué (n 44) 149.

46 M Husovec, *Injunctions against Intermediaries in the European Union* (Cambridge University Press 2017) 50.

47 Commission, 'Online Platforms and the Digital Single Market

acknowledged that specific issues for certain types of illegal content had been identified that demand a 'sectorial, problem-driven approach'.[48] Article 17 DSM-directive embodies a specific approach to copyright infringing material online.[49] The EU legislature thereby created an exception to the neutrality-rule for copyright (Section C.II). The DSA still upholds the idea of neutrality, but the legislature creates obligations for proactive action against illegal content in specific situations outside copyright. Section C.III and C.IV discuss these and how they relate to the precedingly discussed rules.

I. Neutrality of the platform: E-Commerce Directive

19 In 2000, the European legislature introduced the E-Commerce Directive. The European Commission wanted to clarify the legal position of online intermediaries when their users partake in illegal activities.[50] The E-Commerce Directive does *not* create a ground for liability.[51] The Commission merely focused on situations in which online intermediaries should not be held liable to respect users' freedom of expression and to stimulate the development of an innovative digital single market.[52] The E-Commerce Directive restricts the scope of obligations that (national) authorities can impose on online content-sharing platforms to act against illegal content. It provides liability exemptions (Articles 12–14) and prohibits general monitoring obligations (Article 15) as discussed below.[53]

1. Article 14: liability exemption for hosting services

20 The exemptions of Articles 12 to 14 E-Commerce Directive are based on the idea that the service providers are not the providers of information themselves but are merely occupied with the transmission or storage of that information. Shortly put, they lack the control over and knowledge of the content of that information.[54] Online content-sharing platforms function as intermediaries that store information of their users so that other users can access it. It is commonly accepted in legal practice and academic literature that these activities fall under "hosting" (Article 14 E-Commerce Directive).[55] Following Article 14 the online content-sharing platform is not liable when 1) it does not have actual knowledge of the illegal activity or information and is not aware of any facts from which this illegal activity is apparent, or 2) it acts "expeditiously" to remove or disable access to the information after obtaining such knowledge or awareness.[56]

21 The CJEU has stressed that the hosting activities of a platform must be neutral, i.e., merely technical

Opportunities and Challenges for Europe (Communication)' COM (2016) 288 final 9.

48 Commission, 'Online Platforms and the Digital Single Market Opportunities and Challenges for Europe (Communication)' COM (2016) 288 final 8-9. See also: G Frosio and C Geiger, 'Taking Fundamental Rights Seriously in the Digital Services Act's Platform Liability Regime' [2022] European Law Journal (forthcoming), https://www.researchgate.net/publication/350320059_Taking_Fundamental_Rights_Seriously_in_the_Digital_Services_Act%27s_Platform_Liability_Regime_European_Law_Journal_2022_forthcoming?enrichId=rgreq-e145523290ca326851f87a780b0646f8-XXX&enrichSource=Y292ZXJQYWdlOzM1MDMyMDA1OTtBUzoxMDA3MTYwODI5OTQzODEwQDE2MTcxMzcyNjI3MTA%3D&el=1_x_2&_esc=publicationCoverPdf> accessed 3 February 2023.

49 Frosio and Geiger (n 48) 11

50 E-Commerce Directive, recital 5; Commission, 'Proposal for a directive on certain legal aspects of electronic aspects in the internal market' COM(1998) 586 final (Explanatory Memorandum) 6; Kulk (n 1) 104. The uncertainty about the legal position was seen as one of the obstacles that existed for a "genuine single market for electronic commerce" cross-border online services: Commission, 'Proposal for a directive on certain legal aspects of electronic aspects in the internal market' COM(1998) 586 final (Explanatory Memorandum) 12.

51 Senftleben and Angelopoulos (n 5) 6. Creating grounds for intermediary liability is therefore mostly left to the Member States themselves. Article 8(3) Copyright Directive and Article 11 Enforcement Directive are exceptions, see further Section C.II.

52 See Kulk (n 1) 104 and Barata ea (n 22) 21.

53 This section discusses the E-Commerce Directive. These rules still apply until the DSA has fully entered into force, which will be on 17 February 2024 (Article 93 DSA).

54 Kulk (n 1) 105.

55 Kulk (n 1) 111; Barata ea (n 22) 5; Senftleben and Angelopoulos (n 5) 6; Husovec, *Injunctions against Intermediaries in the European Union* (n 46) 52; and case law: Case C-236/08-238/08 *Google France and Google v Louis Vuitton* [2010] ECLI:EU:C:2010:159, para 114; Case C-324/09 *L'Oréal v eBay* [2011] ECLI:EU:C:2011:474, paras 109-110 and Case C-70/10 *Scarlet Extended / SABAM* [2011] ECLI:EU:C:2011:771, para 27.

56 Article 14(1)(a) and (b) E-Commerce Directive.

and automatic.[57] The E-Commerce Directive does not dictate how online content-sharing platforms could obtain their knowledge of illegal activity.[58] Member States have worked this out in different ways.[59] A few Member States have specific rules on 'notice-and-action'-systems.[60] The legal contours of these systems are strongly debated and are a topic in case law of the CJEU as well.[61] This case law is discussed under C.I.3.

2. Article 15: general monitoring obligations prohibited

22 Although Article 14 E-Commerce Directive provides no guidelines of what obligations can be imposed on online platforms, Article 15 explicates that it should not amount to a "general monitoring obligation". The directive does not give a clear definition. Recital 48 suggests that 'duties of care' can be imposed on hosting platforms aimed at detecting and *preventing* illegal activities. Recital 47 indicates that such a general monitoring obligation differs from "monitoring obligations in a specific case". What is supposed to be the difference between "general" and "specific" has been disputed.[62] A topic of debate has been whether Article 15 prohibits preventive measures aimed at future illegal activities or "re-uploads".[63] This could result in an obligation for online platforms to monitor *all* content.

3. Case law of the CJEU

23 In successive rulings, the CJEU attempted to outline what obligations to moderate content are allowed under Article 14 and 15. In *L'Oréal v. eBay* the CJEU explained that Article 15 entails that an online platform cannot be required to actively monitor "all the data of each of its customers".[64] However, the CJEU allows an order to take specific measures to terminate an infringement and prevent future infringements, as long as it is effective and proportionate.[65] Such an order could be the suspension of the individual offender.[66]

24 In further case law, *Scarlett Extended v. SABAM* and *SABAM v. Netlog*, the CJEU specified that measures aimed at preventing future infringements of intellectual property law are allowed, but must comply with Article 12 to 15 E-Commerce Directive.[67] In both cases, the measure at issue was an injunction against a hosting service provider requiring it to install a filtering system.[68] The CJEU held that this filtering system would necessitate the platform to preventively monitor all electronic communications to assess what of it is infringing and thus blocked.[69] This requires active observation of all information and all users, which the CJEU found to be prohibited by Article 15.[70]

25 Additionally, the CJEU held that this filtering obligation had to be assessed in light of the protection of fundamental rights of the persons affected by the filtering (i.e., users).[71] According to the CJEU, a filtering system might not be able to adequately distinguish between unlawful and lawful content. The potential blocking of lawful content undermines the freedom of information of the platform's users.[72]

57 E-Commerce Directive, recital 42; Case C-324/09 *L'Oréal v eBay* [2011] ECLI:EU:C:2011:474, para 113.

58 Husovec, *Injunctions against Intermediaries in the European Union* (n 46) 53.

59 Husovec, *Injunctions against Intermediaries in the European Union* (n 46) 53.

60 Kulk (n 1) 115. For example: Finland has a statutory notice-and-takedown regime for copyright infringements; the Netherlands has adopted a code of conduct.

61 Senftleben and Angelopoulos (n 5) 7.

62 Senftleben and Angelopoulos (n 5) 7.

63 Kuczerawy (n 32) 524-543; Senftleben and Angelopoulos (n 5) 7-8.

64 Case C-324/09 *L'Oréal v eBay* [2011] ECLI:EU:C:2011:474, para 139.

65 Case C-324/09 *L'Oréal v eBay* [2011] ECLI:EU:C:2011:474, para 141.

66 Barata ea (n 22) 9.

67 Case C-70/10 *Scarlet Extended / SABAM* [2011] ECLI:EU:C:2011:771, para 34; Case C-360/10 *SABAM v. Netlog* [2012] ECLI:EU:C:2012:85, paras 29-30.

68 Case C-360/10 *SABAM v. Netlog* [2012] ECLI:EU:C:2012:85, para 26; Case C-70/10 *Scarlet Extended / SABAM* [2011] ECLI:EU:C:2011:771, para 29.

69 Case C-70/10 *Scarlet Extended / SABAM* [2011] ECLI:EU:C:2011:771, para 38.

70 Case C-70/10 *Scarlet Extended / SABAM* [2011] ECLI:EU:C:2011:771, paras 39-40; Case C-360/10 *SABAM v. Netlog* [2012] ECLI:EU:C:2012:85, para 38.

71 Case C-70/10 *Scarlet Extended / SABAM* [2011] ECLI:EU:C:2011:771, paras 41-45; Case C-360/10 *SABAM v. Netlog* [2012] ECLI:EU:C:2012:85, para 39.

72 Case C-70/10 *Scarlet Extended / SABAM* [2011]

26 *McFadden v. Sony* concerned a mere conduit service provider (Article 12) and is relevant in light of the accessibility of lawful content.[73] The CJEU reiterated that Article 15(1) E-Commerce Directive prohibits a measure requiring "monitoring of all information transmitted".[74] The measure at issue, requiring an intermediary to prevent users to make copyright-infringing material available, must be strictly targeted without "thereby affecting the possibility of internet users lawfully accessing information using the provider's services", because that would infringe the users' freedom of information.[75]

27 These rulings together raised questions about the permissibility of other filtering obligations. The filtering obligations in the *SABAM*-cases were broad in time (unlimited period), applied to all content and all users.[76] Could it be that measures are only "general" if they ask from platforms to proactively seek for *all* potentially illegal content, but that specific notifications or court orders leading to monitoring of all content are excluded from the scope of Article 15?[77] Based on the wording used by the CJEU in the case law until *McFadden*, the answer would likely have been 'no'.[78] The CJEU excluded measures requiring "monitoring of all information".[79] However, the *Glawischnig-Piesczek*-ruling in 2019 confused this course.[80]

ECLI:EU:C:2011:771, para 52; Case C-360/10 *SABAM v. Netlog* [2012] ECLI:EU:C:2012:85, paras 50-51.

73 Case C-484/14 *McFadden v. Sony* [2016] ECLI:EU:C:2016:689.

74 Case C-484/14 *McFadden v. Sony* [2016] ECLI:EU:C:2016:689, para 87.

75 Case C-484/14 *McFadden v. Sony* [2016] ECLI:EU:C:2016:689, para 93.

76 Senftleben and Angelopoulos (n 5) 12.

77 Senftleben and Angelopoulos (n 5) 12 and footnote 34.

78 Senftleben and Angelopoulos (n 5) 13; JP Quintais ea, 'Copyright Content Moderation in the EU: An Interdisciplinary Mapping Analysis' (ReCreating Europe 2022) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4210278 accessed 31 January 2023, 80; Kuczerawy (n 32) 540.

79 Case C-484/14 *McFadden v. Sony* [2016] ECLI:EU:C:2016:689, para 87.

80 C Rauchegger and A Kuczerawy, 'Court of Justice Injunctions to remove illegal online content under the eCommerce Directive: Glawischnig-Piesczek' (2020) 57 Common Market Law Review 1496.

4. Glawischnig-Piesczek

28 *Glawischnig-Piesczek* concerned a dispute between Eva Glawischnig-Piesczek, an Austrian politician for the Greens, and Facebook. A Facebook user published an article about the Greens on its personal page, resulting in a thumbnail with the title of that article, complemented by a picture of Glawischnig-Piesczek. The user posted a comment in connection to the article. An Austrian court found this comment to be defamatory to Glawischnig-Piesczek.[81] The question at issue was whether an injunction ordering an online platform to remove "identical and equivalent" information to the information previously declared to be illegal was compatible with Article 15 E-Commerce Directive.

29 The CJEU does not mention its previous case law cited above at all. It states that Article 15 does not concern monitoring obligations in a specific case.[82] Such a specific case could be a certain piece of information examined and assessed by a court and found to be illegal.[83] The CJEU further considered that, because of the "genuine risk that information which was held to be illegal is subsequently reproduced and shared by another user", it is legitimate that the online platform is ordered to block access to information that is identical or equivalent to the content of the illegal information.[84] This requires the platform to monitor all the content uploaded to the platform.[85]

30 However, as the CJEU continues, Article 15 E-Commerce Directive means that an order to monitor must not be an "excessive obligation" on the online platform and that the different interests at stake should be balanced.[86] The required monitoring should be limited to information containing the elements specified in the order and the identical or equivalent nature of that content does not require the platform to "carry out an independent assessment". The CJEU thereby takes into consideration that the platform had "automated search tools and

81 Case C-18/18 *Glawischnig-Piesczek* [2019] ECLI:EU:C:2019:821, para 12.

82 Case C-18/18 *Glawischnig-Piesczek* [2019] ECLI:EU:C:2019:821, para 34

83 Case C-18/18 *Glawischnig-Piesczek* [2019] ECLI:EU:C:2019:821, para 35.

84 Case C-18/18 *Glawischnig-Piesczek* [2019] ECLI:EU:C:2019:821, paras 36-38.

85 Rauchegger and Kuczerawy (n 80) 1504.

86 Case C-18/18 *Glawischnig-Piesczek* [2019] ECLI:EU:C:2019:821, paras 43-44.

technologies" at its disposal.[87] This reasoning caused a lot of debate in academic literature. Until now, the debate remains unsettled.[88]

31 Angelopoulos and Senftleben argue that the CJEU herewith turns Article 15 in a reasonability test, rather than a hard prohibition.[89] It seems to permit an obligation leading online platforms to use filtering technologies to detect and remove illegal content amongst *all* the content of their users, as long as online platforms are not required to independently assess whether content is illegal and filtering is limited to predetermined information.[90] In this case there was a national court that determined the comment to be illegal. This leaves open the question whether notices of private entities could lead to an obligation to remove identical and equivalent content.[91]

II. Stronger obligations to act: the case of copyright

32 Liability of online content-sharing platforms for copyright infringements is a sector-specific *lex specialis* to the *lex generalis*-system of the E-Commerce Directive as discussed in Section C.I.[92] It is governed by an interplay of the Copyright Directive, E-Commerce Directive and the DSM-directive.[93] In this area, the EU legislature has envisaged strong obligations to act against infringing content, sometimes requiring *ex ante* actions.

33 The Copyright Directive harmonises the rules of copyright law to a great extent.[94] Platform liability for copyright infringements of their users is therefore more harmonised at EU level compared to other types of illegal content and has taken shape in two ways. There is direct liability (Article 3 Copyright Directive and since 7 June 2021 Article 17 DSM-directive) and indirect liability as an intermediary (Article 8(3) Copyright Directive). As a result, the platform might be obliged to act against the infringements and to engage in content moderation. The CJEU has played a significant role in determining the contours of the liability of online content-sharing platforms when their users upload copyright infringing material.[95]

1. Direct liability: Article 3 Copyright Directive

34 The Copyright Directive grants an exclusive right to copyrightholders to "authorise or prohibit any *communication to the public* of their works" in Article 3. This exclusive right encompasses communication at a distance.[96] This concept is broadly interpreted to cover the multiple ways offered by new technologies to disseminate works.[97] A user that uploads copyright protected material to an online content-sharing platform, so that others can access or even download it, communicates it to the public.[98] If the user does not have permission from the rightholder and there

87 Case C-18/18 *Glawischnig-Piesczek* [2019] ECLI:EU:C:2019:821, paras 45-46.

88 See e.g.: JP Quintais ea, 'Copyright Content Moderation in the EU: An Interdisciplinary Mapping Analysis' (ReCreating Europe 2022) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4210278 accessed 31 January 2023, 81; F Reda, 'Wieviel Automatisierung verträgt die Meinungsfreiheit?' 2 May 2022, https://verfassungsblog.de/wieviel-automatisierung-vertragt-die-meinungsfreiheit/ accessed 5 February 2023.

89 Senftleben and Angelopoulos (n 5) 14.

90 See e.g. D Keller, 'Facebook Filters, Fundamental Rights, and the CJEU's Glawischnig-Piesczek Ruling' (2020) 69 GRUR International 616, 620. She suggests that this ruling prohibits the obligation on online platforms to employ human reviewers.

91 Senftleben and Angelopoulos (n 5) 15.

92 Quintais and Schwemer (n 7) 191.

93 The Enforcement Directive also applies, but will be left outside the scope of this analysis.

94 Directive 2001/29/EC of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society [2001] OJ L 167/10 ("Copyright Directive").

95 See e.g. its most recent case: Joined cases C-682/18 and C-683/18 *YouTube and Cyando* [2021] ECLI:EU:C:2021:503.

96 Copyright Directive, recital 23-24.

97 Copyright Directive, recital 5 together with recital 23. This broad interpretation has been confirmed by the CJEU in its case law: Joined cases C-682/18 and C-683/18 *YouTube and Cyando* [2021] ECLI:EU:C:2021:503, para 63. Some constitutive case law of the CJEU on the concept "communication to the public": Joined Cases C-403/08 and C-429/08 *Football Association Premier League and Others* [2011] ECLI:EU:C:2011:631; Case C-466/12 *Svensson* [2014] ECLI:EU:C:2014:76; Case C-160/15 *GS Media* ECLI:EU:C:2016:644, paras 35 and 37 (concepts 'communication' en 'public'); Case C-527/15 *Brein/Filmspeler* [2017] ECLI:EU:C:2017:300.

98 Case C-610/15 *Stichting Brein* [2017] ECLI:EU:C:2017:456, para 34. See i.a. about this DJG Visser, 'YouTube and Cyando. Auteursrecht en platformaansprakelijkheid' [2021] AA 1022, 1023.

is no exception that protects them, they infringe copyright. This makes the upload illegal.[99]

35 But what is the legal position of the online content-sharing platform when this happens? In some situations, the CJEU has ruled, they could be directly liable as "communicators to the public". The most recent case in this context is *YouTube and Cyando*, in which the CJEU ruled specifically on content-sharing platforms.[100] Previous cases *Stichting Brein* and *GS Media* already dealt with the question of an act of communication by a platform.[101] On the basis of these cases, first of all, it has to be established whether the online content-sharing platform played an *indispensable* role in facilitating the act of communication.[102] In addition, the intervention by the platform should be deliberate.[103] He should intervene in full knowledge of the consequences of doing so with the aim of giving the public access to protected works.[104] In paragraph 84 of the judgment, the CJEU lists factors that have to be taken into account.[105] These factors imply that as long as the content-sharing platform has a filtering technology that detects infringements, it does not make a communication to the public itself.[106] The question remains whether the platform can nevertheless be ordered to act against copyright infringements of its users (indirect liability).

2. Indirect liability: liability for infringements by others

36 If an online content-sharing platform is not a direct infringer on the basis of Article 3 Copyright Directive, the rightholder can still apply for an injunction against an intermediary to end the infringement (Article 8(3)).[107] It is a *lex specialis* of Article 14(3) E-Commerce Directive.[108] The specific details of this injunction must be determined at a national level, but the E-Commerce Directive determines its outer contours.[109] The scope of injunctions is limited by both Article 15 E-Commerce Directive and the freedom of expression.[110] In *YouTube & Cyando*, the CJEU states that an injunction can also be imposed on an platform falling under the exemption of Article 14.[111] Then it repeats its pre-*Glawischnig-Piesczek* case law.[112] As found in *Scarlet Extended* and *SABAM*

99 Recital 12 DSA.

100 Joined cases C-682/18 and C-683/18 *YouTube and Cyando* [2021] ECLI:EU:C:2021:503, para 60.

101 Case C-610/15 *Stichting Brein* [2017] ECLI:EU:C:2017:456; Case C-160/15 *GS Media* [2016] ECLI:EU:C:2016:644.

102 Joined cases C-682/18 and C-683/18 *YouTube and Cyando* [2021] ECLI:EU:C:2021:503, para 68; Case C-610/15 *Stichting Brein* [2017] ECLI:EU:C:2017:456, paras 36-37.

103 Joined cases C-682/18 and C-683/18 *YouTube and Cyando* [2021] ECLI:EU:C:2021:503, para 68.

104 Joined cases C-682/18 and C-683/18 *YouTube and Cyando* [2021] ECLI:EU:C:2021:503, para 81.

105 "inter alia, the circumstance that such an operator, despite the fact that it knows or ought to know, in a general sense, that users of its platform are making protected content available to the public illegally via its platform, **refrains from putting in place the appropriate technological measures** that can be expected from a reasonably diligent operator in its situation in order to counter credibly and effectively copyright infringements on that platform, and the circumstance that that operator participates in selecting protected content illegally communicated to the public, that it provides tools on its platform specifically intended for the illegal sharing of such content or that it knowingly promotes such sharing, which may be attested by the fact that that operator has adopted a financial model that encourages users of its platform illegally to communicate protected content to the public via that platform."

106 JP Quintais ea, 'Copyright Content Moderation in the EU: An Interdisciplinary Mapping Analysis' (ReCreating Europe 2022) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4210278 accessed 31 January 2023, 83; DJG Visser, 'YouTube and Cyando. Auteursrecht en platformaansprakelijkheid' [2021] AA 1022, 1026.

107 Kulk (n 1) 103.

108 C Angelopoulos, 'European Intermediary Liability in Copyright. A Tort-Based Analysis'(PhD-thesis, University of Amsterdam 2016) 61.

109 Kulk (n 1) 103. Article 11 Enforcement Directive repeats this obligation for Member States and expands it to all intellectual property rights infringements.

110 JP Quintais ea, 'Copyright Content Moderation in the EU: An Interdisciplinary Mapping Analysis' (ReCreating Europe 2022) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4210278 accessed 31 January 2023, 79-80; Joined cases C-682/18 and C-683/18 *YouTube and Cyando* [2021] ECLI:EU:C:2021:503, para 134.

111 Joined cases C-682/18 and C-683/18 *YouTube and Cyando* [2021] ECLI:EU:C:2021:503, para 131.

112 C Angelopoulos, 'YouTube and Cyando, Injunctions against Intermediaries and General Monitoring Obligations: Any Movement?' *Kluwer Copyright Blog* 9 August 2021, http://copyrightblog.kluweriplaw.com/2021/08/09/youtube-and-cyando-injunctions-against-intermediaries-and-general-monitoring-obligations-any-movement/> accessed 3 February 2023.

v. Netlog, Article 15 means that an online platform cannot be required to have a filtering mechanism entailing general and permanent monitoring to prevent future infringements.[113] National authorities should strike a fair balance with the freedom of expression and information of internet users.[114]

37 Nevertheless, as the CJEU continues in paragraph 140 to 142 *YouTube & Cyando*, the platform could be required to expeditiously remove or block access to content and to take appropriate measures to prevent further infringements, when a rightholder notifies the platform of an infringement. After *YouTube and Cyando*, it is disputed what the CJEU perceives to be "general monitoring" by online platforms.[115] How far could the measures to prevent further infringements go?

3. Direct liability: Article 17 DSM-directive

38 Since 7 June 2021, the Article 17-framework further complicated the landscape of liability of online content-sharing platforms for copyright infringements. Departing from the safe harbour for hosting platforms, Article 17 introduces obligations on online content-sharing platforms to proactively prevent uploads of illegal content upon receival of necessary information from copyrightholders. It is a *lex specialis* of Article 14 E-Commerce Directive and Article 3 Copyright Directive.[116] Article 17 DSM-directive is based on the wish to strengthen the position of copyrightholders on the internet.[117] Online content-sharing platforms profit from copyright infringing content through targeted advertising, while copyrightholders are barely remunerated for this exploitation of their works: the so-called *value gap*.[118]

39 The starting point of Article 17 is that online content-sharing service providers ("OCSSPs", defined in Article 2(6) DSM-directive) "perform an *act of communication to the public* when [they give] the public access to copyright-protected works (...) *uploaded* by its users".[119] Article 17(3) determines that such an OCSSP does not fall under the liability exemption of Article 14(1) E-Commerce Directive. The online content-sharing platforms under consideration in this article should be seen as to largely fall under the definition of Article 2(6).[120] Consequently, OCSSPs should obtain authorisation of rightsholders for these uploads, for example through licensing agreements (Article 17(1)). If this authorisation is not obtained by the OCSSP, the liability framework of Article 17(4) enters into force. This provision contains three "best-efforts-obligations": the OCSSP should a) make best efforts to obtain an authorisation; and b) make best efforts to ensure that notified copyright protected works are unavailable ('notice-and-takedown'), but also c) make best efforts to prevent future uploads of this protected content ('notice-and-staydown'). The obligation under c) is an *ex ante* legal obligation to prevent illegal content. If the OCSSP does not meet these obligations, he is liable for the copyright infringements.

40 These "best-efforts"-obligations caused a lot of controversy.[121] To comply with these obligations,

113 Joined cases C-682/18 and C-683/18 *YouTube and Cyando* [2021] ECLI:EU:C:2021:503, para 135.

114 Joined cases C-682/18 and C-683/18 *YouTube and Cyando* [2021] ECLI:EU:C:2021:503, para 138.

115 C Angelopoulos, 'YouTube and Cyando, Injunctions against Intermediaries and General Monitoring Obligations: Any Movement?' *Kluwer Copyright Blog* 9 August 2021,http://copyrightblog.kluweriplaw.com/2021/08/09/youtube-and-cyando-injunctions-against-intermediaries-and-general-monitoring-obligations-any-movement/> accessed 3 February; JP Quintais ea, 'Copyright Content Moderation in the EU: An Interdisciplinary Mapping Analysis' (ReCreating Europe 2022) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4210278> accessed 31 January 2023.

116 Commission, 'Guidance on Article 17 of Directive 2019/790 on Copyright in the Digital Single Market (Communication)' COM(2021) 288 final ("Guidance").

117 See DSM-directive, recital 61.

118 E Rosati, 'Five considerations for the transposition and application of Article 17 of the DSM Directive', (2021) 16 Journal of Intellectual Property Law & Practice 265 < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3793056> accessed 3 February 2023;: M Husovec and JP Quintais, 'How to license Article 17? Exploring the Implementation Options for the New EU Rules on Content-Sharing Platforms' (2021) 4 GRUR International 325, 327.

119 Emphasised added.

120 Read in connection with recitals 62 and 63. Article 17(6) determines that this liability framework does not apply to new OCSSPs with an annual turnover below EUR 10 million.

121 There is a lot written about Article 17, previously called Article 13: before ánd after its entry into force. It still continues today, because Member States are struggling with the implementation of the article into their national laws. See e.g.: Husovec, '(Ir)Responsible Legislature? Speech Risks under the EU's Rules on Delegated Digital Enforcement' (n 6); F Reda, 'Filtered Futures Conference: Exploring The Fundamental Rights Constraints of Automated Filtering After the CJEU Ruling on Article 17' *Kluwer Copyright Blog* 17 June 2022 < http://copyrightblog.kluweriplaw.com/2022/06/17/filtered-futures-conference-exploring-

online content-sharing platform inevitably need to install automatic filtering technologies.[122] Due to the impreciseness of these technologies (Section D), they may also block legal content.[123] However, Article 17(7) commands that compliance with the "best-efforts"-obligations of Article 17(4) does not lead to the unavailability of legal (non-infringing) content.[124] Therefore, scholars and other commentators perceive Article 17 to contain *conflicting obligations*.[125]

41 Article 17(8) furthermore iterates the prohibition on the imposition of a general monitoring obligation on online content-sharing platforms. In addition, Article 17(9) contains a set of *ex post* procedural safeguards that online content-sharing platforms should have in place for users whose content is removed or blocked. Recital 70 clarifies that the working of this liability framework, thus the content moderation that follows therefrom, should be in line with the freedom of expression.[126]

III. Obligations to act outside copyright: new EU initiatives on the horizon

42 Since the E-Commerce Directive entered into force 20 years ago, the wish to control the spread of illegal content online led to several regulatory initiatives of the EU legislature.[127] This resulted in a rather fragmented landscape of obligations for platforms to act against illegal content.[128] There are rules for specific types of content, such as child sexual abuse and terrorist content.[129] There are rules for specific online platforms: video-sharing platforms.[130] And then there are soft law initiatives: a Communication and a Recommendation of the Commission trying to set general principles for the fight against illegal content online, focusing on all platforms and all types of content.[131]

43 In this section, I analyse what obligations to prevent *ex ante* that certain illegal content appears online for online content-sharing platforms can be observed resulting in *de facto* obligations to *ex ante* carry out a review of content. I describe the new DSA-proposal and the Terrorist Regulation, since these give concrete substance to what is required from online platforms.

1. Digital Services Act: notice-and-action

44 On 19 October 2022 the Digital Services Act was officially adopted by the EU legislature.[132] This is

the-fundamental-rights-constraints-of-automated-filtering-after-the-cjeu-ruling-on-article-17/> accessed 5 February 2023.

122 See e.g.: MRF Senftleben ea, 'The Recommendation on Measures to Safeguard Fundamental Rights and the Open Internet in the Framework of the EU Copyright Reform' (2018) 40 EIPR 149, 151 and 159; Metzger and Senftleben (n 11) 120.

123 See e.g. F Reda, J Selinger and M Servatius, 'Article 17 of the Directive on Copyright in the Digital Single Market: a Fundamental Rights Assessment' (Study Gesellschaft für die Freiheitsrechte 2020), < https://ssrn.com/abstract=3732223> accessed 5 February 2023, 4 and 13ff.

124 Commission, 'Guidance on Article 17 of Directive 2019/790 on Copyright in the Digital Single Market (Communication)' COM(2021) 288 final ("Guidance"), 2 and 20. See also DSM-directive, recital 66.

125 See e.g. Husovec, '(Ir)Responsible Legislature? Speech Risks under the EU's Rules on Delegated Digital Enforcement' (n 6).

126 DSM-directive, recital 70.

127 Barata ea (n 22) 24ff; I Buri and J van Hoboken, '"The Digital Services Act (DSA) proposal: a critical overview"' (Discussion paper IViR/DSA Observatory 28 October 2021), 5.

128 See for an overview of the different regulatory measures: Barata (n 22) 30-31.

129 Directive 2011/92 of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography [2011]; Regulation (EU) 2021/784 of 29 April 2021 on addressing the dissemination of terrorist content online [2021], Article 21; Commission, 'Proposal for a Regulation laying down rules to prevent and combat child sexual abuse' COM(2022) 209 final ("CSA Proposal").

130 Directive 2010/13 of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive), as amended by Directive 2018/1808 [2018].

131 Commission, 'Tackling Illegal Content Online. Towards an enhanced responsibility for online platforms'(Communication)' COM (2017) 555 final 13; Commission, 'Recommendation on measures to effectively tackle illegal content online', C(2018) 1177 final.

132 Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market For Digital Services and Amending Directive

a horizontal regulation that applies to all digital services and contains general rules. The Commission proposed this regulation to update and harmonize the currently applicable rules on responsibilities of digital services.[133] It largely upholds the general liability framework applicable to online platforms, as provided for by the E-Commerce Directive, but additionally introduces due diligence obligations for the digital service providers. These due diligence obligations are called "asymmetric" obligations, because their application depends on the type of service provider.[134]

45 While maintaining this "core" of the liability framework, it is quite likely that the DSA will revitalize the regime to some extent.[135] The DSA is a regulation and thus directly applicable in the Member States, without a need for transposition. It defines certain concepts relevant for the moderation of illegal content by online content-sharing platforms. It, e.g., defines "illegal content" as discussed in Section B.I. Furthermore, it introduces four categories of digital services, relevant for the application of the due diligence obligations.[136] Barata et al describe these as "Russian dolls", because the first category comprises all the other categories and with every step, the categories get more specific.[137]

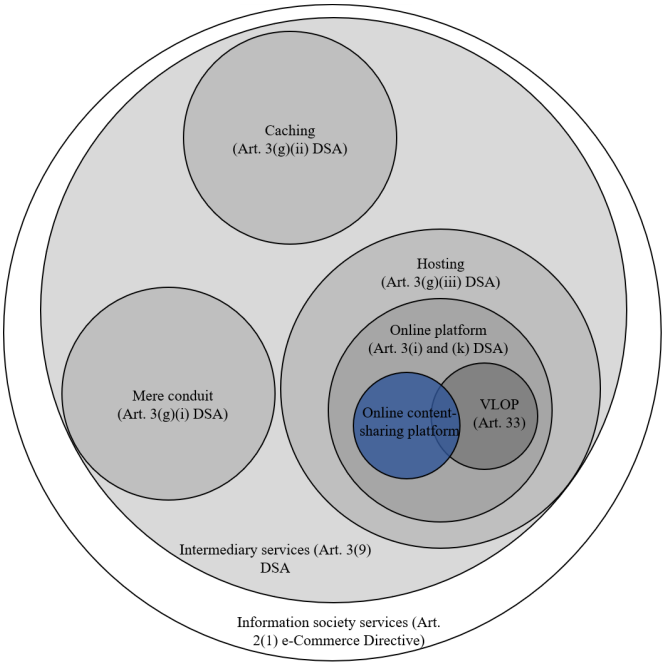

Figure 3: The relation between the different digital services

46 As I display in Figure 3, online content-sharing platforms fall under the provisions that concern intermediary services, hosting services, online platforms and in some cases very large online platforms ("VLOPS").[138]

47 Article 6 DSA contains a liability exemption for hosting services, with identical wording to Article 14 E-Commerce Directive. The European legislature chose to harmonise part of the 'notice-and-action'-mechanisms through an obligation in Article 16 DSA, applicable to hosting providers, including online platforms. Shortly put, the online content-sharing platforms are required to have a mechanism that allows their users to report 'illegal content'.[139] Removal or disabling of access should be undertaken "in the observance of the principle of freedom of expression".[140]

2000/31/EC (Digital Services Act).

133 Commission, 'Shaping Europe's Digital Future' COM (2020) < https://ec.europa.eu/commission/presscorner/detail/en/fs_20_278 > accessed 5 February 2023, 6; recitals 3-5 DSA; Buri and Van Hoboken (n 127) 4.

134 Barata ea (n 22) 33; Buri and Van Hoboken (n 127) 8.

135 Barata ea (n 22) 11.

136 Recital 41 DSA.

137 Barata ea (n 22) 32.

138 The figure is based on the different provisions and recitals of the applicable legislative instruments.

139 Article 16(3) determines that such a notice gives rise to the 'actual knowledge or awareness' meant in Article 6 DSA, which means that the online platform is no longer exempted from liability if he does not act expeditiously to remove or disable access to the content. This concerns an obligation to act *ex post* (after content is already uploaded) and will thus remain outside the scope of this article.

140 Recital 22 DSA. It is not immediately clear whether this provision is a 'due-diligence'-obligation or complements the liability rules. This issue however remains outside the scope of this article, see on this Quintais and Schwemer (n 7) 211.

48 Article 8 repeats the prohibition of a general monitoring obligation for intermediary services as established under Article 15 E-Commerce Directive. It is likely that the case law as discussed in Section C.I.3 remains applicable, as the Commission expressed in the Explanatory Memorandum that the liability rules and key principles of the E-Commerce Directive are upheld and remain valid.[141] The Commission elaborates on the scope of the prohibition in recital 30 DSA. The prohibition does not "concern monitoring obligations in a specific case". Article 9 sets basic conditions for orders of national authorities to online platforms to act against illegal content. Following recital 31, it seems that the European legislature wants to establish a certain limit to 'excessive monitoring obligations' in line with the CJEU's case law in *Glawischnig-Piesczek*.[142]

49 All in all, the DSA does its best to define responsibilities of online platforms. In light of the further discussion of requirements to act against illegal content to avoid liability, it is interesting that the prohibition of a general monitoring obligation is upheld, and that removal of illegal content has to be done in line with the freedom of expression of users. The threat of liability and national court orders will likely motivate the online content-sharing platforms to set up automatic filtering systems to deal with the notices and removal of content.[143] Moreover, along the DSA, sector-specific approaches (such as Article 17 DSM-directive) exist that go further than the neutral approach of the DSA (in continuation of the E-Commerce Directive).

2. Regulation of terrorist content

50 Without the wish to be exhaustive, I address one sectoral approach to illegal content: Regulation 2021/784 addressing the dissemination of terrorist content.[144] It requires cooperation of online content-sharing platforms to combat the spread of terrorist content on their services.[145] Another example would be the proposed regulation for the detection and removal of online child sexual abuse to *complement* the DSA.[146]

51 Article 5(2) of the Terrorist regulation contains the obligation to take specific measures when the platform is exposed to terrorist content. These specific measures are proactive measures, to be taken prior to when the content is uploaded (*ex ante*), such as the identification and preventive removal of terrorist content.[147] Such an obligation exists, when the competent national authority informs the platform about the content (Article 5(4)). It *de facto* creates an obligation to *ex ante* monitor content.[148] The regulation further shapes this obligation: the measures should be applied in a way that respects users' freedom of expression and information (Article 5(3)(c)) and should not lead to a general monitoring obligation or an obligation to use automated tools. Article 5(8) upholds Article 15 E-Commerce Directive. Automated tools to give effect to the obligation are allowed (Recital 25). When automated tools are used, appropriate safeguards should be provided to "to avoid the removal of material that is not terrorist content".[149] The Terrorist Regulation provides an example of how online content-sharing platforms can be *de facto* required by national authorities to priorly review content to detect illegal content outside copyright. It also shows how this obligation should not affect legal content, should not be a general monitoring obligation and should be effectuated in a way that respects the freedom of expression.[150]

141 Proposal for a DSA (Explanatory Memorandum DSA) page 3-4.

142 Case C-18/18 *Glawischnig-Piesczek* [2019] ECLI:EU:C:2019:821, para 46.

143 Buri and Van Hoboken (n 127); EDRI, 'Delete first, think later' 24 March 2021 <https://edri.org/our-work/delete-first-think-later-dsa/> accessed 5 February 2023.

144 Regulation (EU) 2021/784 of 29 April 2021 on addressing the dissemination of terrorist content online [2021].

145 See more extensively on these obligations: A de Streel and M Ledger, 'Regulating the moderation of illegal online content' in: J Barata ea, 'Unravelling the Digital Services Act package' (IRIS Special 2021-1, European Audiovisual Observatory 2021) 26.

146 Commission, 'Proposal for a Regulation laying down rules to prevent and combat child sexual abuse' COM(2022) 209 final (Explanatory Memorandum) 2-3. It builds on the DSA-framework by setting out more specific requirements on detection (Article 7 and 10) and removal (Article 14) of this specific type of illegal activity.

147 Article 5(2) Terrorist Regulation gives examples of these measures. See also: Rojszcak (n 26) 14.

148 J Barata, 'Terrorist content online and threats to freedom of expression. From legal restrictions to choreographed content moderation' 14 March 2022, https://verfassungsblog.de/os4-content-threats/ accessed 3 February 2023.

149 Article 5(3) Terrorist Regulation.

150 Terrorist Regulation, recital 5: "while taking into account the fundamental importance of the freedom of expression, including the freedom to receive and impart information and ideas in an open and democratic society".

IV. De facto obligations to carry out a prior review of content

52 The aforementioned legal framework allows, in specific situations, that obligations are imposed on platforms to prevent uploads from predefined illegal content. The Article 17-DSM-framework requires platforms not only to takedown notified content, but also ensure that notified content that allegedly infringes copyright is not re-uploaded ("staydown"). Such an obligation does not directly follow from the general framework of the E-Commerce Directive and the DSA. Since the DSA finetunes the liability framework of the E-Commerce Directive, it is fair to assume that the Article 17-regime is a *lex specialis* to the DSA-regime.[151]

53 The DSA introduces an obligation for online content-sharing platforms to have notice-and-action-mechanisms. A notification that content is to be regarded illegal, leads to "actual knowledge" of the platform, requiring it to act. What makes Article 17 special, is the staydown-obligation of Article 17(4)(c).[152] But, it is not to say that obligations to detect illegal content before it is uploaded (*ex ante*) cannot exist for other types of illegal content as well.[153] It is allowed by CJEU case law (*Glawischnig-Piesczek*) and in line with recital 25 DSA. Furthermore, such obligations follow from EU sector-specific regulation, such as the Terrorist Regulation (C.III.2).

54 The discussed legislation and case law thus allow obligations to prevent that identical or equivalent information is re-uploaded imposed on platforms, as long as they do not entail a "general monitoring obligation". To achieve the prevention of such uploads, online platforms are *de facto* required to *ex ante* examine uploaded content. I further refer to these obligations as "*de facto* obligations to carry out a prior review of content to detect specific illegal content".[154] The CJEU has made clear that obligations, in whatever form, requiring online platforms to monitor content should 1) not be general monitoring obligations, and 2) are additionally governed by the necessity to balance freedom of expression.

55 Although the Article 17-framework has its own provision using slightly different words, Article 17(8), Article 15 E-Commerce Directive, and Article 8 DSA all contain a prohibition on "general monitoring obligations" for the service providers.[155] It can therefore be assumed that the ban on general monitoring obligations will have the same scope and meaning under the DSA and the Article 17-framework as it did under the E-Commerce Directive.[156] The question is what distinguishes specific monitoring from general monitoring and whether, in line with *Glawischnig-Piesczek*, it can be regarded as a 'reasonability-test', meaning that orders to block content similar or equivalent to previously determined illegal content are allowed, as long as they do not require an independent assessment of the online content-sharing platforms.

56 I displayed the schematic relation between the different obligations in Figure 4. In the next section, I explain why these obligations require platforms to use automatic filtering technologies. In the several above discussed legal provisions and case law of the CJEU, it is repeatedly found that in order to balance the freedom of expression and information of users, lawful content should be left 'untouched'. The next section explains how the use of automatic filtering technologies make exactly that requirement hard to reach creating an imbalance with the freedom of expression and information.

151 Quintais and Schwemer (n 7) 204; Peukert ea (n 18); E Rosati, 'The Digital Services Act and copyright enforcement: The case of Article 17 of the DSM Directive' in: J Barata ea, 'Unravelling the Digital Services Act package' (IRIS Special 2021-1, European Audiovisual Observatory 2021) 67. See also recital 11 DSA: the Copyright Directive and the DSM-directive establish *specific* rules to the DSA and should remain unaffected.

152 E Rosati, 'The Digital Services Act and copyright enforcement: The case of Article 17 of the DSM Directive' (n 151) 71.

153 Rauchegger and Kuczerawy (n 80) 1523.

154 I align with the definition used by the CJEU in Case C-401/19 *Poland v. Parliament and Council* [2022] ECLI:EU:C:2022:297, para 53. Other definitions are: "obligations to proactively monitor content" (Keller (n 90) 616; the A-G in its opinion to Case C-401/19 *Poland v. Parliament and Council* [2022], Opinion of AG Saugmandsgaard Øe, ECLI:EU:C:2021:613, refers to "preventive measures" and "prior restraints", para 77.

155 See also recital 66 DSM-directive and recital 30 DSA. These recitals contain further information that seem to weaken the prohibition on general monitoring obligations to some extent.

156 This is supported by the Commission's Guidance, 22. The Commission has expressed the same for its proposed Regulation on Child Sexual Abuse: it wishes these requirements to "comply with the underlying requirement of fairly balancing the various conflicting fundamental rights at stake that underlies [the prohibition on general obligations to monitor]": Commission, 'Proposal for a Regulation laying down rules to prevent and combat child sexual abuse' COM(2022) 209 final (Explanatory Memorandum) 5.

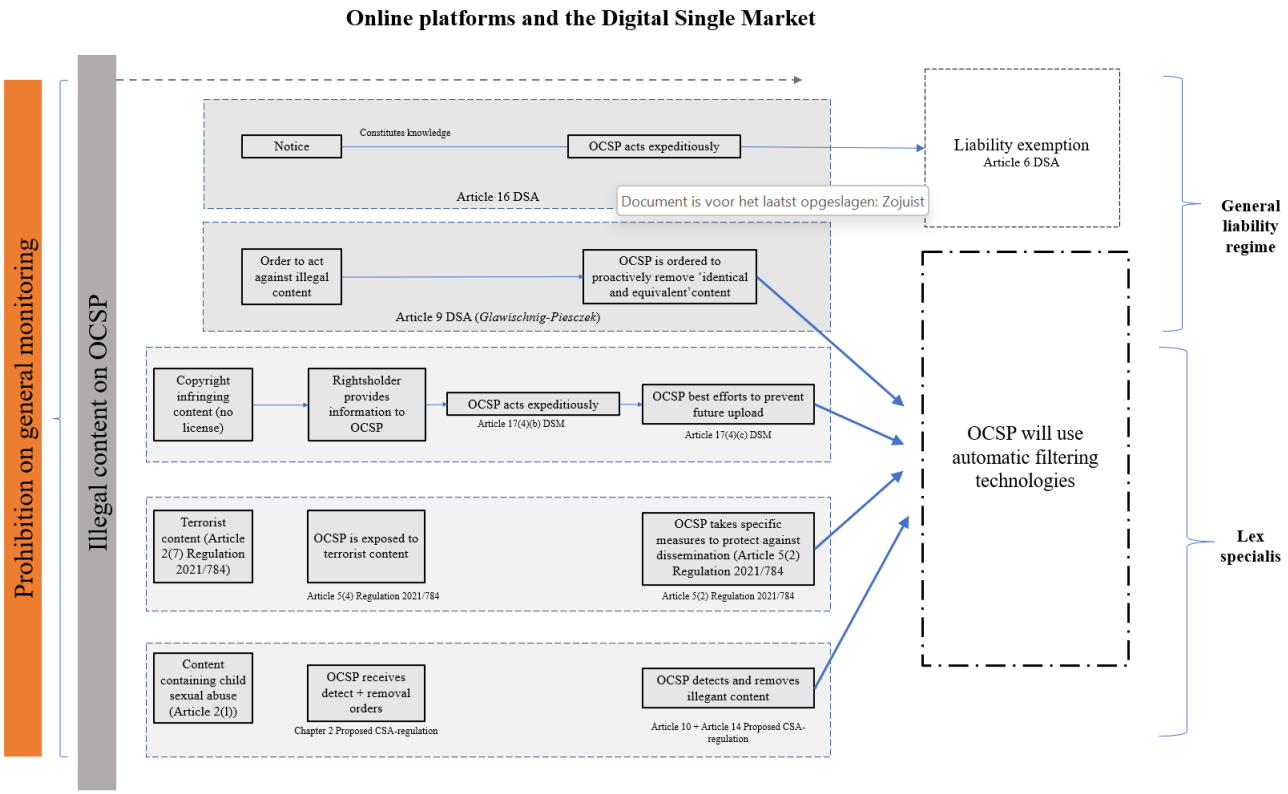

Figure 4: the relations between different obligations to act against illegal content, governed by the prohibition of a general monitoring obligation

D. Automatic filtering technologies and the risk of over-blocking

57 From the discussion of the EU legal framework in Section C, we can conclude that the platform liability framework should be enforced *in observance* of the prohibition of a general monitoring obligation and the freedom of expression as laid down in Article 11 of the Charter.[157] In this section, I distil one of the problems of *de facto* obligations to carry out a prior review of content for the safeguarding of this fundamental right. I explain that online content-sharing platforms resort to automated filtering technologies to comply with their responsibilities.[158] These technologies enable to search for infringing content ("content recognition") in order to manually or automatically block that content ("filtering").[159] The central question to this section is *how* the use of these technologies (potentially) interferes with users' freedom of expression and information through the risk of over-blocking.

I. Use of automatic filtering technologies is inevitable

58 Under the obligations at issue, online content-sharing platforms have to engage in *ex ante* content moderation of illegal content to ensure they can be exempted from liability.[160] Consequently, while the exact scope of what types of 'specific' monitoring obligations are admissible is disputed, the legal framework leads to the use of automated technologies. When online content-sharing platforms are *de facto* obliged to prevent uploads of specific content, it is commonly accepted that they need to resort to *automatic filtering technologies* that block notified content that is indeed found to be illegal.[161] Its use is also stimulated by the

157 See for example Joined cases C-682/18 and C-683/18 *YouTube and Cyando* [2021] ECLI:EU:C:2021:503, para 113.

158 See also the figure in Section C.IV.

159 See the discussion of these technologies in the opinion of the AG to Case C-401/19 *Poland v. Parliament and Council* [2022], Opinion of AG Saugmandsgaard Øe, ECLI:EU:C:2021:613, paras 57ff.

160 Frosio and Geiger (n 48) 13; see on the relation between liability and content moderation also: S Kulk and T Snijders, 'Casestudy Content Moderation door online platformen' in: S Kulk and S van Deursen, *Juridische aspecten van algoritmen die besluiten nemen. Een verkennend onderzoek*, (WODC 2020) 49.

161 Keller (n 90) 618; R Gorwa, R Binns and C Katzenbach, 'Algorithmic content moderation: Technical and political challenges in the automation of platform governance'

Commission.[162] Humans will not be able to cope with the stream of notices following from the notice-and-action-mechanisms in place.[163] Nor will they be able to search through all the uploads to identify "identical or equivalent" content in the case of an imposition to actively block identical or equivalent notified content (*Glawischnig-Piesczek*).[164]

59 Content-sharing platforms deploy different technologies to tackle illegal content.[165] Substantial empirical research describes these technologies and how they work.[166] Broadly, these works distinguish "*matching* technologies" and "*predicting* technologies".[167] *Matching* technologies typically aim for identifying whether uploaded content *matches* content that was already found or notified as illegal.[168] *Matching* technologies are particularly useful for a platform that needs to detect predefined illegal content. *Predicting* technologies aim at *classifying* (or *predicting*) the content as falling into one of the categories of illegal content.[169] The scope of this article is too short to exhaustively discuss the technical details of the different technologies that are used.

60 What the technologies have in common, is that they aim for "content recognition", for which they rely on algorithms.[170] An example of a *matching* technology is the Content ID-technology of YouTube, used to find copyright infringing content.[171] Very simplified, it works as follows. The technology used is *fingerprinting*.[172] Copyright holders can add files with details about their copyright protected works to a *reference database*.[173] This file is given

[2020] Big Data & Society 1, 2; J van Hoboken ea, 'Hosting intermediary services and illegal content online: An analysis of the scope of article 14 ECD in light of developments in the online service landscape' (Study for the European Commission by IViR 2019) 26.

162 Commission, 'Impact Assessment Report Annexes accompanying the Proposal for a Regulation on a Single Market for Digital Services (Digital Services Act)' (Staff Working Document) SWD(2020) 248 final Part 2/2, 158 (Annex 9): "Usually, online platforms are well-placed to proactively reduce the amount of illegal content stored by them. Measures range from various filtering technologies (...)"; Commission, 'Tackling Illegal Content Online. Towards an enhanced responsibility for online platforms'(Communication)' COM (2017) 555 final.

163 Frosio and Geiger (n 48) 40-41.

164 Van Hoboken ea (n 161) 46; Frosio and Geiger (n 48) 41; Keller (n 90) 618.

165 EUIPO, 'Automated Content Recognition: Discussion Paper – Phase 1 'Existing technologies and their impact on IP' (Discussion Paper 2020).

166 See amongst others: EUIPO, 'Automated Content Recognition: Discussion Paper – Phase 1 'Existing technologies and their impact on IP' (Discussion Paper 2020); Commission, 'Impact Assessment Report Annexes accompanying the Proposal for a Regulation on a Single Market for Digital Services (Digital Services Act)' (Staff Working Document) SWD(2020) 248 final Part 2/2 (Annex 11); Gorwa, Binns and Katzenbach (n 161) 3; E Engstrom and N Feamster, 'The Limits of Filtering: A Look at the Functionality & Shortcomings of Content Detection Tools' (Engine 2017) < https://www.engine.is/the-limits-of-filtering > accessed 5 February 2023; EUIPO, 'Automated Content Recognition. Discussion Paper – Phase 2 'IP Enforcement and management use cases' (Discussion Paper 2022) < https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2022_Automated_Content_Recognition_Phase_2_Discussion_Paper/2022_Automated_Content_Recognition_Phase_2_Discussion_Paper_FullR_en.pdf-> accessed 3 February 2023. See further: JP Quintais ea, 'Copyright Content Moderation in the EU: An Interdisciplinary Mapping Analysis' (ReCreating Europe 2022) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4210278 accessed 31 January 2023, 259ff; M Senftleben, 'Institutionalized Algorithmic Enforcement—The Pros And Cons Of The Eu Approach To UGC Platform Liability' (2020) 14 FIU Law Review 299; Engstrom and Feamster (n 166); see also Kulk and Snijders (n 160) 49ff.

167 Commission, 'Impact Assessment Report Annexes accompanying the Proposal for a Regulation on a Single Market for Digital Services (Digital Services Act)' (Staff Working Document) SWD(2020) 248 final Part 2/2 (Annex 11): matching tools (hashing) and classification tools (machine learning); Gorwa, Binns and Katzenbach (n 161) 3: systems that aim to match content and systems that aim to classify or predict content as belonging to one of several categories; EUIPO, 'Automated Content Recognition: Discussion Paper – Phase 1 'Existing technologies and their impact on IP' (Discussion Paper 2020): hashing, watermarking and fingerprinting (matching technologies) and AI-based content recognition (predicting technology).

168 Gorwa, Binns and Katzenbach (n 161) 3.

169 Gorwa, Binns and Katzenbach (n 161) 3. Online content-sharing platforms increasingly use these machine learning algorithms to detect illegal content, such as hate speech: Kulk and Snijders (n 160) 55.

170 Gorwa, Binns and Katzenbach (n 161) 3.

171 Google, 'Hoe werkt Content ID?'(video), <https://support.google.com/youtube/answer/2797370> accessed 5 February 2023.

172 Engstrom and Feamster (n 166) 12-14.

173 Gorwa, Binns and Katzenbach (n 161) 7.

a fingerprint—produced by an algorithm—of a particular characteristic of the content, such as the frequency values of a song.[174] Other uploaded content is submitted to the same algorithm. When the fingerprints match, the content is detected as "infringing".[175] This is a variant of the technique known as *hashing*. An algorithm produces a *hash* on the basis of the characteristics of a digital file.[176] A *hash* (a numeric code) and fingerprints are unique representations of files.[177]

II. Current incapacity according to the state of the art

61 To the current state of art, these technologies are not sufficiently able to distinguish legal content from illegal content.[178] I broadly distil three limitations. First of all, the technologies do not detect illegal content at all times. When a technology uses *hashes* to find *matches*, the *hash* of a piece of content results from algorithmic computation of that piece.[179] When there is a slight difference with regard to the original "illegal" content file, the computation produces a completely different hash; it does not detect the illegality. In relation to hate speech, it has e.g., been found that algorithms can easily be "manipulated" by using wrongly spelled words.[180]

62 A second aspect that makes technologies "imperfect", is that they do not understand *context*. For several types of illegal content, its illegality is *context-dependent*. Even if the technologies are able to adequately identify content that matches with an illegal aspect (e.g., it contains copyright protected aspects or contains the text of a post found to be illegal), they are not sophisticated enough to (at all times) determine its illegality in the specific context.[181] In the context of copyright, the protected material can be used as a quotation or a parody. This would legitimate its use (in line with Article 5 Copyright Directive). For the assessment of hate speech, context is equally essential.

63 Thirdly, these technologies largely depend on reference files.[182] When the quality of the reference files is not assured, e.g., a piece of content initially identified as illegal is not, the use of the technology will not result in the desired detection.[183] The combination of these limitations can be problematic because online content-sharing platforms fear liability when illegal content is not adequately removed. I describe in the next section how this can lead to over-blocking.

III. Risk of over-blocking because of the incentive to block excessively

64 The automated filtering technologies depend on parameters that are designed and determined beforehand by human decision.[184] These parameters influence the scope of the content that is deemed to be illegal. In other words: online content-sharing platforms can design the technologies as they wish. In the area of copyright law, it has repeatedly been found that the fear of liability causes online content-sharing platforms to block excessively.[185] Online

174 Engstrom and Feamster (n 166) 14; EUIPO, 'Automated Content Recognition: Discussion Paper – Phase 1 'Existing technologies and their impact on IP' (Discussion Paper 2020) 15ff.

175 Gorwa, Binns and Katzenbach (n 161); Engstrom and Feamster (n 166) 14.

176 Engstrom and Feamster (n 166) 12.

177 Engstrom and Feamster (n 166) 12-14; EUIPO, 'Automated Content Recognition: Discussion Paper – Phase 1 'Existing technologies and their impact on IP' (Discussion Paper 2020) 7.

178 For more extensive discussion of the technicalities of these technologies and their limitations, for example: Engstrom and Feamster (n 166) 17ff; Gorwa, Binns and Katzenbach (n 161).

179 Engstrom and Feamster (n 166) 18.

180 Kulk and Snijders (n 160) 49; T Gröndahl e.a., All You Need is "Love": Evading Hate Speech Detection (Proceedings of the 11th ACM Workshop on Artificial Intelligence and Security), 2018, arXiv:1808.09115.

181 Engstrom and Feamster (n 166) 18; Gorwa, Binns and Katzenbach (n 161) 8.

182 See on the problem of "less sophisticated notice senders": JM Urban, J Karaganis and BL Schofield, 'Notice and Takedown in Everyday Practice' (UC Berkeley Public Law Research Paper No 2755628) < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2755628> accessed 5 February 2023, 116 (Study 3).

183 Commission, 'Impact Assessment Report Annexes accompanying the Proposal for a Regulation on a Single Market for Digital Services (Digital Services Act)' (Staff Working Document) SWD(2020) 248 final Part 2/2 (Annex 11), 193.

184 See e.g. J-P Mochon ea, 'Content Recognition Tools on Digital Sharing Platforms: proposals for the implementation of article 17 of the EU Copyright Directive' (CSPLA's Mission Report 2020) 24.

185 For empirical evidence of liability risk leading to an

content-sharing platforms aim, in essence, for profit maximization.[186] Therefore, they want to minimize the risk of liability.[187] On the other hand, the revenue of online content-sharing platforms through advertisements increases when more content is uploaded. The online content-sharing platforms thus have to navigate between legal (liability) interests and factual interests.

65 Currently, the legal framework producing the obligations at issue does not create a ground for liability when too much content is blocked but they do when too little content is blocked.[188] In light of the impreciseness of the technologies at the platform's disposal and because more advanced technologies are expensive, it is likely that online platforms wishing to avoid liability design their technologies to block everything that is potentially illegal.[189] The risk of extensive blocking when online content-sharing platforms use automated technologies has been extensively discussed in relation to the Article 17-framework.[190] The extensive blocking in combination with the imprecise technologies creates a risk of over-blocking.[191] Legal content is unjustifiably blocked. The user that uploaded legal content is thus not able to *express* themself and other users are *denied access* to this information. It is this risk that caused Poland to issue an annulment procedure against Article 17.

E. Case C-401/19 Poland v. Parliament and Council

66 Poland claimed before the CJEU that Article 17, and specifically Article 17(4)(b) and (c) should be annulled, because they require OCSSPs *de facto* to use automatic filtering technologies to carry out preventive monitoring of all content, which constitutes an infringement of the right to freedom of expression and information (Article 11 Charter).[192] The CJEU ruled on 26 April 2022 that the liability regime of Article 17 survives, but emphasised the strict application of safeguards to protect users' freedom of expression in the case of filtering obligations.[193]

67 The CJEU's judgment provides general insights for the question what filtering is permissible in the case

incentive to over-block: Urban, Karaginis and Schofield, (n 182) 42-44; S Bar-Ziv and N Elkin-Koren, 'Behind the Scenes of Online Copyright Enforcement: Empirical Evidence on Notice & Takedown, (2018) 50 CONN L REV 339, 377.

186 M Senftleben, 'Bermuda Triangle – Licensing, Filtering and Privileging User-Generated Content Under the New Directive on Copyright in the Digital Single Market' (2019) <https://ssrn.com/abstract=3367219> accessed 5 February 2023, 8; Husovec, '(Ir)Responsible Legislature? Speech Risks under the EU's Rules on Delegated Digital Enforcement' (n 6) 3.

187 Urban, Karaginis and Schofield (n 182) 42-44; Bar-Ziv and Elkin-Koren (n 185) 377.

188 Senftleben in the context of copyright content moderation and Article 17 DSM: Senftleben,'Bermuda Triangle – Licensing, Filtering and Privileging User-Generated Content Under the New Directive on Copyright in the Digital Single Market' (n 186) 8.

189 For the relation between higher liability risks and higher costs for advanced technologies: M Senftleben, 'Bermuda Triangle – Licensing, Filtering and Privileging User-Generated Content Under the New Directive on Copyright in the Digital Single Market' (n 186) 8; Husovec, '(Ir)Responsible Legislature? Speech Risks under the EU's Rules on Delegated Digital Enforcement' (n 6) 3; Kulk and Snijders (n 160) 58. For the risk of over-blocking: Husovec, '(Ir)Responsible Legislature? Speech Risks under the EU's Rules on Delegated Digital Enforcement' (n 6) 3; also acknowledged by the AG in Case C-401/19 *Poland v Parliament and Council* [2022], Opinion of AG Saugmandsgaard Øe, ECLI:EU:C:2021:613, paras 142 and 146; Senftleben, 'Institutionalized Algorithmic Enforcement—The Pros And Cons Of The Eu Approach To Ugc Platform Liability' (n 166) 312. For empirical evidence of liability risk leading to an incentive to over-block: Urban, Karaginis and Schofield (n 182) 42-44; Bar-Ziv and Elkin-Koren (n 185) 377. See for the risk of over-blocking in relation to terrorist content: J Barata, 'Terrorist content online and threats to freedom of expression. From legal restrictions to choreographed content moderation' 14 March 2022, https://verfassungsblog.de/os4-content-threats/ accessed 3 February 2023.

190 See for example: Reda, Selinger and Servatius (n 123) 4 and 13ff.

191 I defined over-blocking in Section A.I. Over-blocking means that not only illegal, but also *legal* content is blocked

192 Case C-401/19 *Poland v Parliament and Council* [2022] ECLI:EU:C:2022:297, paras 23-24.

193 BJ Jütte, 'Poland's challenge to Article 17 CDSM Directive fails before the CJEU, but Member States must implement fundamental rights safeguards' (2022) 17 JIPLP 693; C Geiger and BJ Jütte, 'Constitutional Safeguards in the "Freedom of Expression Triangle" – Online Content Moderation and User Rights after the CJEU's judgment on Article 17 Copyright DSM-Directive' *Kluwer Copyright Blog* 6 June 2022 http://copyrightblog.kluweriplaw.com/2022/06/06/constitutional-safeguards-in-the-freedom-of-expression-triangle-online-content-moderation-and-user-rights-after-the-cjeus-judgement-on-article-17-copyright-dsm-directive/ accessed 5 February 2023; G Frosio, 'Freedom to Share' (2022) 53 IIC 1145.

of obligations to *de facto* carry out a prior review of content to detect specific illegal content.[194] In this section, I describe what the CJEU concluded on the compatibility of these obligations with the users' freedom of expression and the prohibition of a general monitoring obligation. I refer, where relevant, to the discussion in academic literature.

I. A limitation of the right to freedom of expression

68 The CJEU assessed whether the liability framework of Article 17 is compatible with Article 11 Charter. First, the CJEU had to decide whether there is a limitation of users' right to freedom of expression. If so, this limitation can be justified if it is provided for by law, respects the essence of that right and the limitation is proportional given other interests at stake (Article 52(1) Charter).[195] The CJEU importantly decided to review Article 17 in its entirety.[196]

69 As a first point of departure, the CJEU clarified that, following case law of the ECtHR (*Vladimirov Kharitonov v. Russia*), the internet is now a 'principal means' by which individuals express themselves and communicate on the internet.[197] Online content-sharing platforms therefore play an important role in "enhancing the public's access to news and [facilitating] the dissemination of information (...) providing an unprecedented platform for the exercise of freedom of expression and information".[198] As a second point, the CJEU confirmed that the liability regime of Article 17 *de facto* requires these platforms to carry out a prior review of content that users wish to upload. In line with the A-G, the CJEU concluded that to be able to carry out this prior review, according to the current state-of-the-art, online content-sharing platforms need to resort to automatic filtering technologies.[199] These two considerations led the CJEU to conclude that such prior filtering restricts an important means of disseminating online content and therefore constitutes a limitation of Article 11 Charter.[200] The judgment is directed at the EU legislature; the limitation is a direct consequence of the regime laid down by the EU legislature in Article 17 DSM-directive.[201]

70 The CJEU continued to examine whether the limitation is justified. The limitation results from the obligations of Article 17(4)(b) and (c), provisions of an EU act, and is therefore provided for by law.[202] Furthermore, according to the CJEU, the limitation at issue respects the essence of the right to freedom of expression and information.[203] The CJEU considered that Article 17(7) and (9) read together with recitals 66 and 70 DSM-directive constitute an obligation of result to assure that the efforts of the online content-sharing platforms do not result in the unavailability of 'lawful works'.[204] In this way, according to the CJEU, the Directive reflects the CJEU's course (*UPC Telekabel Wien*) that measures adopted by service providers for effective copyright protection should not affect lawfully posted content.[205]

II. Proportionality

71 Most refined is the CJEU's assessment of the proportionality of the filter obligations at hand. Following Article 52(1) Charter, the limitation must

194 JP Quintais ea, 'Copyright Content Moderation in the EU: An Interdisciplinary Mapping Analysis' (ReCreating Europe 2022) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4210278 accessed 31 January 2023, 126.

195 Case C-401/19 *Poland v Parliament and Council* [2022] ECLI:EU:C:2022:297, para 63.

196 Case C-401/19 *Poland v Parliament and Council* [2022] ECLI:EU:C:2022:297, para 21.

197 Case C-401/19 *Poland v Parliament and Council* [2022] ECLI:EU:C:2022:297, para 46.

198 Case C-401/19 *Poland v Parliament and Council* [2022] ECLI:EU:C:2022:297, para 46.

199 Case C-401/19 *Poland v Parliament and Council* [2022] ECLI:EU:C:2022:297, paras 53-54; see Case C-401/19 *Poland v Parliament and Council* [2022], Opinion of AG Saugmandsgaard Øe, ECLI:EU:C:2021:613, paras 57-69.

200 Case C-401/19 *Poland v Parliament and Council* [2022] ECLI:EU:C:2022:297, para 55.

201 Case C-401/19 *Poland v Parliament and Council* [2022] ECLI:EU:C:2022:297, para 56.

202 Case C-401/19 *Poland v Parliament and Council* [2022] ECLI:EU:C:2022:297, para 72 read in conjunction with *Delfi v. Estonia*, App no. 64569/09 (ECtHR, 16 June 2015) paras 121ff.

203 Case C-401/19 *Poland v Parliament and Council* [2022] ECLI:EU:C:2022:297, paras 76ff.

204 Case C-401/19 *Poland v Parliament and Council* [2022] ECLI:EU:C:2022:297, paras 77-80.

205 Case C-401/19 *Poland v Parliament and Council* [2022] ECLI:EU:C:2022:297, para 80; Case C-314/12 *UPC Telekabel Wien* [2014] ECLI:EU:C:2014:192, paras 55-56.

1) protect the rights and freedoms of others[206], 2) be necessary and 3) proportionate.[207] The obligations at issue protect the right to intellectual property (Article 17(2) Charter).[208] Moreover, these obligations are necessary to protect this right, because a less restrictive measure would not be 'as effective'.[209]

72 The question is whether the obligations do not disproportionately restrict the right to freedom of expression of the users. The CJEU believed they are proportionate and gave six requirements for filtering systems.[210] I display the four most relevant arguments for this article here.[211]

73 First of all, the CJEU recognised the need for strict safeguards in the case of automated processing to prevent the risk that exists for the freedom of expression of the users.[212] These strict safeguards exist in the "clear and precise limit" following from Article 17(7) and (9) and recitals 66 and 70. According to the CJEU, this means that measures that *filter and block lawful content when uploading* are excluded.[213] In other words, the CJEU said that imprecise filters cannot be used to comply with the filter obligations.

74 Second, the CJEU considered that the liability regime functions around the condition that the rightsholder provide the platform with "undoubtedly relevant and necessary information" with regard to that content. The need for such substantiated notices protects the interests of users who lawfully use the services, since the platforms will not block when such information is not given.[214]

75 Third, in relation thereto, the CJEU affirmed that the obligation on OCSSPs should not result in a general monitoring obligation (Article 17(8) DSM-directive; Article 15(1) E-Commerce Directive).[215] Interestingly enough, the CJEU defined this as an "additional safeguard" for the observance of the users' freedom of expression.[216] It means, according to the CJEU, that OCSSPs cannot be required to prevent the uploads of content which, in order to be found illegal, would require an "independent assessment of the content" of them. The CJEU referred *in analogy* to *Glawischnig-Piesczek*, thereby suggesting that similar arguments exist in other cases where the prohibition of a general monitoring obligation applies.[217] In paragraph 91, the CJEU clarified that this means that in some cases, illegal content cannot be prevented and can only be taken down after notification by a rightholder. In line with *YouTube and Cyando*, these notifications should enable the platform to judge

206 Or: 'genuinely meet objectives of general interest recognised by the Union' (Article 52(1) Charter), but this is not mentioned by the CJEU, so left outside the scope of this article.

207 P Graig and G de Búrca, *EU Law: Text, Cases, and Materials* (Oxford University Press 2020) 431.

208 Case C-401/19 *Poland v Parliament and Council* [2022] ECLI:EU:C:2022:297, para 82: 'to ensure that intellectual property rights are protected in such a way as to contribute to the achievement of a well-functioning and fair marketplace for copyright (...) copyright protection must necessarily be accompanied to a certain extent, by a limitation on the exercise of the right of users to freedom of expression and information'.

209 Case C-401/19 *Poland v Parliament and Council* [2022] ECLI:EU:C:2022:297, para 83.

210 JP Quintais, 'Between filters and fundamental rights. How the Court of Justice saved Article 17 in C-401/19 – Poland v. Parliament' 16 May 2022, 'https://verfassungsblog.de/filters-poland/' accessed 5 February 2023; M Senftleben, 'The Meaning of "Additional" in the Poland ruling of the Court of Justice: Double Safeguards – Ex Ante Flagging and Ex Post Complaint Systems – are Indispensable' *Kluwer Copyright Blog* 1 June 2022, http://copyrightblog.kluweriplaw.com/2022/06/01/the-meaning-of-additional-in-the-poland-ruling-of-the-court-of-justice-double-safeguards-ex-ante-flagging-and-ex-post-complaint-systems-are-indispensable/ accessed 5 February 2023.

211 The other two arguments concern the specific characteristics of Article 17 DSM-directive as a copyright-provision and are thus (less) relevant outside copyright. The first is given in paragraph 87 and concerns the protection of copyright exceptions and limitations in Article 17(7) DSM-directive. The second is given in paragraph 96 and concerns Article 17(10) that requires the Commission to organise stakeholder dialogues.

212 Case C-401/19 *Poland v Parliament and Council* [2022] ECLI:EU:C:2022:297, para 85; it refers to its own considerations in Case C-311/18 *Facebook Ireland v. Schrems* [2020] ECLI:EU:C:2020:559, para 176, which concerned the right to the protection of personal data.

213 Case C-401/19 *Poland v Parliament and Council* [2022] ECLI:EU:C:2022:297, para 85.

214 Case C-401/19 *Poland v Parliament and Council* [2022] ECLI:EU:C:2022:297, para 89.

215 Case C-401/19 *Poland v Parliament and Council* [2022] ECLI:EU:C:2022:297, para 90.

216 Case C-401/19 *Poland v Parliament and Council* [2022] ECLI:EU:C:2022:297, para 90.

217 Case C-401/19 *Poland v Parliament and Council* [2022] ECLI:EU:C:2022:297, para 90; Case C-18/18 *Glawischnig-Piesczek* [2019] ECLI:EU:C:2019:821, paras 41-46.

that content at issue is illegal "without a detailed legal examination".[218]

76 These considerations show that the CJEU wished to emphasise that lawful content must not be blocked *ex ante*, but the OCSSP cannot be required either to carry out an independent assessment. It seems that the CJEU wanted to clarify that automatic filtering technologies should only be used if there is enough information, e.g., specified in a notice, to specifically target the illegal content and prevent its upload.

77 Fourth, the CJEU's last relevant requirement for a 'proportionate filtering system' are the procedural safeguards contained in Article 17(9). The requirement of an effective and expeditious complaint-and-redress-mechanisms and out-of-court-redress-mechanisms are sufficient to tackle any remaining blocks of legal content (over-blocking).[219] In addition to the *ex ante* safeguards mentioned above, users must thus have the actual ability to fight over-blocking of their content.[220]

F. General take aways for ex ante content moderation obligations outside copyright

78 In this article, I attempt to map the legal implications of the CJEU's ruling in C-401/19 on Article 17 DSM-directive for the more general regime of *de facto* obligations on online content-sharing platforms under EU law to act against illegal content *ex ante*. The CJEU ruled that the *staydown*-obligation in Article 17 respects the freedom of expression, as long as strict safeguards are taken into account. As we have seen, online content-sharing platforms can be under the obligation to *prevent* the upload of certain illegal content outside the area of copyright law. I compare the different obligations in this concluding section. I first construe for which obligations the ruling could be relevant. Second, I address where differences between the specific regime of Article 17 DSM-directive and other obligations to moderate content *ex ante* limit the comparison. I end with an inventory of the general take-aways.

I. Obligation to de facto carry out a prior review of content limits freedom of expression

79 In the C-401/19 judgment, the CJEU confirmed that the Article 17-framework *de facto* obliges online content-sharing platforms to carry out a prior review of user-uploaded content. The rest of its judgment is centred around the compatibility of this obligation with the freedom of expression as laid down in Article 11 of the Charter. That makes the judgment relevant for *de facto* obligations by European and national public institutions for online content-sharing platforms to priorly review content to detect illegal content outside the copyright realm.[221] I elaborated on the existence of these obligations in Section C. These obligations, such as the obligations under the Terrorist Regulation and following from injunctions under the DSA, in line with *Glawischnig-Piesczek*, only take up a small part of the content moderation responsibilities of online content-sharing platforms.[222]

80 As a first point, the CJEU acknowledges that online content-sharing platforms need to use automatic filtering technologies to carry out the required prior review. As a second point, the CJEU acknowledges the importance of the Internet for the exercise of the right of freedom of expression. Prior automatic filtering constitutes a limitation of this right. In Section D, I explained that the use of these technologies is inevitable when these platforms face liability if they do not prevent the upload of certain illegal content. Therefore, the second point holds true for other *de facto* obligations to priorly review content too: the required filtering limits the freedom of expression. The justification of this limitation requires careful examination.[223]

218 Case C-401/19 *Poland v Parliament and Council* [2022] ECLI:EU:C:2022:297, para 91; Joined cases C-682/18 and C-683/18 *YouTube and Cyando* [2021] ECLI:EU:C:2021:503, para 116.

219 JP Quintais, 'Between filters and fundamental rights. How the Court of Justice saved Article 17 in C-401/19 – Poland v. Parliament' 16 May 2022, <https://verfassungsblog.de/filters-poland/> accessed 5 February 2023.

220 M Senftleben, 'The Meaning of "Additional" in the Poland ruling of the Court of Justice: Double Safeguards – Ex Ante Flagging and Ex Post Complaint Systems – are Indispensable' *Kluwer Copyright Blog* 1 June 2022, http://copyrightblog.kluweriplaw.com/2022/06/01/the-meaning-of-additional-in-the-poland-ruling-of-the-court-of-justice-double-safeguards-ex-ante-flagging-and-ex-post-complaint-systems-are-indispensable/ accessed 5 February 2023.

221 Since this article focuses on content moderation by platforms resulting from regulation of platforms the question whether C-401/19 has implications for voluntarily automatic prior filtering by online content-sharing platforms is left outside the scope of this article.

222 See further Section C.III.

223 Case C-401/19 *Poland v Parliament and Council* [2022] ECLI:EU:C:2022:297, paras 60ff; the CJEU demonstrates that

81 The CJEU's ruling is primarily based within the copyright content moderation triangle relationship between platform, rightsholder and user (see Figure 2).[224] But the CJEU confirms that requiring online content-sharing platforms to filter *ex ante* restricts an important means of disseminating content online. Its conclusions should therefore be considered against the background of the content moderation triangle relationship (see Figure 1) between platform, parties with protected interests and user. By protecting such interests through the removal of allegedly illegal content, the platform limits the freedom of expression of the user that uploaded that content. Geiger and Jütte call this the "constitutional dimension" of the CJEU's ruling.[225]

II. No one-to-one comparison

82 The CJEU's demands strict safeguards for the required prior filtering.[226] However, it must be understood that the proportionality assessment of a limitation to a fundamental right predominantly entails assessing whether the infringing act can be balanced in light of the other rights and freedoms it seeks to protect.[227] This limits the extent to which the safeguards described in Case C-401/19 equally apply outside copyright. For the obligation following from Article 17 DSM-directive, the CJEU noted that it seeks to protect intellectual property (Article 17(2) Charter), more specifically copyright.[228] The other discussed obligations do not protect intellectual property. They aim to protect public security (terrorist content) or private life (hate speech). This influences the construction of the proportionality review.

83 Furthermore, the "stay-down"-obligation in Article 17, is up to now, the only obligation known under EU law that requires an *ex ante* review by online content-sharing platforms on the basis of information provided by private parties (rightsholders). The other discussed obligations, such as the ones following from court orders (Article 9 DSA, *Glawischnig-Piesczek*) and those of the Terrorist Regulation (Article 5(2) and (4)), require *ex ante* review on the basis of information about assessed illegal content by a public authority. Consequently, the information on which the platform has to act, and the automatic filtering is based, differs in nature. This presumably influences the proportionality test as well.

III. Take-aways: no general monitoring, no imprecise filters and ex post safeguards

84 In consideration of the nuances made in Section F.II, the relevant conclusions of the CJEU on the justification of prior automated filtering in light of the freedom of expression could be summarized as follows. These could read as a guidance to public authorities (such as the EU legislature or national courts) to formulate the *de facto* obligations to carry out prior review, such as those under the DSA and the Terrorist Regulation, in line with users' freedom of expression.

85 The obligation at issue limiting the freedom of expression must be provided for by law. The act permitting the limitation must itself define the scope of this limitation.[229] The CJEU considered that the limitation at issue respects the essence of the freedom of expression, because the act itself (Article 17(7) and (9)) prescribes that the exercise of the obligation *must be strictly targeted* to illegal

in interpreting the measure or rule at issue, preference should be given to an interpretation in accordance with the Charter: para 70: "(...) in accordance with a general principle of interpretation, an EU measure must be interpreted, as far as possible, in such a way as not to affect its validity (...) preference should be given to the interpretation which renders the provision consistent with primary law (...)".

224 Section B.III.

225 C Geiger and BJ Jütte, 'Constitutional Safeguards in the "Freedom of Expression Triangle" – Online Content Moderation and User Rights after the CJEU's judgment on Article 17 Copyright DSM-Directive' *Kluwer Copyright Blog* 6 June 2022 http://copyrightblog.kluweriplaw.com/2022/06/06/constitutional-safeguards-in-the-freedom-of-expression-triangle-online-content-moderation-and-user-rights-after-the-cjeus-judgement-on-article-17-copyright-dsm-directive/ accessed 5 February 2023.

226 Case C-401/19 *Poland v Parliament and Council* [2022] ECLI:EU:C:2022:297, paras 60ff, and explicitly para 67: '(...) The need for such safeguards is all the greater where the interference stems from an automated process (...)'.

227 As follows from Article 52(1) Charter. See Graig and De Búrca (n 207) 431.

228 Case C-401/19 *Poland v Parliament and Council* [2022] ECLI:EU:C:2022:297, para 82.

229 Article 52(1) Charter. Case C-401/19 *Poland v Parliament and Council* [2022] ECLI:EU:C:2022:297, para 64: the requirement that any limitation (...) must be provided for by law implies that the act (...) must itself define the scope of the limitation (...)". Nevertheless, it may be necessary to leave it to the platforms to decide on the specific measures taken: para 75.

(copyright infringing) content.[230] This implies that *de facto* obligations to carry out a prior review must be strictly confined to not affect lawful content.[231]

86 Unfortunately, as described in Section D, this is hard to achieve. The CJEU probably saw this too and prescribes some safeguards to ensure that the obligation is a proportional limitation of the freedom of expression. The CJEU seems to do a little 'trick' here (and this makes this case so interesting): it places the prohibition of a general monitoring obligation in the key of the proportionality test. That is, online content-sharing platforms cannot be required to prevent the upload from content if that means they would first need to independently assess its illegality (in spirit of *Glawischnig-Piesczek*).[232]

87 As we have seen, the prohibition of a general monitoring obligation remains very much alive. Filtering should thus be targeted. Under Article 17 DSM-directive, this could be achieved through precise information provided by rightsholders. For the other discussed obligations, under the DSA and Terrorist Regulation, the prohibition continues to apply and will require that the order to act contains sufficient information to ensure that certain content is unmistakably illegal.[233]

88 Additionally, the CJEU emphasises, that a platform can only be obliged to filter when the automatic technologies are precise, in the sense that they *do not block* lawful content.[234] The required automatic filtering should be constrained. Still, due to the impreciseness of the technologies, the CJEU considers it relevant to emphasise the need to have effective *ex post* safeguards as complaint and redress mechanisms.[235]

89 These considerations demonstrate that obliging platforms to carry out a prior review which requires them to use automatic filtering technologies should be carefully targeted. Platforms should only be required to use automatic technologies for very specific and clear-cut cases. Nevertheless, it is good to remember that the need to protect certain public interests, such as protecting the public against terrorism, might permit broader filtering. The proportionality test might balance out that way. However, the CJEU in C-401/19 has manifested that the filtering must be surrounded with "effective and expeditious" *ex post* mechanisms.

G. Concluding remarks

90 This article has shown that the fundamental importance of the freedom of expression and information of the users of the internet needs to be taken seriously when addressing illegal content online both inside and outside the area of copyright law. In C-401/19 the CJEU gives an insight into what that actually means for *ex ante* content moderations obligations on online content-sharing platforms. Requiring online content-sharing platforms to prevent the uploads of certain illegal content *de facto* requires them to use automatic filtering technologies. The CJEU treats the prohibition of a general monitoring obligation as a safeguard to the freedom of expression. Consequently, online content-sharing platforms should only block content that is clearly illegal. Automatic filtering technologies should be limited to this content too. For authorities establishing *de facto* obligations to carry out a prior review under the DSA and Terrorist Regulation, as discussed in this article, Case C-401/19 shows the need to take the freedom of expression of internet users into consideration and provides starting points for this strictly targeted task. Consequently, Case C-401/19 can have implications outside the area of copyright when used to assess whether the legal frameworks of the DSA and the Terrorist regulation could survive the CJEU's test.

230 Case C-401/19 *Poland v Parliament and Council* [2022] ECLI:EU:C:2022:297, paras 77ff: "(...) shall not result in the prevention of the availability of works or other subject matter uploaded by users, which do not infringe copyright (...)". It prescribes a "specific result to be achieved".

231 In line with Case C-314/12 *UPC Telekabel Wien* [2014] EU:C:2014:192 paras 55-56.

232 Case C-401/19 *Poland v Parliament and Council* [2022] ECLI:EU:C:2022:297, para 90.

233 In the literature, some authors have argued in favour of limiting filtering to 'manifestly infringing content', but the CJEU does not use these words. See e.g. C Geiger and BJ Jütte, 'Constitutional Safeguards in the "Freedom of Expression Triangle" – Online Content Moderation and User Rights after the CJEU's judgment on Article 17 Copyright DSM-Directive' *Kluwer Copyright Blog* 6 June 2022 http://copyrightblog.kluweriplaw.com/2022/06/06/constitutional-safeguards-in-the-freedom-of-expression-triangle-online-content-moderation-and-user-rights-after-the-cjeus-judgement-on-article-17-copyright-dsm-directive/ accessed 5 February 2023.

234 Case C-401/19 *Poland v Parliament and Council* [2022] ECLI:EU:C:2022:297, para 85.

235 Case C-401/19 *Poland v Parliament and Council* [2022] ECLI:EU:C:2022:297, paras 91-94.

Copyright Protection of Broadcasts in Australia

The intersections between originality, economic investment, and social-oriented perspectives

by **Kanchana Kariyawasam and Anubhav Dutt Tiwari***

Abstract: This article examines the copyright protection of broadcasts in Australia. It investigates the difference in the legal treatment of creative subject matter, in the form of original literary, dramatic, musical, and artistic works, versus productive subject matter, in the form of broadcasts. The analysis focuses on the social-oriented perspective of granting copyright protection to broadcasters, separately from that afforded to creators of original works. This paper also emphasises the social-oriented rationale for the protection of broadcasters' rights under copyright law in Australia; that is, the wider interests of the public to access original content and information through broadcasts. Finally, this paper argues that copyright law in Australia needs to protect the interests of original creators and broadcasters, while enabling the wider public to access original content and excluding others from unauthorised use of their respective contributions.

Keywords: Copyright; Broadcasters' Rights; Social-oriented rationale; Australia

Recommended citation: Kanchana Kariyawasam and Anubhav Dutt Tiwari, Copyright Protection of Broadcasts in Australia: The intersections between originality, economic investment, and social-oriented perspectives, 14 (2023) JIPITEC 148 para 1.

A. Introduction

1 Copyright was envisioned to protect the original and creative endeavours of human authorship, and to prevent others from reproducing or communicating such works without permission. To achieve this end, "a balance was conceived between exclusive control and freedom to enable future creativity".[1] In this context, a *creation* is understood as either a tangible or non-tangible embodiment of subject matter in the literary and artistic domains, which is the result of significant intellectual effort by the person who undertakes its *creation*.[2] Generally, the creator/author of a literary, dramatic, musical, or artistic work is the owner of any copyright subsisting in the work. Over time, however, copyright protection has also been granted to subject matter other than literary, dramatic, musical, or artistic works. For instance, a *production* is defined as either a tangible or non-tangible embodiment, other than a creation of subject matter in the literary and artistic domains, which is the result of time, effort, and resources by

* Kanchana Kariyawasam, Associate Professor, Griffith Business School, Griffith University, Queensland, Australia. PhD (Griffith University, Australia), LLM (Advanced) (University of Queensland, Australia) and LLB (Hons) (University of Colombo, Sri Lanka). I would like to thank Law Futures at Griffith University for supporting this research and Anubhav Dutt Tiwari, PhD Candidate, Faculty of Law, Monash University, Victoria, Australia. LLM (University of Essex, UK) and BA LLB (Hons) (National University of Juridical Sciences, India).

1 Christophe Geiger, 'Freedom of Artistic Creativity and Copyright Law: A Compatible Combination?' (2018) 8 UC Irvine Law Review 413.

2 Andrew Christie, 'Simplifying Australian Copyright Law - the Why and the How' (2000) 11 Australian Intellectual Property Journal 40, 45-47.

the person who undertakes its *production*.[3] Hence, the owner of the copyright in sound recordings, films, and broadcasts will generally be the maker, producer, or broadcaster. The focus of this article is specifically on 'broadcasts' as the subject matter of copyright where, similarly to a production, but specifically because of the huge institutional resources required, protection is afforded as an incentive to broadcasting organisations.

2 Unlike authors' rights, which reward authors for their creative effort by protecting their rights under the copyright law, the protection afforded to broadcasters safeguards the results of corporations' pure investments and entrepreneurial efforts to communicate such creative works to the public. Broadcasters produce and transmit audio or video content for the benefit of the general public, which requires major financial, technical and organisational investment in infrastructure and logistics so that the public can receive programs via a "signal" or "transmission".[4] The protection of broadcasting organisations, therefore, is not based on the creativity involved in creating such works, but on the utilitarian and economic justifications in communicating these works to the public.[5] Here, the utilitarian or social-oriented perspective is introduced as a rationale for copyright protection, which focuses on the interests of the public and society, and also embraces the technological strides in the dissemination of information and content to society.[6]

3 Consequent to the utilitarian rationale, the neighbouring right (rights neighbouring to copyright for authors) was conceptualised especially for people or entities who are not technically authors: performing artists, producers of phonograms, and *those involved in radio and television broadcasting*. Typically, it offered broadcasters derivative rights: existing authorial works are used or developed; the subject matter protected by such right is the product of technical and organisational skill, rather than authorial skill; and the rights are initially given to the body or person financially and organisationally responsible for the material's production and dissemination, rather than the human creator.[7] Hence, the economic rationale for granting neighbouring rights to broadcasters is to protect the substantial investments made by broadcasting organisations for the provision of program content and the transmission of that content *to the public*, especially by limiting the ability of third parties to exploit the products of such investments.[8]

4 According to the World Intellectual Property Organisation (WIPO), "the neighbouring right for broadcasters thus mainly exists to protect the broadcasting organisations' entrepreneurial effort and investment which materialize in the form of their broadcasts (or related online signals) as an end product".[9] The emphasis on the protection of broadcasting organisations also stems from its economic contribution which is more than twice that of the music sector and more than three times that of the film industry.[10] Similarly, the former Director-General of the European Broadcasting Union (EBU) argued that:

> (b)roadcasters pay billions of euros to produce or acquire and distribute the content of the highest technical quality and have paid tens of billions more to convert analog transmission systems to digital systems. Without appropriate protection of the broadcasting signal, the returns on this significant investment are under threat.[11]

5 Essentially, the EBU's argument states that broadcasters engage in planning, producing, acquiring, scheduling, and transmitting programs for the public benefit and these acts come at a significant cost and demand the broadcasters' financial, technical,

3 Ibid.

4 European Broadcasting Union, 'Legal and Policy Focus Broadcasters' Rights: Towards a New WIPO Treaty' [2021] 11 <https://www.ebu.ch/files/live/sites/ebu/files/Publications/strategic/open/legal--policy-focus-broadcasters-right-wipo-treaty.pdf > accessed 9 May 2022.

5 Mani Sakthivel, *Broadcasters' Rights in the Digital Era: Copyright Concerns on Live Streaming* (Brill 2020) 97.

6 See Gillian Davies *Copyright and the Public Interest* (2nd edn., Sweet & Maxwell 2002).

7 See Lionel Bently and Brad Sherman, *Intellectual Property Law* (4th edn, OUP 2014) 33. See also George H. C. Bodenhausen, 'Protection of 'Neighbouring Rights'' (Spring 1954) 19 Law and Contemporary Problems 156.

8 Sam Ricketson & Jane Ginsburg, *International Copyright and Neighbouring Rights* (2nd edn, Vol.II, OUP 2006) 1207. See also Stephen Stewart, *International Copyright and Neighbouring Rights* (Butterworths 1989) 190-191;

9 European Broadcasting Union, 'Legal and Policy Focus Broadcasters' Rights: Towards a New WIPO Treaty' [2021] 11 <https://www.ebu.ch/files/live/sites/ebu/files/Publications/strategic/open/legal--policy-focus-broadcasters-right-wipo-treaty.pdf > accessed 9 May 2022.

10 Ibid.

11 WIPO Magazine, 'Protecting Broadcasters in the Digital Era' [2013]. <https://www.wipo.int/wipo_magazine/en/2013/02/article_0001.html> accessed 7 May 2022.

and organisational investment.[12] The protection of the broadcast signal is thus based on the technical and organisational efforts made by the broadcaster for transmission purposes and on restricting third parties from benefiting from the broadcasters' investments.[13]

6 It is in this background that this article attempts to highlight a key intersection between broadcasters' rights under copyright law in Australia, the author's copyright in their original works that are broadcasted, as well as the social-oriented rights of the public in accessing such works through broadcasts. The article argues that in introducing a new aspect of copyright protection that sources its rationale on the public interest rather than originality, there has been a consequent fragmentation of copyright law. This inherent fragmentation requires a closer analysis and engagement from the lens of the interests of the various stakeholders—the broadcasters, the wider public and original creator (wherever applicable)—while at the same time anticipating conflict between the interests of such stakeholders.

7 This article is henceforth divided into three sections. Section 1 provides the historical background on the journey of *broadcasts,* from radio broadcasts to television and now digital broadcasts. Section 2 focuses on copyright law in Australia, particularly dealing with the copyright protection of broadcasters, to emphasise the foundational understandings of the protection afforded therein and the dichotomy with the *originality* requirement for authors. This section also sheds light on the judicial conception of broadcasters' rights in Australia which underlines such fragmentary nature of protection. Section 3 focuses on the public interest argument emphasising the evolving complexities that must be continually assessed. Finally, the article concludes that the cooperative underlying scheme among authors' and broadcasters' rights, as well as the social-oriented rights of the public to access works through broadcasts, need to be continually assessed and balanced in law, legal judgments, and policy decisions, particularly in light of technological advancements.

B. Background and Development of Broadcasts: The Journey from Radio, to Television and Digital Broadcasts

8 Before diving into the issues emerging from copyright protection of broadcasters, a brief discussion on the concept of a "broadcast", and its historical evolution, is relevant. In the *Cambridge Dictionary*, the broadcast has multiple definitions, including (a) "to send out a programme on television or radio", and/or (b) "to spread information to a lot of people", and/or (c) "to send out sounds or pictures that are carried over distances using radio waves".[14] Broadcasting is recognised as being a "key sector in modern society, not only economically but, more than most industries, culturally, socially and politically";[15] it is "the quintessential electronic mass medium".[16] As Glenn Withers identifies, "it is also a sector that is more than most linked to the digital revolution in technology at the core of the new global knowledge economy".[17] Broadcasting is also recognised as being "arguably the most influential and powerful industry operating today. The media impose an inescapable presence in contemporary life and infuse all areas of public communication".[18] Evidently, broadcasting encapsulates a number of services, at the heart of which lies the provision or delivery of sound and/or pictures to a viewer or listener.

9 Regarding the history of broadcasts, radio is the earliest mass broadcasting technology, with telegraphy and telephony appropriately being called the two "older sisters" of radio technology. Telegraphy involves sending coded electronic impulses over distance, whereas telephony involves sound transmissions. While these two technologies are point-

12 European Broadcasting Union, 'Legal and Policy Focus Broadcasters' Rights: Towards a New WIPO Treaty' [2021] 6 <https://www.ebu.ch/files/live/sites/ebu/files/Publications/strategic/open/legal--policy-focus-broadcasters-right-wipo-treaty.pdf > accessed 9 May 2022.

13 IRIS plus, 'New Services and Protection of Broadcasters in Copyright Law' (2010-5) 8 <https://rm.coe.int/1680783bb8> accessed 10 May 2022.

14 Cambridge Dictionary, 'Broadcast' (Cambridge 2020) <https://dictionary.cambridge.org/dictionary/English/broadcast> accessed 8 May 2022.

15 Glenn Withers, 'Economics and Regulation of Broadcasting' (2002) 93 Discussion Paper 2 <https://openresearch-repository.anu.edu.au/bitstream/1885/41411/3/No93Withers.pdf> accessed 9 May 2022.

16 James F. Hamilton, 'Excavating Concepts of Broadcasting: Developing a method of cultural research using digitized historical periodicals' (2018) 6 Digital Journalism 1136, 1138.

17 Glenn Withers, 'Economics and Regulation of Broadcasting' (2002) 93 Discussion Paper 2 < https://openresearch-repository.anu.edu.au/bitstream/1885/41411/3/No93Withers.pdf > accessed 9 May 2022.

18 Paolo Baldi & Uwe Hasebrink, *Broadcasters and Citizens in Europe: Trends in Media Accountability and Viewer Participation* (Intellect 2007) 117.

to-point transmissions, from a sender to a receiver, radio technology entails "broadcast transmissions, which take place between a sender and an indefinite number of receivers".[19] The receivers are invariably the general public, or a particular group within the public. Although the history of radio technology might seem primitive to those living in an era of high speed-internet, smartphones and 5G, at the time, these developments were nothing short of magic.

10 Further, the technological developments in broadcasting have been the brainchild of numerous outstanding inventors worldwide. Broadcasting gained prominence at the end of the 1890s when Guglielmo Marconi initiated the world's first commercial radio service. After the technology was developed to move images as well as sounds, the concept of broadcasting was further expanded. With the end of the First World War came what Andrew Crisell refers to as the "golden age of radio" and the "rise of television".[20] This latter improvement allowed listeners to see what they were hearing. In 1926, at Selfridge's department store in London, British inventor John Logie Baird held world's first public demonstration of a television system, using mechanical rotating discs to scan moving images into electrical impulses.[21] The prelude to television broadcasting began as early as 1928, when Charles Jenkins broadcasted silhouetted images under the name of "W3XK", which was an experimental television station in Washington, DC, in the United States of America (USA).[22] In 1939, while transmitting the inaugural telecast of the opening ceremonies at the New York "World's Fair", the USA's National Broadcasting Company became the first network to introduce regular television broadcasts.[23] Thus, the world entered an era of television broadcasting which took off in parallel to radio broadcasting. The global TV and radio broadcasting market was expected to grow from US$317.05 billion in 2020 to US$347.81 billion in 2021 at a compound annual growth rate of 9.7%.[24]

11 Digital television is nothing less than a revolutionary new way to broadcast television content, replacing the National Television System Committee of USA analogue standard that had been in place since 1953.[25] With the advent of the internet, most broadcasting methods instigated digital broadcasting networks, which offer channels for distributing digital content. The digital era has given viewers control over where and how they watch content, and has made it difficult to overestimate the effects of these changes in television distribution on the diverse kinds of content, production, and viewer strategies.[26] For broadcasters, the increasing prevalence of digital technologies comes with a drawback— the option available to viewers to watch a rebroadcast, i.e., a simultaneous or subsequent broadcast of an initial broadcast, thus, leading to the increased ease of obtaining unauthorised access to copyrighted content.[27] Nevertheless, the journey from radio to television and now, digital broadcasting, shows the continuing technological strides in communicating sounds and pictures to the public *en masse.*

12 From the standpoint of legal and policy matters, a continuing focus on the ongoing evolution of the broadcasting industry is important because communication to the public entails standards and regulations, while balancing the interests of broadcasters and the authors of the works being broadcasted. It is also relevant from the perspective of understanding the manner of regulating the broadcasting industry in the interests of society, particularly in the present digital age, while anticipating further technological strides in the years to come. It is, therefore, crucial to engage with the underlying reason for which broadcasting has been encouraged until now; that is, the delivery of content and information to the wider public in the

19 Andrew Crisell, *An Introductory History of British Broadcasting* (2nd edn, Routledge 2002) 14.

20 *Ibid.*

21 Evolution of Television <https://opentext.wsu.edu/com101/chapter/9-1-the-evolution-of-television/> accessed 7 May 2022.

22 Broadcasting: The History Of Radio, The History Of Television, The Future Of Radio And Television, Cable Television <https://law.jrank.org/pages/4884/Broadcasting.html#ixzz6ZmaknDK4> accessed 5 May 2022.

23 Ibid.

24 GlobeNewswire, "Worldwide TV and Radio Broadcasting Industry to 2030 - Featuring Comcast, DISH Network and Viacom Among Others" at <https://www.globenewswire.com/news-release/2021/08/11/2278613/28124/en/Worldwide-TV-and-Radio-Broadcasting-Industry-to-2030-Featuring-Comcast-DISH-Network-and-Viacom-Among-Others.html> accessed 14 May 2022.

25 Television Broadcasting, History Of <https://www.encyclopedia.com/media/encyclopedias-almanacs-transcripts-and-maps/television-broadcasting-history> accessed 8 May 2022.

26 Laura Osur, 'Netflix and the Development of the Internet Television Network' 10 (Thesis, Syracuse University 2016) <https://surface.syr.edu/cgi/viewcontent.cgi?article=1448&context=etd> accessed 9 May 2022.

27 See WIPO, 'Draft Report of the Standing Committee on Copyright and Related Rights', (Thirtieth Session, 2015) <https://www.wipo.int/edocs/mdocs/copyright/en/sccr_30/sccr_30_6.pdf> accessed 8 May 2022.

larger interests of society, or its key social-oriented purpose and rationale.

C. Broadcasting rights under Australian copyright law

13 In Australia, Part III of the *Copyright Act 1968 (Cth)* provides copyright protection for works—original literary, dramatic, musical and artistic works—, while Part IV grants exclusive rights over subject matter other than such works, including sound recordings, cinematograph works, *broadcasts,* and published editions. In assessing the rationale behind the protection of broadcasters' rights under the *Copyright Act*, especially the separate neighbouring rights accorded to broadcasting organisations, it is necessary to begin with an analysis of the Spicer Committee Report.[28]

I. Protecting the 'other' subject matter – broadcasts: Early discussions under the Spicer Committee and the Gregory Committee

14 The Spicer Committee was formed to review the Australian copyright law in 1958. It observed that as a Dominion of Britain, the applicable law on copyright had followed the British law on copyright. An anomaly emerged, however, when the *Copyright Act of 1911 (UK)* was repealed by the *Copyright Act of 1956 (UK).* The 1956 Act included a provision that allowed for certain provisions of the 1911 Act to be applied in countries other than the UK. Thus, the need for a review of the Australian copyright law emerged, and relatedly, the need for a separate law.[29] The Spicer Committee was thus formed to recommend the features of the new copyright law in Australia. Effectively, it analysed the transition between the *Copyright Act 1911 (UK),* and the *Copyright Act of 1956 (UK)*; and in doing so, based its reasoning on the observations of a similar committee formed to provide recommendations culminating in the *Copyright Act of 1956 (UK)*—the Gregory Committee.[30]

15 The Spicer Committee identified its objective as to "balance the interests of the copyright owner with those of copyright users and the general public".[31] It recognised that the *Copyright Act of 1956 (UK)* had introduced new copyright subject matters including in the form of television broadcasts and sound broadcasts made by the British Broadcasting Corporation and the Independent Television Authority.[32] From an Australian perspective, the Spicer Committee also recognised the importance of granting similar protection to broadcasters. However, there were at least two critical issues before the Spicer Committee with respect to broadcasts. First, how must *broadcasts* be understood, particularly as a separate subject of protection from creative works? Second, should broadcasts be provided protection specifically under the new Australian copyright law, and why? At the outset, the Committee recognised that, in relation to broadcasts, a qualified person could only be a body corporate.[33] It also recommended that the broadcasters must be under legislative authority to function as such. This essentially means that while individuals can be original authors, they cannot become 'broadcasters'. Unlike broadcasters, however, they are not subject to legislative regulations to function as authors, artists, musicians, etc.

16 Another important observation of the Spicer Committee was that it regarded broadcasts as a modern iteration of public performances or recitations. According to it, "(r)eproductions of performances by artists and others are often made by broadcasters for the purposes of subsequent broadcasting".[34] Therefore, the Committee understood broadcasts as being *reproductions* of creative works, which is an important distinction when it relates to creative works per se. Further, it was "the reproduction or dissemination to the public" that was to be the subject of separate protection, as was recommended by the Gregory Committee, and eventually found a place in the *Copyright Act of 1956 (UK).*[35] The Spicer Committee agreed with the Gregory Committee, recognising that "in a country such as Australia, with its different time zones and a limited number of co-axial cables, we think that this practice (reproduction) is necessary and

28 Copyright Law Review Committee, *Report to Consider what Alterations are Desirable in the Copyright Law of the Commonwealth* (1959).

29 Ibid 9-10.

30 Board of Trade, *Report of the Copyright Committee* (Cmd 8662, 1952) 41-2 (Gregory Committee).

31 Copyright Law Review Committee, *Report to Consider what Alterations are Desirable in the Copyright Law of the Commonwealth* (1959) 8.

32 Ibid 54.

33 Ibid 16.

34 Ibid 26.

35 Ibid.

desirable".[36] A significant aspect here is that the Spicer Committee recognised that the protection of copyright in broadcasts was important from a public interest perspective, and even envisaged the State's role in authorising or licensing broadcasting organisations.

II. The protection of broadcasts as distinct from the protection of original works

17 Eventually, the *Copyright Act* incorporated the Spicer Committee's recommendations and included "broadcasts" as a separate subject matter for protection. Under various provisions, the *Copyright Act* makes a clear distinction between the creator of a work, such as a sound recording or cinematographic film, and the broadcaster of such creations. For example, it provides protection for broadcasting organisations while defining a "broadcast" as "a communication to the public delivered by a broadcasting service within the meaning of the Broadcasting Services Act".[37] It also recognises copyright in "television broadcasts" and "sound broadcasts".[38] "Television broadcast" has been defined as "visual images broadcast by way of television, together with any sounds broadcast for the reception along with those images".[39] Sound broadcasts, conversely, refer to the broadcasting of sounds that are not part of television broadcasts.[40] Thus, reading these definitional provisions together, it can be inferred that "broadcasts" for the purposes of Australia's copyright law means the *communication to the public* in the form of visual images and sounds, and it is this *communication* that is envisaged as *broadcasting* and afforded protection. An extension of the discussion leads to the observation that "broadcasts" also refer to the dissemination to the public of *aggregates* of visual images and sounds, in the form of a cinematograph film or sound recording.[41]

18 With respect to the rights flowing from such copyright protection, the copyright that subsists in broadcasts is as follows: for images broadcast on television, the exclusive right "to make a cinematograph film of the broadcast, or a copy of such a film";[42] for a sound broadcast and the sound of a television broadcast, the exclusive right "to make a sound recording of the broadcast or a copy of such a sound recording";[43] and for a television broadcast or sound broadcast, the exclusive right "to re-broadcast it".[44] On the contrary, copyright in cinematograph films, for instance, grants exclusive rights to the creator to make copies of the film, to afford the film to be seen and heard in public, and *communicate the film to the public*.[45] Thus, a pertinent difference emerges here—as a creator of a cinematograph film it is not incumbent to exercise the exclusive right to communicate the film to the public. As a broadcaster, however, the broadcast or communication to the public is inherent to the copyright coming into existence. In other words, for broadcasters communicating to the public is not merely an exclusive right emanating from the broadcast, it is an essential *prerequisite* to the existence of copyright protection that grants exclusive rights.

19 In addition, an infringement in relation to a television or sound broadcast may occur when a copy of a cinematograph film of the broadcast or a record embodying a sound recording of the broadcast is produced.[46] Whereas, in relation to the film or recording itself, the infringement may occur simply when these are copied or recorded.[47] Finally, even when broadcasts are assessed from the perspective of the copyright owner, the *maker of the broadcasts* (broadcast of the cinematograph film, for instance) is regarded as the owner of the copyright;[48] whereas, in relation to a cinematograph film itself, the *maker of the film* owns the copyright.[49] Sections 22 (3) (b), 22 (4) (b), and 22 (5) of the *Copyright Act* define how the "maker" is identified in terms of sound recordings, cinematographic films, broadcasts, and other communications, respectively. In relation to a

36 Ibid.

37 Copyright Act 1968 (Cth) s 10.

38 Copyright Act 1968 (Cth) s 87.

39 Copyright Act 1968 (Cth) s 10.

40 Ibid.

41 Refer to the definitions of a 'cinematograph film' and a 'sound recording' under Copyright Act 1968 (Cth) s 10 (1).

42 Copyright Act 1968 (Cth) s 87(a).

43 Copyright Act 1968 (Cth) s 87(b).

44 Copyright Act 1968 (Cth) s 87(c).

45 Copyright Act 1968 (Cth) s 86.

46 Copyright Act 1968 (Cth) s10(1).

47 Ibid.

48 Copyright Act 1968 (Cth) s 99.

49 Copyright Act 1968 (Cth) s 98(2).

sound recording or cinematograph film, reference is made to the "maker", who must be a qualified person at the time the recording or film is made.[50]

20 From a theoretical perspective, the difference emanating from the above provisions lies between a natural law theory providing inherent rights to creators vis-à-vis a utilitarian justification, which protects broadcasting organisations that function to disseminate creative original works to the wider public.[51] Copyright protects all creations of the human mind and intellect, whatever their form or merit and regardless of the audience for which they are destined.[52] Copyright law has traditionally been the primary source of legal protection for original works, based on the requirement of originality.[53] The notion of originality is a requirement for copyright protection but does not extend to broadcast signals and transmissions. This is because broadcasters do not necessarily produce original works but distribute the information embodied in the created works.[54] Broadcasters, such as producers, serve a strictly technical role in copyright exploitation and do not necessarily add value in any artistic or creative capacity.[55] This lack of qualifying criteria relates to the fact that broadcasting is primarily a technical rather than creative or innovative act;[56] and hence, entrepreneurial rights have no requirement for originality. It is argued that:

> while this notion of 'originality as a fundamental aspect of eligibility criteria' is central to general copyright law, it appears not to extend to broadcast signals as unique subject matter. This is because.... Broadcasting organisations enjoy protection of their broadcasts by virtue of the mere technical act of transmission, without any application of de facto eligibility criteria. The result is therefore that there is no form of filter akin to an originality threshold or idea-expression dichotomy that prevents some broadcasts from being protected pursuant to balancing the goals of the intellectual property system. As such, it appears that broadcasters' rights hold a very unique place in the overall intellectual property landscape, as it is perhaps the only form of right in which there is no explicit and coherent application of the doctrine of functionality.[57]

21 The unique place enjoyed by broadcasters thus emerges from the social-oriented rationale that has often been referred to as the incentive theory. Proponents of the incentive theory aim "to encourage creative activities and by doing so, to disseminate cultural and economic benefit to the general public other than creators".[58] The emphasis is thus on the public or society, in conjunction with the protection afforded to creators or authors—while recognising the entrepreneurial and resource contribution involved in broadcasting.

22 In furtherance of this point, the regulatory scheme on broadcasting in Australia itself points to the importance of dissemination to the public of creative works and information in various visual and sound forms. Earlier, it was noted that the definition under the *Copyright Act* directs to that of a "broadcasting service" under the *Broadcasting Services Act 1992* (Cth) (Broadcasting Act).[59] According to the Broadcasting Act, "broadcasting service" refers to "a service that delivers television programs

50 Copyright Act 1968 (Cth) s 89(1) (sound recordings) and s 90(1) (cinematograph films). 'Maker' is defined in relation to cinematograph films only, as the director, producer, and screenwriter of the film: Copyright Act 1968 (Cth) s 10(1).

51 Gillian Davies, *Copyright and the Public Interest* (2nd edn, Sweet & Maxwell 2002) Chap 1.

52 European Space Agency, 'About copyright and neighbouring rights' <https://www.esa.int/About_Us/Law_at_ESA/Intellectual_Property_Rights/About_copyright_and_neighbouring_rights> accessed 9 May 2022.

53 Peter S Menell, 'An Analysis of the Scope of Copyright Protection for Application Programs' (1989) 45 Stanford Law Review 1045, 1046.

54 See WIPO, "Study on the Social and Economic Effects of the Proposed Treaty on the Protection of Broadcasting Organizations' (2010) at <https://www.wipo.int/edocs/mdocs/copyright/en/sccr_21/sccr_21_2.pdf> accessed 12 May 2022.

55 Bryan Kareem Khan, 'An Economic Analysis of the Intellectual Property Rights of Broadcasting Organisations' (Thesis, Erasmus University 2019) 75 <http://amsdottorato.unibo.it/8781/1/Khan_Bryan_tesi.pdf> accessed 8 May 2022.

56 Ibid 80.

57 Ibid. See also, Anne, Fitzgerald and Tim, Seidenspinner, '*Copyright and Computer Generated Materials* - Is it *Time to Reboot the Discussion About Authorship*?' (2013) 3 Victoria University Law and Justice Journal 47, 50.

58 Megumi Ogawa, *Protection of Broadcasters' Rights* (Martinus Nijhoff Publishers 2006) 5.

59 It is important to note that the law on broadcasters and their rights is found in various legal regimes. According to Megumi Ogawa, broadcasters' rights are commonly under the telecommunications law, broadcasting law and intellectual property rights law, specifically, the copyright law. However, it may also be found in other regimes such as competition law, contract law, etc. This is also an instance of legal fragmentation though not the subject of this article. Megumi Ogawa, *Protection of Broadcasters' Rights* (Martinus Nijhoff Publishers 2006) Chap 2.

or radio programs to persons having equipment appropriate for receiving that service, whether the delivery uses the radiofrequency spectrum, cable, optical fibre, satellite or any other means or a combination of those means".[60] The Broadcasting Act also recognises various categories of broadcasters that signify the scale of resources associated with broadcasting.[61] Moreover, the Broadcasting Act provides for the distribution of broadcasting bands as well as licensing that form the basis of the regulatory scheme applicable to broadcasting in Australia.[62] Thus, the legal landscape recognises that broadcasting involves the delivery of content through a resourceful structure and an elaborate technological system established and facilitated by broadcasters.

III. The judicial perspective on the fragmentary scheme of copyright law vis-à-vis broadcasts and original works

23 *TCN Channel Nine Pty Ltd v Network Ten Pty Ltd* [63] (Panel case) is the first Australian case on the issue of infringement of copyright in broadcasts. The respondent, Network Ten, a commercial broadcasting organisation in Australia, aired program excerpts from the applicant, TCN Channel Nine, another commercial broadcasting station. The excerpts were made up of twenty segments ranging in length from eight seconds to forty-two seconds from sixteen different programs. The applicant had not given the respondent permission to do so. The applicant filed a claim against the respondent in the Federal Court of Australia, alleging that taping segments of the applicant's programs and broadcasting excerpts of the applicant's programs constituted an infringement of copyright in broadcasts owned by the applicant in violation of sections 87(a) and 87(c) of the *Copyright Act*. The respondent denied any infringement of copyright.

24 The Panel Case resolved for the first time the issue of the definition of a television broadcast with respect to copyright law in Australia. Among other things, the Panel Case considered the issue of *originality*. The Court discussed the differences between protections under Part III of the *Copyright Act* which covers "works" and Part IV of the same which covers "subject matter other than works" in examining whether the principles which apply to the former also apply to the latter. According to the primary judge, Justice Conti, there is "considerable conceptual difficulty" in such application.[64] Instead, he determined that the case of *Nationwide New Pty Lid v Copyright Agency Ltd* [65], which dealt with a published edition, was of assistance to determine the principles that apply to television broadcasts because both a published edition and a television broadcast are copyright materials in which the "originality of expression is not involved in the establishment of copyright so protected".[66] The Court noted that "television broadcast copyright is attributable not to originality, as in the case with Part III works, *but to technical considerations associated with the infrastructure of production. Nevertheless, technical considerations involve notions of quality....*" (author's emphasis).[67]

25 The primary judge referred to the historical background of broadcasts to justify the position that a television broadcast was comprised of several images, which together constituted a "program". In so doing, there is a reference to why copyright protection should be granted to broadcasters, and it is clear that *this is not due to originality*. The focus here is on protecting the broadcasts against piracy, because of the "considerable cost and skill involved".[68] Hely J in the Federal Court, expressly finds that "the requirement of originality which is imposed by s 32 of the *Copyright Act 1968* in the case of works does not apply in relation to a television broadcast".[69] Callinan J, was more emphatic in his position that there was "blatant commercial exploitation"[70] by Network Ten. In siding with the Federal Court's broad interpretation of a television broadcast, he admitted that such construction would confer higher-level protection for copyright in such subject matter but did not oppose such higher protection. To buttress his point, he elaborated on the nature of the interests that broadcasts seek to protect:

60 The Broadcasting Services Act 1992 (Cth), s 6(1).

61 The Broadcasting Services Act 1992 (Cth), s 11.

62 See, for instance, the Broadcasting Services Act 1992 (Cth), Parts 3-5.

63 (2001) 108 FCR 235.

64 Ibid 12.

65 *Nationwide News Pty Ltd v Copyright Agency Ltd* (1996) 34 IPR 53.

66 (2001) 108 FCR 235, 15.

67 Ibid 44.

68 Board of Trade, *Report of the Copyright Committee* (Cmd 8662, 1952) 41 (Gregory Committee).

69 (2001) 108 FCR 235 at 34.

70 Ibid 28.

> (t)he production of any programme, indeed each and every frame and segment of it, comes at a cost. It is produced in order to make money by inducing advertisers to pay to have their activities advertised in association with its broadcast one or more times. Further value may arise from the isolation, reproduction and broadcasting of an image or images, with or without sound, from it, and the licensing of it or an isolated image or images from it, whether by and in a photograph, a film or a video film. What is clear in this case is that value did lie in the copying, reproduction and rebroadcasting of segments, albeit generally fairly brief segments, of the respondents' programmes. That value had two aspects: it enabled the appellant to gain revenue from advertising associated with The Panel; and it relieved the appellant of the cost *of buying or producing other matter to occupy the time taken by the rebroadcasting, during The Panel, of the copied and reproduced segments...*" (own emphasis) [71]

26 Moreover, the Panel case demonstrated that originality was not a requirement in the establishment of copyright in broadcasting:

27 (i)n the case of Part IV copyright, 'originality' is not a touchstone for the assessment of substantiality as originality forms no part of the identification of the interest protected by the copyright. For that reason, the notion that reproduction of non-original matter will not ordinarily involve a reproduction of a substantial part of a copyright work can have no application in the case of Part IV copyright. Nonetheless, the High Court's observation that the element of 'quality' bears on the substantiality question, and may involve consideration of the 'potency of particular images or sounds, or both', invites an assessment of the relative significance in terms of story, impact and theme conveyed by the taken sounds and images relative to the source broadcast as a whole.[72]

28 The significance of the Panel case is thus immense since as noted from the above-stated observations of the judges, there is not necessarily a clash with the notion of *originality*, rather, the Court is recognising a separate justification for providing copyright protection to broadcasters. The Federal Court expressly applied the utilitarian justification of dissemination to the public through broadcasts, which is undertaken by the broadcasters while employing significant resources and skills, other than authorial skills.

71 Ibid 27.

72 *TCN Channel Nine v Network Ten* [2005] FCAFC 53, [55].

IV. Copyright law in Australia: a fragmented reality comprising many rationales

29 From the previous discussion, it is evident that there is a clear recognition of the social-oriented perspective of granting copyright protection to broadcasters in Australia. This contrasts with the creator-oriented perspective, which excludes copyright protection for broadcasters to inhibit the creators' rights. In essence, there is a fragmentation within the copyright law in Australia with varied underlying justifications and orientations, which is due to the difference in the treatment of protection to the original content and its broadcast. Both may enjoy copyright protection separately, but it is important to underscore that such protection is because of the fragmentation under the law. This fragmentation has occurred with the introduction of protection to broadcasts that has, in turn, introduced the social-oriented perspective as a primary reason for copyright protection. The purpose here is not to criticise the fragmentation under the law itself, but to emphasise the need to anticipate clashes and disputes arising thereof, and revisit the underlying rationales in addressing these issues.

30 While the two streams of protection rationales—to the original authors and the broadcasters—may appear to be competing, Professor Ginsburg notes that, in fact, both are trying to achieve the betterment of society but through different methods.[73] Similarly, Simone Schroff highlights that there must be a balancing of any competing rationales and a continued emphasis on the various stakeholders' perspectives, rather than exclusively relying on normative theories propounding the basis of protection.[74] Effectively, a critical engagement within the existing framework of copyright protection to broadcasts is the current need, especially with the emergence of digital modes of broadcasting.

31 Jani McCutcheon also enunciates the above point, saying, it is difficult to discuss authorship in isolation because the requirement of originality is correlative and an "author is most remarkably the source of originality, a foundation of copyright subsistence".[75] However, the term "authorship" is

73 Jane C. Ginsburg, 'A Tale of two copyrights: Literary Property in Revolutionary France and America' (1990) 64 Tulane Law Review 990-1031.

74 Simone Schroff, 'The Purpose of Copyright-moving Beyond Theory' (2021) 16 Journal of Intellectual Property Law & Practice 1262–1272.

75 Jani McCutcheon, 'The Vanishing Author in Computer-Generated Works – A Critical Analysis of Recent Australian

not adopted for "subject matter other than works". Hence, "the existence of a human author is not a requirement for copyright protection of 'other subject matter' under Part IV of the *Copyright Act*".[76] Although "subject matter other than works" has not been treated through the classical "authorship–originality", the *Copyright Act* permits vesting copyright in the "maker" of the work.[77] When Part IV of the *Copyright Act* assigns copyright to a producer or broadcaster it disdains the requirement of originality. It is not necessarily a clash that is envisaged here; rather, a balance between originality and economic justifications in a complementary way. In the emerging technological and digital advancements, however, there may still be a need to refer to the balancing between the creator's and broadcasters' rights from a utilitarian perspective. Thus, the important takeaway is that, regardless of an implicit distinction in the protection granted to broadcasts as a subject matter and in favour of the broadcasting organisations, there is an important link among the creator of the content, the broadcasting organisations and the *public*. Such linkage needs persistent revisiting on occasions of perceived clashes among the stakeholders.

32 In the next section, we discuss some legislative and policy developments aimed at broadcasting and its protection under the copyright law in Australia to contextualise the discussion so far.

D. Constant need for balancing competing rationales for the protection of broadcasters' rights under copyright law

33 It is pertinent to note that discussions on enhancing the protection for broadcasters due to technological advancements have often invoked the public interest argument. For instance, the *Copyright Amendment (Digital Agenda) Act 2000* was introduced to extend broadcasting rights to cable transmission and online access to broadcasts. Within this Act, it is stated that the objective (among other things) is "promoting the creation of copyright material and the exploitation of new online technologies by allowing financial rewards for creators and investors".[78] The importance of encouraging broadcasters as *investors* was also mentioned in the *Copyright Amendment (Digital Agenda) Bill 1999*.[79] When the *Digital Agenda Act 2000* was implemented, it was based on the recommendations of the Copyright Convergence Group (CCG) appointed by the Minister for Justice in 1993. A careful analysis of the CCG's recommendations reveals that the CCG attempted to address the acts in which new technologies enable the material to be used, particularly electronic forms. While recommending new laws, including laws relating to broadcasts, the CCG has emphasised the "urgent need to provide a copyright framework to support *investment* in new Australian audio-visual enterprises that requires immediate and specific legislative change" (author's emphasis).[80]

34 Similarly, in January 2004, Phillips Fox (now absorbed by global law firm DLA Piper) released a report titled 'Digital Agenda Review: Report and Recommendations'. According to it, the objectives of the amendment of 2000 were "to ensure the efficient operation of copyright industries in the online environment through *promoting financial rewards for creators and investors*, providing a practical enforcement regime, and providing access to copyright material online" (author's emphasis).[81] Alex Malik's submission to the Digital Agenda report stated that "rights owners have the right to offer their products in the way in which they believe will maximise the return on their investment…" and further, "if IP rights holders are forced to offer their product in an alternate format for a lower return, the incentive for further investment and innovation

Case Law' (2013) 36 Melbourne University Law Review 915–969.

76 See *Telstra Corporation Limited v Phone Directories Company Pty Ltd* [2010] FCAFC 149, at [135] per Yates J. See also Anne, Fitzgerald and Tim, Seidenspinner, '*Copyright and Computer Generated Materials* - Is it *Time to Reboot the Discussion About Authorship*?' (2013) 3 Victoria University Law and Justice Journal 47, 50; Andrew Stewart, Philip Griffith, Judith Bannister, and Adam Liberman, *Intellectual Property in Australia* (5th ed, CCH Australia 2014) 168; Mark James Davison, Ann Louise Monotti & Leanne Wiseman, *Australian Intellectual Property Law* (Cambridge University Press 2008) 238.

77 Lasantha Ariyarathne, PhD thesis 2020 (Unpublished).

78 Copyright Amendment (Digital Agenda) Act 2000 (Cth), s 3.

79 Explanatory Memorandum, circulated by authority of the Attorney-General, the honourable Daryl Williams, Copyright Amendment (Digital Agenda) Bill 1999 at <http://www5.austlii.edu.au/au/legis/cth/bill_em/caab1999304/memo1.html> accessed 8 May 2022.

80 Copyright Convergence Group, 'Report on Copyright in the New communications Environment' [1994] <https://static-copyright-com-au.s3.amazonaws.com/uploads/2015/05/R00505-Highway-to-change.pdf> accessed 9 May 2022.

81 Phillips Fox, 'Digital Agenda Review: Report and Recommendations' (2004) 12 <https://static-copyright-com-au.s3.amazonaws.com/uploads/2015/05/R00345-FOX-Final-reportpassword.pdf> accessed 9 May 2022.

would decrease to the detriment of the community at large".[82]

35 In recent times, the discussion on enlarging protection for broadcasters has continued. In their 2016 submission to the Productivity Commission, FreeTV Australia stated that to encourage investment and innovation in Australia's creative sectors, it is critical that Australia's IP system:

> a) provides appropriate protection of broadcasters' rights;
>
> b) provides legal certainty in relation to access to copyright material; and
>
> c) does not impose [sic] unnecessary additional costs on broadcasters.[83]

36 Essentially, these submissions encouraging incentives to broadcasters, through the protection of the rights associated with the copyright on broadcasts, are based on the importance of communicating creative works to the public. It is an acknowledgment that such dissemination requires dedicated protection with a view to attaining certain social ends.[84] The underlying social-oriented rationale is thus at the centre of protective arguments for broadcasters; however, recent issues of content dissemination on the internet and retransmission have posed significant challenges to this justificatory framing.

37 In 2013, the Australian Law Reform Commission (ALRC) presented a comprehensive report on Copyright and the Digital Economy (ALRC Report).[85] This report addressed the emerging challenges for the broadcasting industry in the digital era, in which media and communication policies were seen to be converging. The ALRC noted the challenges faced by the industry with the emergence of content dissemination on the internet. Referring to a 2012 report by the Australian Communication and Media Authority, the ALRC Report highlights the inherent distinctions between traditional broadcasting and emerging technologies, including the internet:

> digitisation of content, as well as standards and technologies for the carriage and display of digital content, are blurring the traditional distinctions between broadcasting and other media across all elements of the supply chain, for content generation, aggregation, distribution and audiences.[86]

38 Consequently, the ALRC has suggested that the Australian Government should consider whether certain exceptions to broadcasters' protection under the *Copyright Act* must be repealed or amended, particularly under section 45 (broadcast of extracts of works), sections 47, 70 and 107 (reproduction of broadcasting), sections 65 and 67 (incidental broadcast of artistic works), section 199 (reception of broadcasts), section 47A (sound broadcasting by holders of a print disability radio license), and part VA (copying of broadcasts by educational institutions).[87] It must be noted that the ALRC was not concerned with any perceived clash between broadcasters' protection versus that afforded to original creators. It was effectively concerned with protecting the balance between the original creators' rights, and the broadcasters' rights in a digital era, which facilitated piracy in several forms. However, from a different perspective, it is essentially a clash between broadcasters' rights and the right of the public to access content on the internet in an easier, more affordable, and more convenient manner.

39 A related issue impinging on further protection for broadcasters in the digital age is the issue of retransmission. The ALRC report does not comprehensively address this aspect, partly due to an earlier report of the Australian Government's Convergence Review 2012. The Convergence Review had recommended a major overhaul in the current system of licensing of broadcasters and had suggested removing it altogether and replacing it with the regulation of "content service enterprises".[88] The ALRC noted that this may require "significant rewriting, and perhaps rethinking of Australian copyright law. Links with the *Broadcasting Services Act* would need to be removed from the *Copyright Act* and decisions made about extending copyright protection and exceptions beyond licensed broadcasters, for example, to all 'content service

82 Ibid.

83 FreeTV Australia, 'Submission by FreeTV Australia to Productivity Commission, [2016] 2 <https://www.pc.gov.au/__data/assets/pdf_file/0006/195693/sub129-intellectual-property.pdf> accessed 9 May 2022.

84 Megumi Ogawa, *Protection of Broadcasters' Rights* (Martinus Nijhoff Publishers 2006) 5.

85 ALRC, 'Copyright and the Digital Economy' (2013) <https://www.alrc.gov.au/publication/copyright-and-the-digital-economy-alrc-report-122/19-broadcasting-2/exceptions-for-broadcasters-2/> accessed 10 May 2022.

86 Ibid 409.

87 Ibid 432-3.

88 Convergence Review Committee, 'Convergence Review Final Report' (March 2012) <https://apo.org.au/sites/default/files/resource-files/2012-04/apo-nid29219_5.pdf> accessed 9 May 2022.

enterprises' otherwise subject to communications and media regulation".[89] In light of this, the ALRC noted that:

> (t)he retransmission scheme raises significant communications and competition policy questions. These should not necessarily be determined by decisions made about copyright law, but in the context of a more comprehensive review of issues at the intersection of copyright and broadcasting – including in relation to the concept of a broadcast as protected subject matter, as an exclusive right and in exceptions.[90]

40 Kimberlee Weatherall sheds important light on the challenge of retransmission for broadcasters. Referring to the issue of whether the contentious future WIPO Treaty on the Protection of Broadcasting Organizations was sufficient or desirable in respect of the predicaments of the broadcasting industry, Weatherall notes that the issue of retransmission, also noted in the submission of FreeTV discussed earlier, was set to be an impediment in ascertaining the future course of copyright protection for broadcasts.[91] Interestingly, her analysis points to the critique of giving into the demands from broadcasters to disallow retransmission of broadcasts, which have been put forth by NGOs on public interest grounds.[92] Thus, whereas the role of broadcasters was envisaged as being geared towards the social-oriented purpose and thus eligible for protection, their demands today, especially relating to designating retransmission as infringement, are being opposed on the same grounds.[93]

41 In order to understand this dichotomy better, Weatherall suggests that broadcast policy must be a key determining factor. What should be paramount is how flexible it is to mould broadcast policy for the State after considering the huge technological strides that might be in store. Weatherall suggests that before taking any legislative steps, this aspect of broadcast policy must be considered because regulation would be an important part of the protection of broadcasters' copyright due to the socio-public interests involved.[94] The situation that is envisaged here, and is, in fact, coming into the picture, is a critical engagement with the social-oriented public interest. This is a welcome aspect in the future that will determine that the technological strides in broadcasting and the consequent protection continue to adhere to its original rationale, i.e., the *availability* of content to the wider public.

E. Conclusion

42 The costs involved in making broadcasts are high. It is argued, therefore, that broadcasters' rights under copyright law are the acknowledgment of the social importance of their work and the financial compensation they are owed. The neighbouring rights which have been specifically introduced to provide protection to subject matters other than original works are a treasure for broadcasters to deal with unauthorised use and distribution of their broadcast signals because, should this right not be available, they would bear substantial losses and be unable to recoup their investments.

43 Considering this critical reason for granting copyright protection to broadcasters that arise out of the foundational rationale of social-oriented rights of the public to access information and original works, it is nevertheless pertinent to acknowledge the tremendous technological developments that keep the broadcasting sector on its toes. Moreover, while the focus of legislators, judges and policymakers has been on the potential conflict of interests between original creators and broadcasters, there is also an emerging conflict between broadcasters and the public through 'infringement' of broadcasters' copyright. The recent debates in Australia on retransmission and on enhanced protections for broadcasters have brought the spotlight back on such clashes. Whether such conflicts can be resolved through a focus on the inherent fragmentation within the copyright law—between the protection offered to original creators and broadcasters—will largely depend on the enhanced recognition and engagement with the underlying social-oriented purpose of granting special copyright protection to broadcasters.

89 ALRC, 'Copyright and the Digital Economy' (2013) 378 <digital-economy-alrc-report-122/19-broadcasting-2/exceptions-for-broadcasters-2/>accessed 10 May 2022.

90 Ibid 379.

91 Kimberlee Weatherall, 'The Impact of Copyright Treaties on Broadcast Policy' in Andrew T Kenyon (ed), *TV Futures: Digital Television Policy in Australia* (Melbourne University Publishing, 2007). See also Ysolde Gendreau, *The Retransmission Right: Copyright and the Redifussion of Works by Cable* (ESC Publishing 1990).

92 Ibid 243.

93 See Proposals by NGOs for a Treaty on the Protection of Broadcasts and Broadcasting Organizations (2004) <http://www.cptech.org/ip/wipo/ngo-broadcast-proposal-v2.8.pdf> accessed 9 May 2022.

94 Kimberlee Weatherall, 'The Impact of Copyright Treaties on Broadcast Policy' in Andrew T Kenyon (ed), *TV Futures: Digital Television Policy in Australia* (Melbourne University Publishing, 2007) 264-5.

44 This article has, therefore, argued that policymakers and judges will, in relation to the copyright law in Australia, need to strike a fair balance between the interests of original creators and broadcasters to reconcile the interests of both, and must, in parallel, critically engage with the right of the public to access the original content. Technological challenges will continue with further developments impacting all stakeholders, which will require a persistent (re) engagement with copyright laws, principles, and the underlying rationales.

Actions and reactions in commodifying cultural heritage hosted in museums

by **Cristiana Sappa***

Abstract: Museums are inclusivity-aimed institutions with a mission of education to knowledge. This mission can be appropriately implemented via the traditional initiatives of preservation and of exhibition, and the less traditional initiatives of sharing information related to cultural heritage via the internet or the metaverse, or yet by elaborating material to be used by visitors in an interactive fashion. It is undeniable that all these initiatives are costly. So, many museums did not resist the temptation of introducing self-funds mechanisms via the use of different legal tools, such as contractual provisions, national rules on cultural heritage and copyright principles. By exploiting these legal measures museums established a control-based approach, that make their focus shift to market dynamics. In the last decade, an open-access approach in this field was initiated by the civil society via bottom-up initiatives, on the top of which the legislator added some regulatory measures more recently. The latter expressely aims at consolidating access and education to knowledge. However, a closer look to the entire set of relevant regulatory measures in particular reveals that underpinning economic interests are the main priority of such an approach related to making images of cultural heritage collected in museums available for re-use pursposes, at a limited cost. These economic interests are only undirectly those of museums, while they are directly those of businesses. Thus, libre open-access practices and policies that encourage wide re-uses, should they be bottom-up or derive from a regulatory framework, would certainly bring two advantages. The first would be to let museums focusing on educational purposes in a fashion that is in line with the digital technology facilities; the second one would be to encourage market operators of any size to conduct business.

Keywords: commodification; museums; digitization of cultural heritage; digitalized cultural heritage; works of visual art; control; access to culture; education to knowledge

Recommended citation: Cristiana Sappa, Actions and reactions in commodifying cultural heritage hosted in museums, 14 (2023) JIPITEC 161 para 1.

A. Introductory remarks on the subject matter of the research

1 Cultural heritage is an umbrella notion covering both intangible and tangibles assets.[1] These assets have a scientific, cultural, historical or demo-ethno-anthropological interest. More broadly, it can be stated that these assets have a civilization-related interest. Thus, it is important to preserve them and enable current and future generations to access them directly or at least any information on

* Cristiana Sappa is Associate Professor at IÉSEG School of Management, 3, rue de la Digue, Lille. She is also affiliate researcher at Centre d'Etudes et de Recherche sur le Droit de l'Immateriel (C.E.R.D.I.).

1 For a discussion on the different facets of the term in the international legal instruments see: Blake, *On defining the cultural heritage*, in *International & Comparative Law Quarterly* 2000, 61 f.;Lixinski (ed.), *International Heritage Law for Communities: Exclusion and Re-Imagination*, OUP, 2019; Ferrazzi, *The notion of "cultural heritage" in the international field: behind origin and evolution of a concept*, in *Int. J. Semiotics of Law* 2021, 743 ff.; Stamatoudi, *The notions of Intellectual Property and Cultural Heritage: overlaps and clashes*, in Id. (ed.), *Research Handbook on Intellectual Property and Cultural Heritage*, EE, Cheltenham, 2022, 8 ff..

them for developing an individual or a community-based identity.[2] Researching tangible and intangible cultural heritage requires answering different sets of questions and an excessively long study, that cannot be done with a decent level of analysis given the limited space provided for a single article. Then, this work merely analyses tangible cultural heritage.

2 A substantial part of tangible cultural heritage is hosted by cultural heritage institutions (CHIs), such as museums, libraries and archives in particular. This comprehensive term was introduced for the first time in the Directive on copyright and related rights in the Digital Single Market[3] to address bodies that were conceived and introduced to facilitate preservation and subsequent access to tangible cultural heritage. Before this definition, those bodies were addressed in a more direct way, and often the acronym GLAMs, i.e. galleries, archives and museums, was used to point out to their practices and policies. CHIs is a broader term than GLAMs because other bodies, such as those collecting audiovisual material are also covered by the definition.[4] In any case, the use of CHI probably embeds the suggestion of leading a legal analysis extended to all the bodies covered by it. However, for reasons that are mainly related to the different peculiarities of each of the above-mentioned CHIs, for the societal evolution that is showing an increasingly massive consumption of images, as well as for some specific market dynamics in the image-related sector, the focus of this work is not as comprehensive. More precisely, the selection made is at two different levels.

3 On the one hand, this work studies museums only. Museums host cultural heritage collections that are composed of pieces that qualify as cultural goods, should they belong to arts or sciences. Three remarks are necessary here. First, the entire museum collection qualifies as cultural good, exactly like libraries or archives collections; also, each piece collected in a museum often qualifies as cultural good. The exploitation of cultural goods, whose definition is not univocal,[5] may be strictly framed by special rules that vary from one country to another and pay particular attention to preservation, for example in some European countries such as Italy, Greece, but also France and Germany. These rules apply on top of copyright (if any), contractual provisions and personal property[6] or real estate principles.[7] Secondly, the term museum is broad and covers collections of items of a different nature, and this implies various sets of challenges: as an example, the digitization of animal species presents technical complexities that artworks do not, while the latter may present concerns on preservation related to the age of the (often) unique tangible copy that the first ones do not have. Thirdly, when hearing the word "museum", we tend to think about very well established and renown art museums, such as the Pompidou Centre in Paris, the Pergamon Museum in Berlin, the Uffizi in Florence; however, museums may host collections with a very different focus (e.g., contemporary art or ancient Greece collections; museums of photographs on the history of mountains or on history of furniture design, etc.), they may be private or public (see the Egyptian museum in Turin

2 This is also the result of an empirical research funded by an ICOM special grant, according to which European museums, primarily in Central and Southeast Europe, "are seen as leverage for reinforcing national identity" INTERCOM – CIMAM, *Museum Watch Governance Management Project*, Report, 2022, 34, available at https://cimam.org/documents/192/Museum_Watch_Governance_Management_Project_INTERCOM-CIMAM.April2022.pdf. On cultural goods as essential elements of identity and belonging of individuals to a national sovreignity see Leone - Tarasco, *sub arts*. 1 - 2, in I. (eds.), *Commentario al codice dei beni culturali e del paesaggio*, CEDAM, Padoue, 2006, 33 ff.

3 Directive 2019/790/EU of 17 april 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, herein after the DSM Directive.

4 An example is the French Institut National de l'Audiovisuel (INA). See the EUCJ, 14 November 2019, C-484/18, Spedidam v. INA. For an interesting copyright-related discussion around the mechanism on evidence introduced for facilitating the exploitation of its collections see Debarnot, La triple validation jurisprudentielle du régime d'exploitation par l'INA des programmes de son fonds intégrant des prestations d'artistes-interprètes, in CCE 2020, n. 3, 1 ff.

5 The notion of cultural good is provided by a multiple set of international and national legal instruments, so there is no one-size-fits-all notion. See Servanzi, *Il patrimonio culturale e le opere fuori commercio nella direttiva digital copyright*, in *Il nuovo diritto delle società* 2019, 657 ff.

6 On the extension of the scope of property rights to the images of the owned goods see Mercier, *L'image des biens, ou la difficile conciliation de droits concurents*, in *Les petites affiches* 2006, 10 ff.; Fusi, *Sulla riproduzione non autorizzata di cose altrui nella pubblicità*, in *Riv. Dir. Ind.* 2006, 98 ff.

7 On the ability of the property right owner to forbid access to premises see in Germany Beater, *Des Schutz von Eigentum und Gewerbebetrieb von Fotografien*, in *Juristenzeitung* 1998, 1101 ff.; in Italy: Court of Rome (Pretura), 3 July 1987, in *IDA* 1989, commented by Carosone, *Prospettive del diritto all'immagine*, 468 ff.; Id. (Tribunale), 27 May 1987, unpublished; Court of Milan, 4 October 1982, in *IDA* 1983, commented by Fabiani, *Proprietà dell'opera d'arte figurative*, 41 ff.; Court of Rome, 23 June 1980, *ivi* 1980, 470 f.; in France Marie Cornu, *L'image des biens culturels: les limites de l'appropriable*, in Bloch (ed.), *Image et droit*, L'Harmattan, Paris, 2002, 611 ff.

managed by a Foundation), of differing sizes (such as the Louvre in Paris and the Cyprus museum in Nicosia), under different cultural heritage regimes, with more or less facilities for going digital, and with more or less awareness about the breadth of their public task.

4 On the other hand, this works focuses on art museums only, not only for the different technicalities related to the digitization of these specific collections compared to those connected to the science collections, but mainly because of the peculiarities related to the legal instruments governing the exploitation of works of visual art, which are at the core of market interests in specific sectors crossing the boundaries with the metaverse, such as virtual reality or video-games. Works of visual arts are referred at point 3 of the Annex of the Directive 2012/28/EU on Orphan Works,[8] which refers to them as including fine art, photography, illustrations, design, architecture, sketches of the latter works and other such works that are contained in books, journals, newspapers and magazines or other works. Therefore, they can be assimilated into the artistic works, as referred to by Article 2 of the Berne convention, i.e. "works of drawing, painting, architecture, sculpture, engraving and lithography; photographic works to which are assimilated works expressed by a process analogous to photography; works of applied art; illustrations, maps, plans, sketches and three-dimensional works relative to geography, topography, architecture or science". This list suggests the variety of techniques for creating works of visual art, as well as the content that they may reproduce. This suggests that individual pieces hosted in a museum may embed a work of visual art that may or may not have enjoyed copyright protection.[9] For instance, sculptures exhibited at the Rodin Museum are works of art that have been protected by copyright. Copyright may have never been there, like it is the case for most of the Greek, Italian, French museums, or may have already expired, like in the case of Van Gogh Museum in Amsterdam or the Chagall Museum in Nice. In other cases, copyright may still cover the exhibited works; for example, the Picasso Museum, the George Pompidou Centre, and the Tate Modern Gallery are hosting works that are still protectable. The point made here is that on a case-by-case analysis, it is possible to understand how many layers of legal protection cover individual pieces collected in a museum and, that copyright may be one of them.

B. Museums across centuries between changing facilities and a stable mission.

5 In ancient times, museums were a place where intellectual and wise men could exchange and debate.[10] In Europe, museums as we know them today were inherited by the enlightenment centuries. The first examples of museums come from the very late 17th Century and the following one. In 1677, the private collection of Sir John Trascendant in Lambeth became property of Sir Elias Ashmole and was moved to the University of Oxford to a building specially built for it. This building was opened to the public in 1683 and was named the Ashmolean Museum; this is considered the Great Britain's first museum. In 1734, Pope Sixtus IV donated more than thousand bronzes to the people of Rome, and this enabled the establishment and the opening to the public of the Capitoline Museums. In 1792, thanks to the French Minister Roland, exhibition premises opened to the public, without any social class-based distinction. Two years later, for the first time the notion of collective ownership of artworks was introduced in France, implying that such works belonged to the national community, who from that moment should take the lead in protecting them, as well as in valorizing them. It is within this framework that the first national museum, the "grand musée de la République", now known as the Louvre, was opened in Paris. Catherine the Great founded the Hermitage Museum in 1764 and it was opened for public viewing

8 Directive 2012/28/EU of 25 October 2012 on certain permitted uses of Orphan Works, herein after the Orphan Work Directive.

9 Collection as a whole can also qualify as works of art and therefore enjoy some copyright protection. More precisely museums can qualify as database. On this see already P. Galli, *Museums and databases*, in *IIC* 2006, 452ff..

10 Some sources referred to Ennigaldi-Nanna's museum, collected by Princess Ennigaldi as the oldest known museum. It dated from 530 BC and was located in the state of Ur and it held Mesopotamian antiquities; apparently it was visited enough to have clay labels in three languages. According to other sources the first museum was the one built in Alexandria, Egypt, in the fourth century before Christ, hosting a library, an astronomic observatory, research tools and material for studying or for artistic purposes. Before this, collection of more or less precious goods could be found in temples or graves, but their aim was related to religion or to recognition of passed away persons, and therefore different from the one of museums. During the Roman times, the practice of collecting objects to enjoy their beauty became more and more regular. Little by little the activity of gathering artwork collected during wars and military campaigns for enjoyment purposes increased. Later, in the Middle Age, Churches plaid the role of museums enabling enjoyment of beauty for the population. Lorenzo De Medici's collection was close to the current idea of a public gallery, but still the aspect of accessibility from the largest public was missing.

in 1852. Under the enlightenment approach, the common aim of museums in different countries is to underline the symbolic values of prestige and glory of the fatherland represented by works hosted in their premises and exhibited to the population, but also to ensure the preservation of historical and artistic values, as well as to introduce the notion of education to knowledge and enjoyment. Thus, since that time, museums can be considered as inclusion-aimed tools, exactly like other CHIs, because they were created and designed for facilitating the access to knowledge of cultural material to the largest public, without any discrimination. This approach is in line with the recent definition provided for the term museum by ICOM, according to which: **"[a] museum is a not-for-profit, permanent institution in the service of society that researches, collects, conserves, interprets and exhibits tangible and intangible heritage. Open to the public, accessible and inclusive, museums foster diversity and sustainability. They operate and communicate ethically, professionally and with the participation of communities, offering varied experiences for education, enjoyment, reflection and knowledge sharing."**[11] Definitions of national laws often contain most of the key term embedded into the ICOM notion, such as the permanent character of the collection, the preservation task, the aim of education[12] and enjoyment.[13]

6 Museums aim at preserving cultural heritage, for enabling the access to cultural heritage,[14] or at least to the information related to cultural heritage, i.e., its reproductions, complemented by any information, i.e. metadata. Preservation and access are essential means to education to knowledge, which is the essential mission of museums.[15] Thanks to education, better implementation of the rights of participation to the cultural life[16] and enjoyment of the benefits of scientific progress and its applications are possible.[17] Traditionally, the educational mission has been implemented via two main activities: preservation initiatives, including indexing and restoration tasks, and exhibition of works within the premises hosting a collection in a permanent or temporary fashion.[18] These activities, together with more or less interactive visits taking place within the premises,[19] have always been covered by the so called public task of museums.

7 However, since education is an ambitious aim, it needs to be interpreted according to the available technology and the social facilities evolving in times. So, digital technology came as an opportunity for educational purposes. Some of the major museums have therefore tried to reach visitors beyond their premises since the early 2000s, for instance via making reproductions of the hosted collections available on their websites. For lack of appropriate technological infrastructures, sometimes lack of awareness, or control-purposed reasons, such making available was not intended to enable subsequent re-uses, at least in an early phase.[20]

11 See the ICOM Extraordinary General Assembly approving the new definition on August 24th 2022, in the framework of the 26th ICOM General Conference held in Prague. The vote is the culmination of an 18-month participatory process that involved hundreds of museum professionals from 126 National Committees from all over the world.

12 Art. 101 of the Italian Code on Cultural Goods and Landscape (codice dei beni culturali e del paesaggio) and L 410-1 of the French cultural heritage code (code du patrimoine).

13 L 410-1 of the French cultural heritage code (code du patrimoine).

14 See for instance art. 2.11 of the KulturgutshuzGesetz stating that: "institution preserving cultural property", in particular museum (libraries and archives) shall mean any institution in the federal territory whose main purpose is to preserve and maintain cultural property and to ensure public access to this cultural property". See also Belder, 'Museums Revisited: The Position of the Museum in the New Governance of the Protection of Cultural Heritage and Cultural Diversity' in Porsdam (ed.), *Copyrighting Creativity: Creative Values, Cultural Heritage Institutions and Systems of Intellectual Property,* Routledge, 2015, 37 ff..

15 See supra footnote 12 and 13.

16 Sappa, *Participating in cultural life via augmented reality on cultural goods: what role for copyright?*, in *GRUR Int.* 2022, 618 ff.

17 Yu, *Intellectual property, cultural heritage and human rights*, in Stamatoudi (ed.), *Research Handbook on Intellectual Property and Cultural Heritage*, EE, Celthenham, 2022, 294 ff., also adds that to the extent that they help current and future creators, these institutions also promote the right to the protection of interests resulting from intellectual productions.

18 Cuno, *The Object of Art Museums*, in Cuno (ed.), *Whose Muse? Art Museums and the Public Trust*, Princeton University Press, 2006, 49 ff., spec. at 52 where the author explains that "[N]othing museums do is more important than adding to our nation's cultural legacy and providing visitors access to it."

19 CHIs can use information and communication technologies as efficient tools for making the visiting experience more intense, developing pedagogical contents, creating documentaries, touristic applications and games according to Commission, *Towards an Integrated Approach to cultural heritage for Europe*, Communication COM(2014) 477, of 22 July 2014.

20 The evidence of this is that some museums used the copyright symbol for discouraging any reuse of available reproductions, without appropriately checking whether there was any on the reproduced good or on the reproduction.

That has been, for instance, the case of the Louvre. Meanwhile, the digital has become more and more invasive in everyone's daily life. At this stage, the question raised by museums started to be whether spreading the information about the hosted cultural heritage *extra muros* as well, for instance via their websites, was part of their public task. In the recent years, institutional initiatives and public policies in different countries might suggest a positive answer to this question.[21] This means that museums are supposed to educate not only via exhibitions, but also via making information on the cultural heritage they collect digitally available, or by disseminating such information in any suitable fashion. This impacts the interpretation of the term "access" to cultural heritage. According to this approach, the notion of access shall be interpreted as a dynamic one, as opposed to a static one. Dynamic access implies that museums aiming at implementing their educational mission should ensure access to the real world premises and tangible goods, as well as access to reproductions and elaborations of digital realm goods, no matter whether they circulate on terminals or devices in the museum premises or beyond. Also, while traditional static access refers to the tangible cultural heritage, as exhibited in museums, the notion of dynamic access covers both tangible cultural heritage and the information related to it, namely reproductions and other complementary metadata. Information on cultural heritage, i.e. typically 2D or 3D digitized versions of cultural goods, with one or a few exceptions, can be more easily replaced than tangible pieces of cultural heritage collections in museums. In other words, to quote Walter Benjamin, goods exhibited in museums present an "aura",[22] and are therefore valued due to their presence in time and space.[23] They are scarce resources,[24] since they are often unique or in limited series. This creates attractiveness for such tangibles that their reproductions do not have.[25] As a consequence, the scarce nature of these goods and the related rivalrous exploitations in the real realm on the one hand, and the abundance of their reproduction, together with the connected non rivalrous exploitation, have an impact on market dynamics, as some of the practices described in the next paragraphs try to show.

C. The control-based and money-oriented approach

8 A traditional way to manage scarce resources, such as cultural goods hosted in museums, is to introduce a control-based approach.

9 Because of the very substantial financial and transaction costs of maintenance related to preservation, restoration, exhibition activities,[26] as well as digitization processes, for making material available, and for elaborating interactive digital, virtual and now even metaverse-based material to be used by visi-

Such a mispractice has been qualified "copyfraud" by Mazzone, *Copyfraud*, *NYU LR* 2006, 1026 ff., spec. note 78. It is also used by Japiot - Lignereux, *L'impression 3D et le droit d'auteur: des menaces à prévenir, des opportunités à saisir*, report of the Commission on the 3D printing for the Conseil supérieur de la propriété littéraire et artistique, 2016; and by Farchy – De La Taille, *Les licences libres dans le secteur culturel*, report for CSPLA, 2017. According to Kirkpatrick, *Rights and Reproductions in Art Museums*, *Museum News* 1986, n. 2, 45 ff., curators suggested to museums to enhance this practice; according to Berkowitz - Leaffer, *Copyright and the Art Museum*, *Col-VLA* 1984, 249ff., spec. 265 and 266 legal advisors suggested to follow it. And more recently see also Weinberg, *Cultural Institutions Behaving Badly: Stupid Reactions to 3D Scanning*, available at https://www.publicknowledge.org/news-blog/blogs/cultural-institutions-behaving-badly-stupid-reactions-to-3d-scanning-and-co, 22 January 2015.

21 The recent Italian Guidelines to the digitization of cultural heritage, issued by the Authority for Digital Italy (AGID) in June 2022, indicate that among the aims of digitization is access and enjoyment of the digital information on cultural heritage, thus implying that bodies managing cultural heritage – including museums – are supposed to go digital for enabling access, next to their exhibition activities. There might be some tips but in this sense also in the Guidance on Public Task Statements, published by the National Archives in UK, in 2015, p. 17 and 18, that refers to Re-Use of Public Sector Information Regulations of 2015. In Germany, museums consider the fact of making images of collected goods available on line as part of their public task, however they do not have a general budget for it.

22 Benjamin, *Das Kunstwerk im Zeitalter seine techniscen Reproduzierbarkeit*, Ursprünglichauf Französischerschienenin zeitschrift für Sozial-forschung, Jg.5, 1936, re-edited by Suhrkamp Verlag, Frankfurt am Main AG, 2012.

23 As also referred in Oruç, *Rethinking Who "Keeps" Heritage: 3D Technology, Repatriation and Copyright*, in *GRUR Int*. 2022, 1 ff.

24 Comments on the current world of abundance and of the rules of IP designed around scarcity are developed by Lemley, *IP in a World Without Scarcity*, in *NYU Law Review* 2015, 460 ff..

25 Non-Fungible-Tokens (NFTs) however, are able to re-establish such scarcity. See Nadini – Alessandretti - Di Giacinto – Martino – Aiello - Baronchelli, *Mapping the NFTs revolution: Market Trends, Trade Networks and Visual Features*, in 11 *Sci Rep* 2021, 20902.

26 Tam, *In Museum We Trust: Analysing the Mission of Museums, Deacessioning Policies and the Public Trust*, in *Fordham Urb. L. J.* 2012, 849 ff.

tors, museums are constantly seeking for funds. In addition, fewer and fewer (public) funds received may discourage them, or at least those less equipped, to take initiatives that would help enhance real dynamic access to information on cultural heritage in an efficient fashion. The fact that their public task traditionally covered preservation and access to on-premise initiatives only makes the museums perceive this as a missed opportunity, but not necessarily as a lack of performance of their public task. However, in order to limit the excessive inertia which that discouragement may create, museums have been—and often still are—strongly tempted to introduce self-funding mechanisms. Different sets of activities can be organized for enabling this fundraising. Concretely, museums may decide to impose authorization and a subsequent fee to access their premises, and to exploit the material they host or they digitized. This authorization-based mechanism works when there is an interest in exploiting such a content, either for digitizing and distributing it, or for digitizing and elaborating it, or also for disseminating exact or elaborated reproductions of tangibles after having acquired them directly. In other words, an authorization-based mechanism for reproducing and re-using cultural goods hosted in museums is viable in presence of a market at the downstream level. As for the works of visual art, such a market is there, and it is flourishing: e.g., for a long time history of art printed editions have been circulated in markets of countries where the subject is taught in schools, and are still largely present in museums shops, as well as in other bookshops. In these literary works typically faithful reproductions of visual works are embedded, as well as in elaborations like advertisement, extended reality experiences, video-games, or NFTs of masterpieces. To manage such authorisations and control the downstream market, different legal instruments have been used by museums. More precisely, these legal grounds span from the most traditional contractual provisions, to national rules on cultural heritage or intellectual property rights (IPRs) (particularly through copyright regimes).

10 Contractual provisions are used to govern the access to the museum premises and impose limits to the enjoyment of works once in the premises too. In particular, contractual provisions may limit the reproduction of works for commercial purposes. This means that, initially, contractual provisions framed rivalrous exploitations, such as the ability to enter into the museum premises, install equipment and reproduce the goods.[27] This already applied with the elaboration of printed copies of the masterpiece signed by the artist or with authorized reproductions before the massive interference of the digital technology in the cultural heritage sector.[28] Then, later, this applied again, with particular reference to the creation of digital collections of reproduced works, for making them available to third parties, or for elaborating material from reproductions, such as merchandising products, but also video-games, or other digital-based (and now, probably, metaverse-based) experiences. This characterizes a first phase of market-oriented practices, during which contractual deals were concluded with any professional market operators such as Bridgeman[29], Getty Trust, Corbis and a few others. These bodies aimed at digitizing entire museum collections and to combine them with other museums' digitized collections, with the clear plan of creating very comprehensive digital databases of cultural heritage.[30] The practice of these private market operators showed their intention to control non-rivalrous exploitations on the market. More recently, in a second and more advanced market-oriented phase, the boom of blockchain-based products shows the same interest of museums to get income from contractual deals with private market operators that may also mint NFTs. In this perspective, agreements have been concluded between national museums and private businesses in different countries.[31] Here, it is possible to compare and con-

27 Provisions on cultural goods often refer to this kind of activities as well. See infra note 47.

28 These initiatives showed that the main related issues leading to litigation were (are) concerning moral rights. See First Instance Court of Paris, 23 March 1992, *RIDA* 1993, n° 155, 181 ff., *Rodin* case.

29 See the extension of this first phase to more recent times: Bridgeman Images, *Important Announcement: Bridgeman signs agreement with MiBACT*, https://www.bridgemanimages.com/en/importantannouncement-mibact-italian-ministry-of-culture/12638. This is connected to infra note 120. Also, the ability of Brdgeman to distribute and license images in a digital world full of digital copies of cultural goods raises the issue on who could be addressed a legal action in case of infringement. See on this M.C. Janssen – Gorbatyuk – Pajares Rivas, *Copyright issues on the use of images on the Internet*, in Stamatoudi, *Research Handbook on Intellectual Property and Cultural Heritage*, cit., 191 ff..

30 See Sappa, *Museums as education facilitators: how copyright affects access and dissemination of cultural heritage*, in Bonadio – Sappa, *The subjects of literary and artistic copyright*, Elgar, Cheltenham, 2022, 233 ff..

31 Tommasi, *Art. 14 of the Copyright Directive and its Italian transposition: has Italy missed an opportunity to fully enhance its cultural heritage in the digital era?*, Final Paper for the Master in Intellectual Property of the University of Turin and the WIPO Academy, 2022, refers to the example of the Tondo Doni, that was digitally reproduced in nine unique copies in 1:1 scale, and then certified on Blockchain; one of these copies was sold in May 2021 for Euro 240,000.00, of which 50% of the net proceeds went to the Uffizi museum. The main aspect that attracted the attention of the Media in

trast different national approaches. In some countries, such as UK, national museums are intensively exploiting this chance to create revenues[32] that may enable them to recover several kinds of costs and to avoid any risk of deaccessioning.[33] Other countries, such as Italy, were already into a control-based approach during the early stage of the first phase of market-oriented practices; in these countries a renewed attention to such a well rooted phenomenon broke out, and it concerned the control and the sale (also through NFTs) of digital reproductions of works in high definition.[34]

11 Aligned with the authorization-based approach, as well as with the commodification of museums' tasks, national rules on cultural heritage in some countries have been designed around "control". The reference immediately goes to some sets of Italian and Greek rules. Back in 1993 the Italian legislator introduced legal rules to limit any exploitation of cultural goods, except for private purposes.[35] This Act was then issued in the very embryonic phase of the digital advent, and therefore designed with minds that were cast back before the digital existed. The same control-aimed rules are still present in Articles 107 and 108 of the Italian Code on Cultural Goods and Landscape (CCGL), issued in 2004.[36] On one hand, thanks to some reforms in 2014 and 2017, these rules are currently limiting the exploitations of cultural goods only when they have a lucrative purpose.[37] On the other hand, the recent National Cultural Heritage Digitization Plan of June 2022 does not take an entirely opposite direction to the one of control-based approach.[38] So far, case law on infringement of Article 108 of the Italian CCGL is very limited[39]; it is however worth noticing that the two cases currently attracting the attention of scholars are very recent and do not concern digital exploitations, but fashion designs[40] and entertainment objects, i.e. puzzles.[41] A similar experience can be witnessed in Greece, where back in 2001 some rules were introduced for

particular is the (lack of) contractual balance and the high return of investment that the company was able to keep. On NFTs and copyright aspects see Mezei – Lapatoura, *All roads lead to tokens – The impact of NFTs on galleries and museums*, in Bonadio – Sganga, *NFTs, Blockchain and copyright*, Routledge, forthcoming.

32 See the examples of the British Museum that accepted the minting of NFTs on some works of Turner, so that they could become accessible; od the Wave of Hokusai. See also the initiative taken by the Belvedere on the work by Gustav Klimt, The Kiss: a high-resolution digital copy was divided into a 100 x 100 grid, resulting in ten thousand unique individual pieces, offered as a NFTs.

33 Tam, *In Museum We Trust: Analysing the Mission of Museums, Deacessioning Policies and the Public Trust*, cit.

34 Again, Tommasi, *Art. 14 of the Copyright Directive and its Italian transposition: has Italy missed an opportunity to fully enhance its cultural heritage in the digital era?*, cit., refers about the action taken by the Italian Directorate General of Museums, affiliated to the Ministry of Culture. This body has recently issued a circular to suspend the ability of museums and private businesses to conclude contracts on the creation and sale of NFTs linked to digital copies of collected works of art. The DG justified this position by indicating the concern of the Ministry to lose "the management, control and exploitation" of digital images of works of national heritage. See also Sappa, *From the Past to the future: NFTs meet cultural heritage rules*, in Bonadio – Sganga, *NFTs, Blockchain and copyright*, Routledge, forthcoming.

35 See Legge Ronchey 4/1993 (i.e. the Ronchey Act, from the name of the political representative that chaired the works).

36 Code of cultural goods and landscape (Codice dei beni culturali e del paesaggio) issued with Decree 42/2004, of January 2004.

37 For a description on the evolution of these rules see Sbarbaro, *Codice dei beni culturali e diritto d'autore: recenti evoluzioni 2 nella valorizzazione e nella fruizione del patrimonio culturale*, *Riv. Dir. ind.* 2016, II, 63 ss.; Modolo, *Promozione del pubblico dominio e riuso dell'immagine del bene culturale*, in *Archeologia e Calcolatori* 2018, 73 ss.; Ciani, *Il pubblico dominio nella società della conoscenza. L'interesse generale al libero utilizzo del capitale intellettuale commune*, Giappichelli, Turin, 2021, 479 ff..

38 See information on such a soft law instrument at https://digitallibrary.cultura.gov.it/il-piano/

39 Court of First Instance of Florence, 14 February 2022, interim order 2992/2021; see also the Pornhub case reproducing the Titian's Venus of Urbino, that the Uffizi officially considered as "totally illegal", see Di Liscia, *Uffizi Is Suing Pornhub After It Turns Masterpieces Into Live Porn*, 2021, http://hyperallergic.com/664137/uffizi-sues-pornhub-after-it-turns-masterpieces-intoporn/.

40 The Uffizi Museum sent a letter to the French *maison* Jean Paul Gauthier back in April 2022 asking to cease all uses of "*the Birth of Venus*" in their *Le Musée* collection. The recipient removed the contested items from its online marketplace, but did not reply to the letter. Thus, the Italian museum Uffizi is now suing Jean Paul Gaultier, invoking the violation of the Italian CCGL and requesting the withdrawal of the 'illegitimate' clothes as well as an award for damages. See Riccio – Pezza, *Unrequited love at the time of French Maisons: the Museum v. Le Musée*, 21 November 2022, Kluwer Copyright Blog.

41 First Instance Court of Venice, 23 November 2022, interim order n. 5317/2022, concerning the use on Ravensburger puzzle of the Vitruvian Man of Leonardo Da Vinci. The Court issued an injunction of use against the Ravensburger company, as well as a penalty for any day of delay in its execution.

limiting the exploitation of cultural heritage.[42] A close look at Article 46 on access and use of monuments[43] and spaces of the recent reforms of 2021, informs that the legal scheme of control remained the same[44], with particular reference to the depiction[45] of goods for commercial purposes.[46] The common aspect is that the cultural goods collected by museums in both these countries are predominantly ancient. Thus, on the one hand, the concerns around preservation are substantial compared to those of countries in which museums host more recent cultural goods. Worries focusing on preservation are typically reflected in legal rules introducing strict conditions—including financial conditions—under which it is possible to install professional equipment in museums for reproducing the collected goods.[47] These rules, however, introduce an additional idea, i.e., the ability of earning some money from the rivalrous exploitation of cultural goods, since it makes sense to pay some fees when impeding any third party to enjoy cultural goods while they are being reproduced by professionals. Next to this, there is more. The ancient age of these goods tells that they are into the public domain because of the absence of copyright. The focus on the financial concerns, related to preservation and the implementation of an adequate public task, encouraged the maintenance of a conservative cultural approach and a subsequent political choice to control not only the rivalrous exploitations in the museum premises (*intra muros*), but also the subsequent non rivalrous ones[48] that typically take place in the digital realm and nowadays in the metaverse. In lack of copyright, other sets of rules, with a different source, have been introduced with this purpose. In this way, the rules initially aimed at preserving and valuing cultural heritage are killing the copyright limit's purpose of growing the public domain for fostering knowledge and creativity or innovation via re-uses,[49] thus affecting fundamental freedoms, such as those of expression and of conducting a business.

42 On the initial rules of 2002 see Morando – Tziavos, *Diritti sui beni culturali e licenze libere (ovvero di come un decreto ministeriale può far sparire il pubblico dominio in un paese)*, in ArcheoFLoss 2011.

43 Under art. 4D of the Greek Act 4858/2021 a. "monuments" means immovable items belonging to the Greek State and located in archaeological and historical sites or isolated, as well as movable monuments belonging to the Greek State and located in museums or collections of the Ministry of Culture and Sports or in legal possession of natural or legal entities.

44 Art. 46 par 4 of the Greek Act 4858/2021 requests for fees in case of production, reproduction and dissemination of works. Art. 46 also points out to art. (4A and) 4B, which states that any reproduction or dissemination of monuments for profit purposes is subject to a prior permission.

45 See art. 4D of Act 4858/2021, defining as a depiction of a monument a faithful reproduction of the existing image of the monument as a whole or in parts, in any way and by any means on a material medium (indicatively on forms or objects) or on an immaterial medium or on an intangible medium (indicative audiovisual material, electronic publications, internet, digital applications).

46 Article 15Γ of Act 4858/2021 is about photography fees. It indicates that for photography or filming in the marine, inter-river or in-lake archaeological sites or historical sites and shipwrecks, art. 46§4 shall apply and therefore charges has to be foreseen, unless the photography or filming is for non-commercial purposes.

47 Art. 108.1 b) of the Italian CCGL indicates that the fees to be paid depends (among others) on the tools used for such a reproduction. Art. 46 of the Greek Act 4848/2021 pointing out to art. 4A, under which the production of images and copies of monuments requires prior permission in different hypothesis. 1. When it concerns a monument, whose nature or state of preservation, exhibition, guarding, maintenance or restoration require access under special conditions to be determined by the competent authority service. 2. When such a reproduction or dissemination is carried out: i. by using an equipment that is bulky or requiring special installation and operating conditions, ii. through laser scanning, with photogrammetric methods or related technologies to create a three-dimensional model, or yet iii. in the context of a process, which requires special production conditions that affect safety, storage, custody, opening hours, public accessibility or other exceptional conditions. In a comparative perspective also have a look at art. 34 of the Turkish Act on Conservation of cultural and natural property 2863/1983 Copying, under which "The Ministry of Culture and Tourism shall have the authority to permit photographing and filming, making the impression and copy of movable and immovable cultural property at archaeological sites and museums affiliated to the Ministry of Culture and Tourism for the purposes of education, training, scientific research and promotion" (emphasis of the author of this piece). In Egypt, an attempt to introduce an approach based on control dates of 2007, when a draft law for limiting the exploitation of pyramids and other pieces of ancient Egyptian art was being discussed, according to McCarthy, *Egypt to copyright the pyramids and antiquities*, in *The Guardian*, 27 December 2007; and Stanek, *Can Egypt copyright the pyramids?*, in *National Geographic News*, 15 January 2008. The author of this paper is not able to report on the current state of art.

48 This is well explained by Modolo, *Riuso dell'immagine digitale del bene culturale pubblico: problem e prospettive*, *AIB studi*. 61, 1 (lug. 2021), 151 ff..

49 Litman, *The Public Domain*, in Emory Law J. 1990, 965 ff.; Samuelson, *Mapping the Digital Public Domain: Threats and Opportunities*, in *Law Contemp. Probl.* 2003, 1423 f.

12 Finally, at a first glance museums may consider copyright as a deterrent while digitizing collections, since they very rarely own them.[50] The recent introduction of Article 6 of the DSM Directive may facilitate the digitization of collections further than the former non mandatory exception of the InfoSoc Directive[51]; this provision, was introduced for fostering the cross-border cooperation between museums (and other CHIs),[52] and it is supposed to do it efficiently, since it is mandatory and cannot be circumvented by contractual provisions. However, it enables museums to reproduce the works they own or permanently hold in their collection for preservation purposes,[53] i.e., to maintain the works in their original or, at least, existing state. It reflects the political will to digitize the EU cultural heritage *en masse*, as key actors of a knowledge society, rather than leaving this to economic operators.[54] It is true that the term preservation is not explained and that there may be ambiguity as to whether the digital reproduction for preservation purposes concerns merely damaged or at a risk of deterioration works or can digitization be organized in a preventive fashion by migrating some works on readable formats, using sustainable format, countering foreseen obsolescence.[55] Considering the educational mission of museums, taking into account that it affects all the works they collect, and that preservation is a key goal in such a mission, it seems reasonable to interpret the notion of preservation of Article 6 extensively and state that conservative strategies are covered by it. In any case, the aim of preservation expressed as the only one implies that the digital copies cannot be accessed by the public, nor re-used.[56] Therefore, while this rule helps museums with the task of preservation, it does not play a major role in the discourse of commodification of the cultural heritage they host.[57]

13 Copyright has also been perceived by museums as an asset enabling some return of money; once the relevant downstream market is identified, copyright can function as a complementary tool in their self-funding initiatives. More precisely, some museums with contemporary art can claim copyright on the works of art they collect. Museums hosting collections of goods that are in the public domain may have tended to claim copyright protection[58] on the single digital reproductions or on the digital collections[59]—and therefore asked for the related fees. This is, for instance, the case of the Louvre, via the Reseau des Musées Nationaux - Grand Palais (RNM-GP[60]) in France.[61] This solution is still the

50 For references Sappa, *La propriété littéraire et artistique dans les institutions muséales à l'ère du numérique. Analyse comparée en droit français et italien*, Thèse, Paris XI – Pavia, 2009.

51 The InfoSoc Directive contained art. 5.2 c), admitting only "specific acts of reproductions", without mentioning whether digital reproduction was a requirement, nor mentioning the purpose of such reproductions. The provision was interpreted as not allowing digitization of entire collections. See EUCJ, 11 September 2014, C-117/13, case *Ulmer*. Also, the fact that this was not a mandatory provision made the EU legal framework look as a patchwork of inconsistent implementations. A thorough discussion on the topic of exceptions and limitations can be found in Sganga, *A new era for copyright exceptions and limitations? Judicial flexibility and legislative discretion in the aftermath of the CDSM Directive and the trio of the Grand Chamber of the CJEU*, in *ERA Forum* 2020, 1 ff..

52 See Recital 26 of the DSM Directive for the rationale of art. 6.

53 See Recital 27 of the DSM Directive, expressly referring to preservation initiatives as addressing "technological obsolescence or the degradation of original supports or to insure such works and other subject matter".

54 Dusollier, *The 2019 Directive on Copyright in the Digital Single Market: Some progress, a few bad choices, and an overall failed ambition*, *CMLR* 2020, 979 ff..

55 *Ibid.*

56 Visentin, *Le nuove eccezioni per la conservazione del patrimonio culturale e per l'uso didattico in ambiente digitale e transfrontaliero*, *Giur it*. 2022, 1273 ff.

57 It has to be noted however that in case private market operators are committed to help museums with the task of digitizing collections for preservation purposes, while performing their contractual obligations these subjects may keep digital copies with them. These copies can then be used for further computational uses, upon authorization, if necessary.

58 Or neighboring rights that may protect non original photographs. As an example Berlin State Museums used to use some Creative Commons licence because of the existence of §72 of the UrheberrechtGesetz. Protection on non creative photographs exists in Italy too, under art. 87 and ff. of the Italian Copyright Act

59 Wallace, *Surrogate Intellectual Property Rights in the Cultural Sector*, 2022, available at https://ssrn.com/abstract=4323691

60 This body is issued from the merger between the Réseau des Musées Nationauxand du Grand Palais des Champs Elysées; it has the status of an *Etablissement Public à Caractère Industriel et Commercial*, i.e. a public sector body that ensures the management of a public task, by producing and trading products and services.

61 Terms and conditions for re-use of images of works collected at the Louvre museums are available https://collections.louvre.fr/en/page/cgu#ART4_EN. See in particular art. 4.1.1 b), stating that "The use for any purpose other than those exhaustively listed in article 4.1.1 a.

favoured one by some museums, notwithstanding the *requirement* that the EU legislator introduced expressly via Article 14 of the DSM Directive, as well as some policy positions expressed at the national level within or out of the EU.[62] It enables them to have the control on exploitations by third parties that would like to elaborate upon the digital reproductions.[63] This approach underlines two things. On the one hand, it shows how legal tools designed for encouraging creativity and to grow the public domain for learning and future creations,[64] such as copyright, may be perceived in a totally different way, i.e. as a self-funding instrument. On the other hand, it emphasises the importance of digital copies as strategic tools for elaborations of cultural goods, i.e., for re-uses of works collected in museums.

14 Ultimately, the temptation of the museums to control some market initiatives for earning some returns that facilitate preservation and access-related initiatives is easily understandable, so is the trend that pushed them to reason like a business. This phenomenon occurred also in reaction to the COVID-19 economic crisis that recently affected the ability of receiving financial resources to face substantial costs in the cultural sector too.[65] However, museums are not business, nor market-structures, they are no-profit bodies. This statement has three main implications. The first one is that they have to prevent or limit and be able to cover any potential risk of damaging the goods they collect, as imposed by cultural heritage provisions.[66] Thus, authorizations and any condition-based systems for accessing the premises and exploiting the cultural heritage, for instance via photography or film making, or for creating advertising material, is reasonable and aligned with preservation purposes. Also, the design of related financial conditions in this framework may reflect the rivalrous exploitation of tangible goods, and therefore they come unsurprisingly, since they are part of a traditional real realm-based business model concerning the use of scarce resources. The second implication is that museums are not structured to compete with companies. While willing to take control on any mass digitization project, for a long time many museums have not had any technological, human or legal resource to do it. They did not have negotiation ability either, nor appropriate enforcement strategies. Therefore, when well established businesses like Bridgeman, Getty Trust or Corbis approached them for concluding a deal, museums accepted. Unfortunately, these contracts were the most often unbalanced,[67] but also most of the publishers in the downstream market would have more easily addressed these private companies than museums for having a licence on the digital reproductions. This is for several reasons. Companies know the market better by definition so they are better in the communication of their products and services; due to the aforementioned unbalanced contracts, companies have digital copies that enable computational uses, while museums often do not have anything more than a mere copy for preservation or limited access purposes; and companies have more comprehensive collections, while museums generally have digital collections of goods that they host, and therefore it is possible to centralize requests when dealing with companies, but not with museums. Companies are also more effective in enforcing their rights in a complex framework where infring-

above, and particularly any commercial use such as the manufacture and distribution of derivative products, audiovisual and multimedia production and printed publications other than those referred to in article 4.1.1, must be the subject of a written request sent by the User to RMN-GP via the website of its photography agency, photo.rmn.fr, or by email to agence_photo@rmngp.fr. The request must indicate the use or uses envisaged. The above uses are granted against payment, at the rates practiced by RMN-GP."

62 Wallace, *A culture on copyright. A scoping study on open access to digital cultural heritage collections in the UK*, Commissioned Report, Towards a Digital Collection, February 2022.

63 Sappa, *La propriété littéraire et artistique dans les institutions muséales à l'ère du numérique*, cit. See also EUCJ, 9 March 2021, C-392/19, case *Bild-Kunst*, which confirms the ability of controlling the dissemination of protected images via legal and technical forms of protection.

64 See supra note 49.

65 See Walsh – Wallace – Pavis – Olszowy – Griffin – Hawkins, *Intellectual Property Rights and Access in Crisis*, in *IIC* 2021, 379 ff., studying access in a patent and copyright perspective (and beyond).

66 As art. 20 of the Italian CCGL illustrates prevention measures are a combined set of activities aimed at limiting risks for the artwork in a museum collection, or the whole collection; in this perspective, some rules expressly ban destruction, as well as any other act or physical contact with the cultural good that is able to damage it; concretely, the reference pinpoints artworks moulding, but it may affect other sort of reproductions too: see for instance art. 46 of the Greek Act 4848/2021 referring to art. 4A. With particular reference to very ancient works, prevention refers to their exhibition without appropriate display cases in premises with strong lights, or yet uncontrolled visits to premises where ancient artworks are, when the air humidity is a main element affecting their preservation.

67 For some tips on the reasons that make these contracts unbalanced, see Sappa, *Museums as education facilitators: how copyright affects access and dissemination of cultural heritage*, in Bonadio – Sappa, *The subjects of literary and artistic copyright*, Elgar, Cheltenham, 2022, 233 ff..

ers are not easily found. For all these reasons, the big companies referred to have neutralized museums on the market and limited museums' abilities to create revenue[68] via control-based mechanisms introduced by cultural heritage or copyright rules in particular. The third implication is that museums have been created as educational and inclusion tools, and they should remain as such. As the ICOM definition expressly states, they are a non-profit institutions, thus, they cannot aim at making any profit that is not reinvested into their educational mission[69]; and this because their annual accounts and budget must be even. Therefore, all the attention to self-financing and market mechanisms is certainly related to their public task and their mission to enhance education. However, a disproportionate focus on financial dynamics risks driving them too far from their initial and essential goals, and shifting their interest to market-oriented practices excessively, with the consequence of distorting their vision, strategies and investments, to the detriment of the general interest of society.

15 In a different and complementary moral perspective, this shift towards market-oriented interests may also become an element to assess the lack of compliance with some copyright[70] or cultural heritage provisions[71] that relate to the artistic integrity of the collections.[72] According to a strict interpretation, these sorts of provisions might be understood to prevent purely market-oriented uses that favour the "trash-ification" of the cultural heritage. This sort of argument has already been used to prevent third-party use of images of cultural heritage. However, it seems that its real underpinning is not the protection of decorum, but the intention to control the economy related to cultural heritage images. Thus, this would reflect the same aim of the above-mentioned tools, but with a different make up. In any case, it is difficult to accept the argument of limiting the use of images on cultural heritage, by museums or by third parties, on the ground of the preservation of decorum. First, the argument is hardly justifiable,[73] considered the secular and democratic nature of access to culture, and its natural destination to be re-used. Second, should it be accepted, it would bring along the challenge of distinguishing appropriate from non-appropriate uses,[74] with the consequence of increasing the number of (potentially bad faith) legal actions. Lastly, such an argument would need to be balanced with important concerns on freedoms of expression[75] and to conduct a business, at least.

68 Factually, the revenues of Italian museums and archeological parks is a little higher than 1% in 2016 according to Tarasco, *Il patrimonio culturale: modelli di gestione e finanza pubblica*, ESI, Naples, 2017, 247 ff.). In France, the Cour des Comptes (i.e. Audit Court) issued a report in 2019, stressing on the fact that the sale of reproductions does not represent an important stake for museums. See also references in Tommasi, *Art. 14 of the Copyright Directive and its Italian* transposition, cit. footnote 60.

69 Amineddoleh, *Protecting Cultural Heritage by Strictly Scrutinizing Museum Acquisitions*, in *Fordham IP&Medial L.J.* 2020, 729 ff., suggests that because of their educational and public purpose, a portion of the museums monetary resources should be mandated for the due diligence required for museums to properly conduct acquisition investigations. More precisely, the author refers to the monetary resources generally granted tax deductions and government funding, while this work refers to other sources of money received by museums.

70 The risk of affecting integrity of works can be grounded into rules on moral rights: see for instance art. L 121-1 of the French code of intellectual property; art. 20 of the Italian Copyright Act.

71 Also Art. 20 of the Italian CCGL impedes uses that are not in line with the historical or artistic character of the goods.

72 See in this sense the answer of the State Secretary for culture of 19 February 2008 to the Italian parliamentary questions n. 4-05031 of 1 October 2007, as reported by Resta, *Chi possiede le piramidi. L'immagine dei beni tra property and commons*, in *Politica del Diritto* 2009, 567 ff.. This answer referred to the ability of reproducing public cultural goods in Italy, notwithstanding the absence of rules on the freedom of panorama, to the extent these reproductions do not modify the object reproduced and they are not offensive towards decorum nor the values the object expresses.

73 Hamma, *Public domain art in an age of easier mechanical reproducibility*, «D-Lib magazine» 2005, n. 11, http://www.dlib.org/dlib/november05/hamma/11hamma.html, is sceptical on the fact that when in front of Mona Lisa in the Louvre premises we find it ridiculous because of the multiple reproductions on biscuit boxes, wall papers and other items that are everywhere on the market.

74 Would low quality merchandise fall into the ban? Uses of famous monuments to advertise products, such as the David of Michelangelo in jeans or with a weapon? Other uses such as instrumentalization of violence, or for political purposes? Exploitations for AI training, such as in the case of Next Rembrandt project, available at www.thenextrembrant.com.

75 Again, see the Italian Act 106/2014 of 29 July 2014, that introduced into the CCGL the principle of free dissemination of images for the purpose of free expression of thoughts. According to that reform the mere presence of a lucrative purpose will not enable to qualify some uses of images of cultural goods as not appropriate. This is well discussed in Modolo, *Riuso dell'immagine digitale del bene culturale pubblico: problem e prospettive*, cit.

D. The current access to culture-aimed trend.

16 Museums rarely own copyrights on their hosted collections. This depends on the discrepancy between legal rules affecting the circulation of tangibles that are embed in protected works, and legal rules affecting copyright ownership of such works. Factually, museums mostly purchasing or being donated goods do not acquire the related copyright. For this reason, and because the limited room left to exceptions and limitations enabling reproductions and dissemination of copies, copyright has often been perceived as an additional deterrent to digitization projects, as well as to projects for making the digital versions of works available to the largest public. Next to this, the notion of access has traditionally been interpreted in a static fashion; only in the 2010s, has attention increased to the availability of information on cultural heritage for interests such as access to culture and education to knowledge. Thus, the broader notion of "dynamic" access has been pointed to for indicating that the outreach of educational initiatives of museums should have also been *extra muros*. Dynamic access may be open, and there is no consensus among museums about what open may mean exactly.[76] In this work dynamic access qualifies as open when online material may be enjoyed without paying any fees (free access), and it may even be re-used for different purposes (*libre*).[77]

17 Several elements and actors played a major role in boosting the implementation of initiatives aimed at achieving dynamic access, i.e., a wider circulation of images, which are mainly supposed to reflect an interest of access to culture and education. Depending on the actors involved and the circumstances, the implemented access may be merely free or even libre.

18 Some museums have remained more anchored to the real world and show a very reluctant attitude to share information. This reluctance may reflect lack of organizational, technical or human resources to go digital, as well as a general and conservative fear of losing control over images, including when legal measures are implemented to preserve them.[78] These museums, as long as performing preservation initiatives and enabling access to premises, may be considered as serving their public task by local authorities because of a traditional interpretation of cultural heritage rules on museums. In contrast, however, other museums have taken action as if dynamic access was part of their public task—even when, while being considered as part of their public task, this is not expressly mentioned in their bylaws or in rules on CHIs, nor is there a budget for it. In this second group, many museums in the last decade stopped claiming copyright on faithful reproductions of public domain works as a matter of policy.[79] Some of them engaged in digitization process for offering the collected material online: this is the case of the Rijksmuseum in Amsterdam, the Egyptian Museum in Turin,[80] the National Museum of Stockholm, the municipal museums in Paris[81] and other smaller and less known institutions, such as the Archaeological Museum of Cagliari who mainly made raw data available.[82] More precisely, these museums have released information—i.e., surrogates of the cultural goods collected in a free and unconditioned fashion—and implemented open-access policies by making reproductions available online for free and with no condition for any potential re-use. This initiative typically concerned reproductions of works in public domain (see the Archaeological Museum of Cagliari or the Egyptian museum in Turin). Others have implemented open-access practices by making reproductions available online for free, and by conditioning their potential exploitation via more or

76 Wallace, *A culture on copyright. A scoping study*, cit..

77 On the distinction between free and libre access see Suber, *Open Access*, the MIT Press, 2012.

78 As known, the Covid19 pandemic has exacerbated the digital divide for institutions without digital resources, expertise and presence, that may not go digital for lack of resources. See on this Hadley, *Covid-19 Impact: Museum Sector Research Findings Summary Report* (Art Fund), 2020, available at https://www.culturehive.co.uk/resources/covid-19-impact-museum-sector-research-findings/

79 McCarty – Wallace, *Survey of GLAM open access policy and practice'*, available at http://bit.ly/OpenGLAMSurvey. Interestingly, private market operators that used similar policies for controlling their released images, eventually made the faithful reproductions of public domain works available for free; such a release reminds to other market operators aiming at elaborating reproductions that they can use these high quality images instead of other reproductions issued by individuals on different platforms.

80 Respectively since 2012 and 2014 these museums made their collection freely available, mainly because the costs related to a control-based approach would have been more hardly sustainable than those related to an open data-based approach.

81 See information on it at https://www.parismusees.paris.fr/en/actualite/open-content-150000-works-from-the-museum-collections-of-the-city-of-paris-freely

82 See the official page of the museum in which data are available under a csv format, https://museoarcheocagliari.beniculturali.it/en/open-data/?Category

less restrictive/open Creative Commons licences.[83] This initiative typically concerned reproductions of protected works or protectable reproductions of works.

19 Next to individual and not necessarily coordinated initiatives at the museums level, important steps were taken thanks to institutional activities at both the local and regional level and to regulatory measures aimed at enhancing access to culture that the EU legislator issued in the last years, (e.g., the Directive on the Information Society of 2001).[84] Institutional activities are now framed by the Europeana project, launched in November 2008, with the ambitious aim of digitizing European cultural heritage and creating a more open and democratic society. Europeana is fed by national digitization projects, such as the Deutsche Digitale Bibliothek,[85] and fostered by the exchange with national bodies, such as the Italian Central Institute for the digitization of cultural heritage.[86] Local initiatives, such as those led by individual museums are also helping Europeana to grow further. More than a decade after its launch, Europeana deals with advanced interoperability issues, even though its policy is to make reproductions and metadata available under open licences (Creative Commons). Meanwhile, the European Commission issued a recommendation in 2021 on the creation of a common European Data Space for Cultural Heritage[87] that should build upon the same Europeana project, as well as many call for projects on this topic. Also, the European Parliament approved the funding of a pilot project in December 2022 for a feasibility study for the creation of a database of public domain works,[88] that should strongly affect the field discussed here.

20 In the meantime, the European Commission also issued regulatory measures aimed at fostering dynamic access of information on cultural heritage, at a first glance for the above-mentioned educational purposes. The first binding[89] measure that captured the attention of museums was the Orphan Work Directive[90] (OW Directive), which came in 2012 after a quite long discussion; it concerns works whose author or right owner cannot be identified or found and introduces measures for enabling a limited exploitation of such works, notwithstanding such an absence of authorization. Factually, a very substantial quantity of orphan works populates museums,[91] therefore the absence of a legal framework addressing the issue created challenges as to digitization projects—and as to any other potential exploitation of the works—should it be by the same museum or by third parties. The OW Directive preserves the ability to introduce a licencing scheme for these kinds of works, but it also contains an exception at Article 6, which notes that museums can exploit or-

83 Wallace – Deazley, *Display at your own risk: an experimental exhibition of digital cultural heritage*, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3378193; McCarthy – Wallace, *Survey of GLAM open access policy and practice*, available at https://douglasmccarthy.com/projects/open-glam-survey/

84 Directive 2001/29/EC on some aspects of copyright and neighbouring rights, herein after the InfoSoc Directive.

85 The DDB is a project funded by the German federal government and by German Länder, on the basis of a financial and administrative agreement of December 2009. For introducing this infrastructure, the federal government has provided a first slot of eight millions and a half from 2009 to 2011. The request to member states of the European Commission to digitize and make cultural and scientific information available via the European Digital Library (Europeana) has been essential for the creation of the DDB.

86 This body was introduced within the Ministry of Culture thanks to the decree (d.p.c.m.) 169/2019.

87 Commission, Recommendation C(2021)7953 on a Common European data space for cultural heritage, of 10 November 2021.

88 Once the exact scope of the project will be defined further by the European Commission, the project is expected to be launched next solar year, i.e. 2023, according to the Open Future Organization blog available at https://openfuture.eu/blog/the-eu-will-fund-a-feasibility-study-for-a-public-repository-of-public-domain-works/

89 Binding measures are also accompanied by soft law instruments. For instance, the Commission, Recommendation 2011/711/EU of 27 October 2011 on the digitization and online accessibility of cultural material and digital preservation, contains some first and interesting elements for better understanding measures that are introduced at a later stage. As its title suggests, it aims at fostering not only preservation but also online availability of information on cultural heritage and its subsequent reuse (See for instance art. 5.a) as a seed for art. 14 of the DSM Directive). See also the recent Commission, Communication COM/2021/118 final, *2030 Digital Compass: the European way for the Digital Decade*, setting the targets of digitization initiatives from now until 2030. This communication focuses primarily on the digitization aims concerning the cultural heritage at risk.

90 On Orphan Works ex multis: Hansen, *Orphan Works: Mapping the Possible Solution Spaces*, Berkeley Digital Library Copyright Project White Paper No. 2, 2012, available at https://ssrn.com/abstract=2019121; van Gompel, *The Orphan Works Chimera and How to Defeat It: A View From Across the Atlantic*, in *Berkley Tech. Law Journal* 2012, 1347ff.; Rodriguez-Moreno, *La nuova disciplina delle opere orfane*, in *NLCC* 2015, 893 ss..

91 Vuopala, *Assessment of the Orphan works issue and Costs for Rights Clearance*, Report for the European Commission, DG Information Society and Media, Unit E, 4, 2010.

phan works under purpose-bound conditions. They can make orphan works available or reproduce them for the purposes of preservation, restoration, indexing, cataloguing, digitisation and making them available. Thus, works covered by such an OW directive, that include some of the works collected in museums, except for photographs, can be digitized and made available online, notwithstanding the absence of their right owner's authorization. Making the reproductions of orphan works available, however does not imply any authorization for subsequent re-uses, that remain reserved to the right owner, whoever and wherever they may be.[92] Seven years after the OW Directive, the DSM Directive saw the day. This legal instrument contains several provisions that are supposed to encourage online access as well as re-uses under specific circumstances. Here the reference goes in particular to the exception and collective licensing scheme pointed out by Article 8 on out-of-commerce works, whose notion covers museum works according to some authors[93] , and it also goes to the lack of protection that has to be ensured in presence of mere reproductions of works of visual art in the public domain according to Article 14, whose introduction is supposed to end the discussion as to the protection of faithful copies of works collected in museums.[94] In a more transversal perspective, it is also worth addressing legal instruments beyond copyright, such as the Faro Convention on the value of cultural heritage for the society.[95] This Convention recognizes the individual and collective right to benefit from the cultural heritage and contribute to its enrichment.[96] In other words, according to this Convention the community has the right to access and participate in cultural heritage, and this suggests that the primary role of museums is to be useful to the development of society; thus, it reinforces the above-mentioned inclusion and educational role of museums, and the crucial importance of any related digitization initiative concerning cultural heritage. The Faro Convention values re-use,[97] since it invites museums to switch from the culture of free dynamic access with no re-use to the culture of free and *libre* re-use. According to some authors, this suggests reconsidering the mission of museums even further, since they would not remain merely cultural attractors, but should become cultural activators, i.e. bodies valuing the collected goods also by actively promoting creativity and innovation processes via the free re-use of data and creation of derivative works.[98]

21 Besides museums, institutional and regulatory initiatives, it is crucial to recognize the critical role that the civil society has played and keeps playing in this. Communities such as Communia or Wikimedia, or yet Open GLAM[99]—together with some projects focusing on complementary, but essential aspects, such as Creative Commons—have engaged in tremendous efforts for making bigger and bigger sets of digital reproductions available to a large public, with the least conditions possible for potential reuses, which has helped museums that would have not been able to do this because of the absence of technological, HR or legal facilities. They have been working in an autonomous and parallel-to-regulation fashion, lobbying with appropriate measures when

92 The OW Directive recently went under a review, finding that the text's mechanisms have been rarely used in practice and its relevance as a potential tool for the mass digitization of cultural heritage has proven to be limited. Despite the challenges the European Commission does not intend to propose any modifications to the Directive or measures to ensure that it has a bigger impact. See on this Matas - Zeintra - De Angelis, *Discover the review on Orphan Works Directive*, available on https://pro.europeana.eu/post/discover-the-review-of-the-orphan-works-directive

93 Servanzi, *Il patrimonio culturale e le opere fuori commercio nella direttiva digital copyright*, in *Il nuovo diritto delle società* 2019, 657 ff..

94 Thus, the provision takes an opposite position compared to the decision of the Bundesgerichthof ZR 104/17. However, two elements risk to empty the rule of its effectiveness: the discretion that courts use to assess originality, which suggests that 3D reproductions of 3D works may easily fit with such a requirement; and the ability to circumvent the rule with contractual provisions enable an easy lock-up of the free information. On this see Sappa, *Hosting the public domain into a minefield: the resistance to art. 14 of the DSM Directive and to the related rules that transpose it into national law*, in *JIPL&P* 2022, 924 ff..

95 Council of Europe, Framework Convention on the Value of Cultural Heritage for the Society, 27 October 2005, Faro. The Convention entered into force in October 2011, after the tenth ratification. On this see Pinton, *The Faro Convention, the Legal European Environment and the Challenge of Commons in Cultural Heritage*, in Pinton – Zagato (eds.), *Cultural Heritage; Scenarios 2015 – 2017*, Cà Foscari, Venice, 2017, 317 ff.. It is worth noting that this Convention has not been signed, nor ratified by countries like France, Germany, Greece; Cyprus has just signed it in 2021 and Italy has ratified it in the same year; it would be interesting to study the reasons for the political choice of these countries.

96 Art. 4 of the Faro Convention.

97 Modolo, *Promozione del pubblico dominio e riuso dell'immagine del bene culturale*, cit.

98 Viola, *Da attrattori ad attivatori culturali*, in *Territori della cultura* 2020, 230 ff..

99 Created in 2013 by the Wikimedia Foundation and Creative Commons. See https://openglam.org

necessary;[100] as a result, a huge number of works are available today and users can exploit them with some flexibility.[101] Next, individuals on social networks have been producing huge quantities of data and reproductions that circulate more or less unframed from one social network to another (Facebook and Instagram at first), and across platforms, such as Flickr. While to some extent, the circulation of works uploaded on social networks are subject to the rules imposed by the social network or the platform, factually this practice leads to a very substantial number of reproductions on the web, which are very hard to track.[102] This wide circulation of faithful (or supposed-to-be) reproductions has probably encouraged the policy of some museums to comply with making cultural heritage-related information digitally available via more open standards.

22 In summary, some regulatory measures that foster the accessibility of digitized cultural content, such as Article 6 of the OW Directive, keep any free and libre re-use under control. More broadly, museums that consider dynamic access as part of their public task, and that introduce open and libre data policies able to enhance a wide re-use of cultural heritage-related information create spill overs, certainly for educational,[103] cultural and social growth. Factually, fewer and fewer museums remain reluctant in making their collections available online. On the contrary, more and more museums make their collections available online, should they officially consider this as a part of their public task or not. However, not all the museums belonging to this second group enable an easy, libre re-use of the information accessible online, via suitable technical formats and licensing conditions. While dynamic access is recognized as a more and more important element for achieving the educational mission appropriately, measures to implement an adequate wide re-use of data are not regularly there. This may be explained in different ways. For instance, the situation is sometimes seen through a non-holistic perspective; thus, the reading of copyright rules does not necessarily embed the incentive to re-use that a more general approach provided by a combined readings of copyright instruments and the Faro Convention would give. Secondly, since the analysis is primarily made with copyright glasses, the concern about costs related to the loss of control on re-uses remains dominant compared to others. This last aspect reveals the maintenance of worries on economic aspects behind the curtains.

E. Are current rules on access and re-use aiming only at non-economic interests?

23 In recent times, actual practice shows that exclusive rights are increasingly perceived as ways too present in the field of museums. Thus, many of these bodies have shifted towards open (and sometimes libre) access policies, at a local or institutional level, even though there is no consistency as to what open access really means.[104] Civil society has helped to find online information on cultural heritage more easily. On top of that, regulatory measures have been introduced. Should these rules enable dynamic access and maintain control on further re-uses, or should they introduce *libre* open-access policies, thus enhancing both dynamic access and any re-use at a very low cost, a close look at them shows that they satisfy economic interests and therefore contribute to the discourse on commodification of information on cultural heritage.

24 Some regulatory measures foster the accessibility of digitized cultural heritage, but keep re-use under the control of museums or whomever acts on their behalf. This suggests that re-use is perceived as more closely connected to market dynamics that museums want to maintain under control for self-funding purposes; in other words, the mere presence of a market interest towards re-use provides legitimacy to the control-

100 See for instance the Public Domain Manifesto of Communia, available at https://publicdomainmanifesto.org, or the Europeana Public Domain Charter of 2010, available at https://pro.europeana.eu/post/the-europeana-public-domain-charter

101 With reference to art. 14 of the Digital Single Market directive, there is an evident connection between it and the legal action against Wikimedia of a Museum, in the famous *Museumfotos* case. See European Copyright Society, *Comment of the European Copyright Society on the Implementation of art. 14 of Directive 2019/790/EU*, in *JIPITEC* 2020, 110ff.. This also suggests how the civil society enhanced the shaping of regulatory measures (also) oriented towards access to culture.

102 Some of the concerns may be related to the decontextualization, lack of appropriate reference to the source of provenance of the image, or yet morality of some use. This means that under some circumstances it is important to balance the freedom of expression, freedom of research and maybe also freedom of conducting a business on the one hand, and the morality of some uses on the other. Some tips on the Italian approach to this issue are in Modolo, *Riuso dell'immagine digitale del bene culturale pubblico: problem e prospettive*, cit., 160 ff..

103 Denoyelle – Durand – Daniel – Doulkaridou-Ramantani, *Rapport sur les régimes de diffusion des images patrimoniales et leur impact sur la recherche, l'enseignement et la mise en valeur des collections publiques*, 2018, available at https://isidore.science/document/10670/1.46r9u7#

104 Wallace, *A culture on copyright. A scoping study*, cit..

based approach, according to which museums are entitled to boost mechanisms for self-funding purposes. Thus, when referring to wide dynamic access, the non-economic interest of easily accessing culture and knowledge is tied to the economic interest of authorizing any re-use of the digitized content. The question is whether regulatory measures introducing *libre* open-access policies are merely embedding an interest in access to culture and knowledge or a solely economic interest, without asking to whom that interest belongs. As an illustration, two rules will be taken into account here.

25 The first measure is Article 14 of the DSM Directive, which expressly reserves some room to public domain.[105] At a first glance, Article 14 seems to be focused on access to culture, in particular when read together with recital 53 of the same Directive, which expressly refers to "access to and promotion to culture, and the access to cultural heritage"; therefore the reference contained to this rule in the former paragraph of this work could be justified. However, two arguments at least can be used for proving that this provision mainly aims at protecting some economic interests.

26 According to a first argument, it is crucial to read current provisions in light of the preparatory and former works. Recommendation 2011/117 contained information about the competitive advantage brought along by digitisation and digital preservation of cultural heritage,[106] and the chance of digitized material for being re-used for both commercial and non-commercial purposes[107] and for "innovative applications".[108] Thus, even though this information is not clearly mentioned in the current provision, it has to be taken into account while interpreting the binding text of the more recent DSM Directive.

27 According to a second argument, it is essential to read each provision in a systemic fashion. Article 14 is one of the provisions in a Directive aimed at governing the good functioning of the Digital Single Market. Thus, unsurprisingly economic interests are connected to each clause contained in this text and to this article as well. Two different perspectives have to be studied in connection with this last statement. First, Article 14 does not necessarily exclude protection for material resulting from acts of reproductions. On the contrary, it expressly states that protection can be enjoyed by original reproductions.[109] On one hand, this part of the provision merely ensures consistency with general copyright requirements; on the other hand, this specific extract of the rule suggests that the outcome of reproductions can enjoy protection and therefore implies the recognition of economic interests too. Second, the option of leaving reproductions unprotected is beneficial for any market operator that wants to exploit them for elaboration purposes.[110] New creations are designed around and built upon former creative works of other authors.[111] Thus, not only protecting, but also limiting protection helps to develop the next generation of creative processes and knowledge. Copyright rules have been planned with this in mind, since fundamentally copyright has been conceived as a legal tool to promote creativity and not as a tool mainly for self-funding purposes. From this perspective, copyright has, therefore, been designed by combining exclusive rights and related limits. Once forms of exclusivity, including copyright, expire "works fall into the public domain and effectively become everyone's shared property"[112]. This implies that the "public owns them and they are in lawful right to create and use reproductions of the artworks for any purpose they like",[113] including for elaborating works for commercial purposes. The cost of accessing and re-using them is lower in absence of copyright (or any other form of) protection, even though contractual provisions are used for charging some fees for re-use.[114] This leads to three statements. The cultural aspects, referred particularly in Recital 53 of the DSM Directive, are certainly there, but they are complementary aspects, not as a primary ones. Also, the economic interests referred to are for whomever

105 European Copyright Society, *Comment of the European Copyright Society on the Implementation of Art. 14 of the Directive (EU) 2019/790 on Copyright in the Digital Single Market*, *JIPITEC* 2020, 226 ff.; Torremans, *The Digital Single Market Directive. Chapter 4 Works of Visual Art in the Public Domain*, in Stamatoudi - Torremans (eds.), *EU Copyright Law. A Commentary*, Edward Elgar, Cheltenham, 2 ed., 2021, 718 ff..

106 See recital 5 of the Recommendation 2011/117, referring to (cultural and) economic benefits of these initiatives.

107 Recital 7 of ibid.

108 Art. 7 (f). of ibid.

109 For a discussion on the potential copyright reproductions of 2D and 3D copies of cultural goods see Sappa, *Hosting the public domain into a minefield*, cit.

110 However see supra footnote 94.

111 Crew, *Museum policies and art images: conflicting objectives and copyright overreaching*, in *Fordham IP, Media & Ent. L. Rev.* 2012, 795ff..

112 As referred by Dusollier, *Scoping study on copyright and related rights and the public domain*, Report for the Committee on Development and IP, WIPO, May 2011.

113 Sanderhoff, *Open images. Risk or opportunity for art collections in the digital age?*, Nordisk Museologi, 2013.

114 This practice remains consistent with the rules on Public Sector Information re-use, because of art. 6.5 of the Directive 2019/1024, discussed in the next lines.

wants to design something upon the reproductions, since, in case of original elaborations, copyright can be enjoyed by their authors and right owners. Factually, this seems to favour market operators' interests, even though it is not possible to exclude *ex ante* that museums themselves elaborate material upon the digitized versions of collected goods. In any case, a systemic and trans-disciplinary reading of rules on copyright and re-use of Public Sector Information points to economic initiatives that can be initiated in the field, which would satisfy related economic interests.

28 The second reference goes to the Directive on the re-use of Public Sector Information and Open Data that was issued in 2019,[115] two months later than the DSM Directive. It (allegedly) tried to reply to the need of fostering a European market for the re-use of some data, as well as the democratization and enhancement of a more participative society. This Open Data Directive is the second review of a text that was introduced in 2003 for boosting the cross-border market of re-uses of information managed by public sector bodies. From 2010 to 2014, the European Commission funded two Thematic Networks on legal aspects of re-use of Public Sector Information (PSI), i.e., LAPSI and LAPSI 2.0.[116] The aim of these thematic networks was to bring legal scholars together in the field in order to study strategies and policies for introducing an appropriate legal framework and practices on PSI re-uses. As the outcome of the first thematic network shows, such a group of scholars worked on aspects closely related to market interests. A constant exchange existed between the members of the LAPSI projects and the representatives of the related DG at the European Commission. In this context, in 2013 the first revision of the Directive was issued.[117] Unsurprisingly, this text was focusing on market interest. However, it is worth mentioning that some reference to non-economic interests—such as the re-use of public sector information for creating a more democratic society—was pointed out already in the very final phase of the LAPSI project and, even more explicitly, in the very beginning of the LAPSI 2.0 project. Seven years later, the second revision of the text of 2003 was issued and, again, market interests are central to this text.[118] This last version applies to museums—as well as others CHIs—too.[119] This means that information produced and managed by museums—including digital reproductions—can be considered as PSI. Thus, the PSI Directive can apply when such an information on cultural heritage is not covered by IPRs belonging to third parties; this implies that when this information is available, it shall be re-usable. Some charges may be included for enabling re-use according to Article 6.2(b) of the Open Data Directive. Next to this, such a Directive is relevant in the discourse because it contains some provisions that limit the exclusive agreements[120] that typically were concluded within the framework of Public-Private Partnerships. In this way, the text enables museums to conclude (more) balanced contracts with well-established companies—such as Bridgeman or Google—that may tend to use their bargaining power while negotiating with them.[121] Finally, Article 11 of the Open Data Directive imposes non-discriminatory conditions for comparable categories of re-uses; within this analysis, this is related to exploitations of works that museums authorize.[122]

29 All this suggests that rules introducing limits to protection and encouraging wide re-uses, via open standards and licences, are there mainly for fostering economic interests. More precisely, such interests are those of private market operators that are already or want to enter the ecosystem developed around museums, such as editors of different products and using different technologies. In contrast, museums do not necessarily have an excessive interest in becoming pseudo-market structures, even though they have an interest in exploiting the elaborated works and material commissioned or independently developed by market operators—such as interactive multimedia

115 V. Sappa, *Access and Re-Use of Public Sector Information in a Copyright Perspective*, in Stamatoudi – Torremans, *EU Copyright Law. A Commentary*, 2 ed., EE, Cheltenham, 2021, 762 ff..

116 LAPSI stand for Legal Aspects of Public Sector Information. Information about the output of LAPSI and LAPSI 2.0 are available here: https://digital-strategy.ec.europa.eu/en/news/legal-aspects-public-sector-information-lapsi-thematic-network-outputs.

117 Directive 2013/37 on the re-use of public sector information.

118 See Recitals 7, 9, 10, 12, 13, 15, 20, 31 (and in particular the reference to the economic value of dynamic data), 36 – 40, 46 - 49, 51, 69.

119 This was not the case in 2003, while cultural heritage institutions entered under the scope of the 2013 Directive on PSI by way of exception.

120 Art. 12 of the Open Data directive states that agreements granting exclusivity are subjects to review on a regular basis, at least every three years. This rule is of particular relevance for agreements such as those noted supra at note 29.

121 See supra III.

122 Questions may raise as to the compliance with this provision of art. 108 of the Italian code on cultural heritage, which suggests that fees for exploiting cultural goods can be issued discretionarily by the authority with jurisdiction, even though some terms of reference are indicated by the same provision in the code.

works, virtual and augmented reality experiences—for educational purposes.

F. Conclusion

30 Internet and digital technologies shaped a world and a society that are substantially different compared to those of ten or twenty years ago, when individuals were simple users of cultural content, while they are now creators of it. Nowadays, individuals, bodies and associations want to access the cultural heritage, but also actively participate in its management and in valuing a subsidiary perspective.[123] This does not imply taking over of museums' tasks and missions. On the contrary, today more than ever it is essential that museums use their authority and their role as cultural mediators.[124] This applies also when, while implementing their educational mission, they release information on the internet and let third parties use them for any purpose, including commercial ones, so that the fundamental freedom of conducting a business is appropriately boosted.

31 The high costs related to preservation of and access to cultural heritage drove museums to take position on how to strike the balance between money-oriented exploitations, mainly for self-funding purposes, and inclusivity-aimed initiatives. If the public tasks of museums can be enhanced via an access that is dynamic and not merely static, even more efforts than in the past may be expected by these bodies, including higher costs. In line with this concern, case law and regulations at first favoured the extension of property rules or other control-based mechanisms on images of tangible goods[125] hosted by museums. However, general management and enforcement costs of control-based systems are higher than the revenues that may be generated by traditional authorization tools, including copyright licences. In commodifying cultural heritage, on one hand, rivalrous uses concerning tangible goods collected in museums may be controlled by authorization-based mechanisms in order to ensure preservation and, at the same time, to satisfy some economic and self-funding interests. On the other hand, images of cultural heritage may be produced and made available by museums, and—in particular—by other market operators too. The latter may replace museums in their role as intermediaries, with companies at the downstream level of the market chain such as publishers in different fields. At this stage, the attention shifts from the tangible goods to their reproductions. Here, as this paper discusses, it is essential that *libre* open-data policies are implemented because they are able to create more spill overs than control-based practices. This is why regulatory measures for limiting control-based approaches on one hand, and for boosting open access and—to some extent—re-uses on the other, have been introduced on the top of the practices of the civil society and of national of regional projects aimed at releasing data on cultural heritage under a free and *libre* access (and re-use) regimes. This statement has to be interpreted with an economic perspective, and not merely in an access-to-culture perspective.

32 *Libre* open data models may positively affect the notoriety of the museum,[126] as well as the ecosystem surrounding it, since they enable third-party economic initiatives to flourish. Therefore, (real) open data practices clearly facilitate the use of information on digitized cultural heritage and are a strategy to satisfy the economic interests of market operators mainly, unless museums are substantially involved in the elaboration of derivative works for commercial purposes. This last position, however, cannot be supported because it would not be sustainable. Museums may enjoy control on the rivalrous exploitations of cultural goods they host, mainly for controlling damages that could affect their preservation. It is totally understandable that museums need funds and need to introduce some activities to gather such funds, in particular in times of reduced public money and where substantial costs related to heritage preservation and access to works exist. The same EU texts on digitization of cultural heritage take these costs into account and do not underestimate the challenge that museums will face while engaging in educational initiatives via the use of digital tools.[127] However, adopting an excessively financial-based approach does not seem to be aligned with the main goal of museums, and therefore it is essential that they are involved in money-oriented exploitations for self-funding purposes as far as necessary and not beyond that. Museums have been created with the political intention to introduce educational tools for the society; the political intention is still there and thus, they should remain as educational tools. In addition, the normative element intro-

123 National Constitutions also refers to this. See for instance art. 118 of the Italian Constitution.

124 Modolo, *Promozione del pubblico dominio e riuso dell'immagine del bene culturale*, cit., 158.

125 Geiger, *La remise en cause du droit à l'image des biens: une privatisation du domaine public enfin freinée?*, in *RLDI* 2005, 6ff..

126 Bertacchini - Morando, *The future of museums in the digital age: new models of access and use of digital collections*, in *International journal of arts management* 2013, 60 ff.

127 See Commission, Communication COM/2021/118 final, *2030 Digital Compass: the European way for the Digital Decade*, cit.; Id., Recommendation C(2021)7953 on a Common European data space for cultural heritage; and Id., Recommendation 2011/711/EU of 27 October 2011 on the digitization and online accessibility of cultural material and digital preservation.

duced by the ICOM definition, which qualifies them as non-profit bodies impedes them to act as mere market structures and imposes them to re-invest all their income into activities of their educational missions.

33 From an economic or strategical perspective, an excessive devotion of museums to economic activities[128] shifts their focus from the core mission they have, and they should maintain education for democratic purposes rather than an economic mission that is typical of market structures, which in any case would see them as neutralized competitors in the market. From a different perspective, museums that re-invest their income into an educational mission might still be limited in the exploitations they make for commercial purposes that dilute the decorum in cultural heritage, according to a (non-desirable, but still existing) strict and morality-based interpretation of provisions that some jurisdictions aiming at keeping the control on the dissemination of images of cultural goods may use.

34 Therefore, the shift to an entirely entrepreneurial paradigm means museums risk to lose three times: politically, ethically and legally. It would also risk creating distortive interpretations of current rules for the mere purpose of controlling the circulation of images and the related economics. In other words, museums should maintain their focus on inclusive practices of dissemination of information on cultural heritage under open formats that encourage third-party re-uses, while keeping their distance from invasive market-oriented approaches. This solution is essential for implementing appropriately fundamental values such as freedom of expression, transparency, development of culture and research, education, as well as pluralism and therefore inclusion.[129]

128 This text quickly mentions NFTs. These assets are the essence of blockchain and Web3.0 philosophy. They reflect the intention to create, manage and exchange values embedded into digital formats; blockchain-based applications put an emphasis on the creation of proprietary rights over digital assets. And this does not shorten the distance from both the possibilities to share information widely offered by the digital infrastructure, as well as from the mission of museums and any open-data underpinning idea, which would aim at create and disseminate information. On NFTs Revolidis, *On Arrogance an Drunkenness – A Primer on International Jurisdiction and the Blockchain*, in *Lex&Forum* 2022, 349 ff..

129 Inclusivity is one of the indicators of community enrichment and well-being according to Kraeger – Cloutier – Talmage (eds.), *Re-Thinking Diversity, Inclusion and Inclusiveness: The Quest to Better Understand Indicators of Community Enrichment and Well-Being*, Springers, 2017.

To Grant or Not to Grant

Injunctions in the World of Standard Essential Patents

by **Michelle Dias and Mudita Gairola***

Abstract: Competition law is a complex law that is ever evolving and finds itself face to face not only with difficult theories of economics and market definition but also with intellectual property law. This interaction between Competition law and Intellectual Property law can be starkly seen in the world of Standard Essential Patents. With the increase in investment in innovation and knowledge, there has been an increase in technological advancements and inventions such as in the field of electronics communications and networks. Subsequently, this has led to the rise in the importance of interoperability. This is where standards, standard-setting organizations and standard essential patents become important. It may seem, especially in this context, that competition law and intellectual property law are in conflict. However, that is necessarily not the case. In this paper, a small aspect of this conflict will be analysed: – whether injunctions should be granted for FRAND-encumbered standard essential patents or not. For this, global trends and the Indian scenario have been studied. The study concludes by suggesting a balance be maintained between both the laws and between the rights of the standard essential patent holder and the standard implementer.

Keywords: standard essential patents; FRAND; intellectual property law; competition law

Recommended citation: Michelle Dias and Mudita Gairola, To Grant or Not to Grant: Injunctions in the World of Standard Essential Patents, 14 (2023) JIPITEC 180 para 1.

A. Introduction

1 A patent is a form of intellectual property (IP) right that seeks to protect technological advancement that has been reduced into practice. It is a negative right that allows the inventor to exclude others from commercially exploiting the invention for a fixed period of time, in return for disclosure of the details of the patented invention. One of the main justifications for such an exclusionary right stems from the need to reward innovators via intellectual property protection as a suitable reward for their intellectual labour.[1] Further, Intellectual Property Rights (IPRs) play a vital role in encouraging investment in the field of innovation. The growing investment in innovation and knowledge acts as a catalyst for further modernization and technological advancements. Progress in the sphere of economy and technology has always been closely linked. Thus, patents incentivize inventors to invest time, energy and money into producing valuable inventions by protecting their rights and giving them effective legal protection.

2 The growing focus on today's knowledge-based economy has led companies to value their patents more and to pay attention to their patent portfolios. In this context, IPR licensing is a key way to generate profit. One of the important ways for a company to do that is to own Standard-Essential Patents (SEPs). Standard-Essential Patents are the patents that are indispensable for implementing

* Michelle Dias, Teaching and Research Associate (Law), GNLU Gandhinagar; Mudita Gairola, LL.B. RGSOIPL, IIT Kharagpur.

1 C. May, A Global Political Economy of Intellectual Property Rights: The New Enclosures? 7 (Routledge, New York 2000).

a standard. Standards play a key role in the global economy and have become a ubiquitous part of our lives as they facilitate trade, allow cost savings for firms, increase economic efficiency and contribute significantly to economic growth.[2] Standards are the technical specifications for a new product or process.[3] Standards are required for interoperability and interconnectivity such as the three-prong plug, Hyper Text Transfer Protocol (HTTP), Global System for Mobile Communication (GSM), Long Term Evolution (LTE), Wireless Fidelity (Wi-Fi) and many more. Standards are so interwoven in our lives that we hardly notice them. They only come to our notice when they don't perform as expected or are not complied with (e.g., different plug standards for electronics). Standards are present in various fields such as in information and communications technology (ICT) products, medical equipment, industrial products, consumer goods, transportation system and manufacturing parts.

3 The key instruments in adopting, analyzing, coordinating and disseminating technology standards in different industries are the Standard-setting organizations (SSOs). SSOs can be governmental like the Bureau of Indian Standards (BIS) or private bodies like the American National Standards Institute (ANSI). They can be found at the national level like Telecommunications Standards Development Society, India (TSDSI), or international level, such as the International Organization for Standardization (ISO). The inventors/the technology owners as well as the implementers of the standard are the members of these SSOs. They are the stakeholders in the standard setting process. The final adoption and completion of the selection process of the standard depends on whether specific rules have been complied with, by the members. Myriad of questions arise when it comes to SEPs and standard setting. Certain pertinent questions play with the interface of competition and IP law.

B. The Tussle between Competition law and IP law in a Standard Setting

4 At the very outset, it may seem that there is a tussle between IP law and competition law. From *ex-ante* view, IP law creates rivalry between firms as they fight to get IP protection and benefits for their innovation. However, from the *ex-post* points of view, IPRs give monopoly to the owners and exclude everyone except the owner from reaping the benefits of the innovation. Thus, interplay with competition law is always in the picture when it comes to IP law. It is the objective of competition law to curtail such activities that threaten free trading and ultimately a free market. Competition law aims to promote competitive behaviour in the market so that ultimately consumer welfare is promoted along with increase in consumer choices. Monopolization is not illegal per se under Competition law but the abuse of such dominant position is.[4] These two branches of law seem to be at odds, as IP law grants exclusivity, while competition law prevents exclusivity when abused. However, this is over-simplification of complex laws, and it has been well established that they are in fact complementary. The end goal in each case is to promote general welfare and innovation. As Mark Lemley put it, *"the goal of both antitrust law and patent law is to maximize allocative efficiency (making what consumers want) and productive efficiency (making these goods with the fewest scarce resources)"*.[5] Thus, IP law is given special treatment under competition law. In India, Section 3 of the *Competition Act*[6] relating to agreements, explicitly exempts reasonable conditions imposed for protecting IPRs and Section 4 relating to abuse of dominance on account of holding of IPRs, considers all the factors under the framework of competition harm before arriving at any conclusion.[7]

5 In a standard-setting organization, anticompetitive conduct may include patent ambush by non-disclosure of relevant patents and violating fair, reasonable, and non-discriminatory (FRAND) licensing commitments by the IPRs holders. The SSOs have policy rules that govern the procedures for the adoption of a standard. They include disclosure rules and licensing rules. These policy rules try to strike a balance between Competition law and IP law. According to the disclosure rules, the participants in a standard-setting process must reveal any existing rights in relation to patents that may be related to the standard. The patents in question are the essential patents required for implementing the standard. The licensing rules, on the other hand, dictate that the terms under which the IPRs owners

2 T.M. Egyedi and K. Blind, The Dynamics of Standards 4 (Edward Elgar, Cheltenham 2008).

3 Hovekamp, H. Et Al., IP and Antitrust: An Analysis of Antitrust Principles Applied to Intellectual Property Law Section 35.1a (Aspen Publication 2003).

4 Section 4 (2), The Competition Act, 2002, No. 12, Acts of Parliament, 2002.

5 Mark A. Lemley, A New Balance between IP and Antitrust, 13 Sw. J. L. & Trade Am. 237 (2007).

6 The Competition Act, 2002, No. 12, Acts of Parliament, 2002.

7 Provisions relating to Abuse of Dominance, Advocacy Booklet, Competition Commission of India (May 11, 2020, 8:20 PM), https://www.cci.gov.in/sites/default/files/advocacy_booklet_document/AOD.pdf.

license the standard-essential patents should be fair, reasonable and non-discriminatory. It is pertinent to note that SSOs don't decide what these terms are. These fair, reasonable, and non-discriminatory terms are decided upon by the implementers and the IPRs holders in private bilateral negotiations. FRAND licensing terms are an *ex-ante* commitment to negotiate with potential licensees of the technologies. This commitment is a pledge by the patent owner to limit the right to exclude. While a patent owner has the exclusive right to not license a patent, adoption of FRAND terms acts a pledge to license the patented technology to parties who need access for the purposes of manufacturing.[8] Since there is no fixed FRAND rate and the SSOs do not outline what exactly are the fair and reasonable rates, many a times the IPRs holders do not comply with the responsibility to license their technology on FRAND terms. Further, the IPRs holders even stop the implementers from using the patent essential for the standard by seeking injunctions. In general, patent holders have the right to file for injunctions and exclude anyone from using their invention, however when FRAND commitments come into picture, this also becomes a concern for competition authorities. Thus, SEPs fall right in the interface of Competition and IP law.

6 The enforcement of the rights of an SEP holder through injunctions may lead to abuse of the dominant position of the SEP holder. The SEP holder's statutory rights to an injunction or an exclusion order are not waived by a normal FRAND contract. As a result, a FRAND agreement does not stop the SEP holder from seeking such remedies. Only in certain situations would a SEP holder's request for an injunction or exclusion order be considered a breach of the FRAND agreement—for example, if a FRAND commitment explicitly prohibits the use of injunctions or exclusion orders, or if the SEP holder requests an injunction before extending a FRAND license offer to the unlicensed implementer. However, the fact that an SEP holder has the right to request an injunction does not imply that the SEP holder can actually obtain such a remedy. This intricacy needs to be studied, and whether injunctive relief is a threat or not, needs to be looked into.

7 Technology standardisation and patent holders' rights must coexist in harmony. The main benefit of standardisation is that it may provide efficiency improvements, which are good for customers. This is because it enables producers to expand the total size of markets, achieving economies of scale and increasing product substitutability. In the realms of information and communication technology (ICT) and the Internet of Things (IoT), standardisation is very important. Standardization is essential for the use of ICT and IoT in the creation of "smart cities", which are able to handle a variety of challenges, such as traffic control, resource management, and public health, in a more effective way. The existence of SEPs and related litigation may have adverse effects on the production, promotion, and distribution of sophisticated products that include several proprietary standards and a growing number of IoT items. Owners of SEPs might, if they so desired, utilise the patent enforcement system to "hold up" or prohibit rivals from releasing competing goods that use the same standards by enforcing their patents. This raises fundamental questions about market competitiveness and the necessity of maintaining interoperability to guarantee the growth of the IoT business. As a result, there is a severe conflict between SEPs (which grant their owners monopolistic powers as R&D incentives/rewards) and standards (which allow for widespread and collective use).

8 Standard-setting organisations (SSOs) typically require SEP-owners to provide an irrevocable undertaking that they are prepared to grant competitors licences on FRAND terms in order to strike a balance between the need for standardisation, required for public use, and the private rights of SEP-holders. However, issues occur when the parties are unable to agree on what constitutes FRAND in a certain situation. The dissemination of technology and the marketing of goods and services may be inconvenienced if SEP-owners and prospective licensees cannot agree on the amount of royalties that should be deemed fair and reasonable, or if one party believes that the terms of the licence are discriminatory, or if the parties cannot agree on the territorial scope of the licence. Following the *Huawei v. ZTE*[9] case, the European Commission (EC) Communication of November 29, 2017, took into account three crucial SEP-related issues: (i) the requirement for a more transparent environment for negotiations between SEP-owners and licensees; (ii) the necessity of having common principles governing the valuation of SEPs technologies and FRAND terms; and (iii) suggestions for a more equitable enforcement system.[10]

8 Shubha Ghosh & D. Daniel Sokol, FRAND in India, University of Florida Levin College of Law Legal Studies Research Paper Series Paper No. 16-46 (2016).

9 EU:C:2015:477

10 Luke Mcdonagh & Enrico Bonadio, *Standard Essential Patents and the Internet of Things*, Policy Dep. Citizens' Right Const. Aff. (2019).

C. Global Perspective

I. United States

9 In 2006, a case came up before the US Supreme Court which dealt with the issue of granting injunctions in relation to patents. This case did not fall in the antitrust domain but was more of an equity decision concerned with private remedies generally.[11] However, this judgment was in direct opposition with what was usually followed in the US: a general rule that courts will issue permanent injunctions against patent infringement absent exceptional circumstances.[12] The Court held in *eBay case*[13] that four traditional principles of equity must be looked into while deciding whether to grant injunctions or not. A plaintiff must demonstrate that: (i) it has suffered an irreparable injury; (ii) remedies available at law (monetary damages) are inadequate to compensate for the injury; (iii) a remedy is in equity is warranted; and (iv) the public interest would not be harmed by a permanent injunction.[14] It was highlighted upon by one of the judges, Justice Thomas that injunctions may not serve the public interest in all cases especially when the patented invention is a small component of the final product that is launched in the market and the threat of injunction is employed for undue leverage in negotiations.[15] This *eBay* test is used to evaluate injunction requests made by SEP holders as well.

10 Some commentators have argued that, after making a FRAND commitment, an SEP holder can no longer meet the eBay requirements for obtaining an injunction. Mark Lemley and Carl Shapiro have posited that, by making a FRAND commitment, an SEP holder has conceded that monetary damages would suffice to compensate the SEP holder for the infringement of its SEPs.[16] An analysis of decisions in cases in which an SEP holder has requested an injunction reveals that, in each case, the SEP holder failed to meet the necessary criteria to obtain an injunction. For example, in *Apple Inc. v. Motorola, Inc.*[17], the Federal Circuit found that Motorola was not entitled to an injunction because it had failed to show that Apple's infringement of Motorola's SEPs had caused Motorola irreparable harm or that monetary damages would inadequately compensate Motorola for that harm. Similarly, in *Microsoft Corp. v. Motorola, Inc.*, Judge Robart denied Motorola's request for an injunction against Microsoft's products that used Motorola's essential patents.[18]

11 However, an important question concerning the SEP holder's right to seek an injunction is whether such a request could make the SEP holder liable under US antitrust law. Several plaintiffs have challenged SEP holders' conduct under the section 2 of the *Sherman Act*.[19] For example, in *Broadcom Corp. v. Qualcomm Inc.*[20], the plaintiff alleged that Qualcomm had monopolized the market for cellular telephone technology and components by, among other things, intentionally deceiving a private SSO. The US Court of Appeals for the Third Circuit found that the SEP holder's allegedly deceptive behavior during the standardization process was anticompetitive conduct actionable under the provisions of section 2 of the *Sherman Act*. After this, multiple plaintiffs used allegation of deceptive behavior to challenge the SEP holder's request for an injunction under the provisions of the act.

12 It is not just the *Sherman Act* but also the *Federal Trade Commission* (FTC) *Act* that has been invoked to try to make SEP holders liable for seeking injunctions under antitrust laws. Section 5 of the FTC Act[21] gives the US Federal Trade Commission authority to prohibit "unfair methods of competition" and "unfair or deceptive acts or practices". However, the FTC alone can initiate an investigation of conduct that allegedly violates section 5 of the FTC Act and there can be no private action. The US Federal Trade Commission investigated the SEP holder's request for an injunction under section 5 of the FTC Act in its 2013 investigation of Motorola Mobility.[22] The

11 S. Michel, Bargaining for RAND royalties in the shadow of patent remedies law, 77 (Antitrust Law Journal 889 2011).

12 MercExchange, L.L.C. v. eBay, Inc., 275 F. Supp. 2d 695 (E.D. Va. 2003).

13 *Supra*, note 10.

14 Valerio Torti, Intellectual Property Rights and Competition in Standard Setting 117 (Routledge Research in Intellectual Property 2016); *Supra*, note 10.

15 eBay Inc v MercExchange LLC, 547 US 388 (2006).

16 M.A Lemley and C. Shapiro, "A simple approach to setting reasonable royalties for standard-essential patents" (2013) 28 Berkeley Technology Law Journal 1135.

17 Apple Inc. v. Motorola, Inc., 757 F.3d 1286, 1331–32 (Fed. Cir. 2014).

18 Microsoft Corp. v. Motorola, Inc., No. 10-cv-01823 (W.D. Wash. Nov. 30, 2012), ECF No. 607.

19 Sherman Anti-Trust Act, 15 U.S.C. § 2 (1890).

20 Broadcom Corp. v. Qualcomm Inc., 501 F.3d 297, 307 (3d Cir. 2007).

21 Federal Trade Commission Act, 15 U.S.C. § 45-58 (1914).

22 Decision and Order, Motorola Mobility, L.L.C., No. 121-0120

FTC alleged that Motorola Mobility, following its acquisition by Google, engaged in "unfair methods of competition and unfair acts or practices" when it sought injunctions against allegedly willing licensees of its SEPs for smart-phones and tablet computers.[23] The FTC charged Motorola Mobility with violating section 5 by engaging in unfair practices that harmed competition in the market for electronic devices and that were "likely to cause substantial injury to consumers". Ultimately, the FTC settled its Motorola Mobility investigation with a consent agreement requiring Motorola to cease and desist from seeking injunctions against alleged infringers.

13 Both the US Department of Justice (DOJ) and the Federal Trade Commission took similar methods, citing worries about the competitive consequences of patent holders who had made FRAND pledges seeking injunctive relief to keep willing licensees out. However, this perspective has lately shifted. There is currently a developing schism between the two agencies regarding how the FRAND procedure should work. In December 2019, the Justice Department, the US Patent and Trademark Office, and the National Institute of Standards and Technology issued a formal policy statement[24] on remedies for SEPs. Injunctions for SEPs should be accessible on the same terms as for patents in general, according to the new declaration. It further maintains that antitrust rules do not apply to FRAND issues in general. This contradicts what has been widely accepted in the United States for many years. However, the on-going case of *FTC v. Qualcomm*, which has been closely followed and has garnered great public and media interest, could give a picture of how things will move on in the US. In this case, the DOJ has openly contested the FTC's accusations that Qualcomm exploited its market dominance to force others to pay greater royalties than they intended, and that Qualcomm then used this additional cash to prevent others from successfully competing with Qualcomm. The interface between Patents Law and Antitrust Law can be seen from this case, which perhaps may decide the role of anti-trust in SEPs and related FRAND activities moving forward.

(F.T.C. July 24, 2013).

23 Complaint, Motorola Mobility, L.L.C., No. 121-0120, at 1 (F.T.C. Jan. 3, 2013).

24 Policy Statement on Remedies for Standards-essential patents subject to voluntary F/RAND commitments, (May 11, 2021 8:30 PM) https://www.justice.gov/atr/page/file/1228016/download.

II. European Union

14 While the European Commission acknowledges that an injunction is a valid remedy, it has determined that where a patent owner has made a voluntary FRAND licencing promise and a licensee is prepared to engage into a FRAND licence agreement, seeking an injunction may constitute an abuse of a dominant position. This was held in the *Motorola*[25] case and the *Samsung*[26] case. The courts believed that the rights of the patent holder to enforce their intellectual property right, access the tribunals and freedom of trade needed to be balanced against the harms that will accrue due to the abuse of the dominant position of the SEP holder, which would be contrary to Article 102 TFEU. Thus, the European Union also recognizes that granting an injunctions as a relief would be inconsistent with FRAND terms.[27]

15 Further, in 2015 in the seminal case of *Huawei v. ZTE*[28] (*Huawei*) the European Court of Justice set the framework for the admissibility of FRAND defences in SEP infringement cases and clarified that in order for the SEP owner to obtain an injunction, (i) it must notify the alleged infringer of the infringement and designate the SEPs infringed as well as the manner in which they have been infringed; (ii) the alleged infringer must express its willingness to take a licence on FRAND terms; (iii) the SEP holder must provide a written licence offer on FRAND terms, specifying in particular the royalty and how it is to be calculated; (iv) the alleged infringer must provide appropriate security and be able to render an account of its acts of use in accordance with recognised commercial practises in the field and in good faith (and in particular without delay tactics) by accepting the SEP holder's offer or making a counter-offer, and (v) the alleged infringer must provide appropriate security and be able to render an account of its acts of use in accordance with recognised commercial practises in the field.

16 If an SEP holder seeks an injunction without first following these steps, a court may permit the alleged infringer to raise the "FRAND defense"—that is, argue that a license for the SEP was not offered on FRAND terms.

25 Case AT.39985 (2014), Motorola - Enforcement of GPRS Standard Essential Patents.

26 Case AT.39939 (2014), Samsung - Enforcement of UMTS Standard Essential Patents.

27 Nicolas Petit, Injunctions for FRAND-Pledged Standard Essential Patents: The Quest for an Appropriate Test of Abuse Under Article 102 TFEU (December 23, 2013).

28 Case C170/13, Huawei Technologies Co. Ltd v. ZTE Corp., ZTE Deutschland GmbH.

17 In 2016, the Dutch technology company Philips began to bring litigations in Germany and the Netherlands to protect an SEP it owned covering mobile cellular communication systems. In *Philips v. Archos*[29], a German regional court refused to grant an injunction, finding that Philips did not satisfy the *Huawei* principles and, thus, Archos had a FRAND defense. On the other hand, a district court in the Netherlands concluded in parallel proceedings that the SEP-implementer, Archos, proved unwilling to license Philips' SEP on FRAND terms as required by *Huawei*. In 2019, the Court of Appeal of The Hague again gave guidance on the interpretation of the Court of Justice of the European Union (CJEU) decision in *Huawei* and the standards for assessing FRAND defences under Dutch law in *Philips v. Wiko*.[30] The Court awarded Philips an injunction against Wiko as it was held to be an 'unwilling licensee'. The divergent national court opinions create confusion and it is important that there should be clarity amongst the members of the European Union as to how to approach this issue. The discussion around this is bound to evolve and develop in the coming years.

III. United Kingdom

18 *Unwired Planet v. Huawei*[31], one of the most significant standards-related patent matters heard by the UK courts recently, was decided by the UK Supreme Court. The Supreme Court ruled that the UK courts had the authority to decide on FRAND conditions for SEP worldwide licences, a ruling that is expected to solidify the UK's position as the preferred location for SEP holders seeking to enforce their legal rights. The Supreme Court concluded that the Courts of England and Wales have jurisdiction and may use a power to prevent infringement of a UK SEP unless an implementer accepts a global licence on FRAND terms in a unanimous ruling delivered by Lord Hodge. The Supreme Court determined that courts have the authority to determine the conditions and fees for FRAND worldwide licences. The Supreme Court also ruled that a UK injunction is the proper response when a UK patent is violated as a result of the implementer's refusal to accept a global licence, as doing so gives them "certainty that they can legally manufacture and sell products that comply with the standard on a worldwide basis," in addition to access to the UK market.

19 The Supreme Court determined that Unwired Planet was not required to provide Huawei a licence on the same terms that it had previously granted Samsung under the European Telecommunication Standard Institute (ETSI) IPR policy. Non-discriminatory "provides focus and narrows the scope for argument about what might count as 'fair' or 'reasonable' for these purposes in a given context," the Supreme Court said in explaining this decision, concluding that "fair", "reasonable", and "non-discriminatory" should not be seen as three separate obligations but rather as a single obligation. The Supreme Court further noted that a "most-favourable licence" word was missing from the ETSI IP rights policy (as was implied by the Huawei interpretation of non-discriminatory). ETSI has previously explored and rejected such a phrase. Because the circumstances of the CJEU case cited were different from those of the *Unwired Planet v. Huawei* case and Unwired Planet had demonstrated its willingness to grant a licence on terms deemed to be FRAND by the courts, the Supreme Court determined that Unwired Planet had not abused its dominant position in the market by starting legal proceedings before making a FRAND offer. Additionally, the Supreme Court ruled that it is not necessary to comply with Competition law in order to make a FRAND offer before seeking an injunction.

20 Because a worldwide licence may be obtained without the need for infringement procedures in many other jurisdictions, the Supreme Court's ruling is expected to strengthen the UK's position as the venue of choice for SEP holders looking to protect their rights. The judgement further improves the position of SEP holders and offers some guidance on how FRAND conditions may be determined, such as by taking into account the global rather than simply the national circumstances. The implementer may choose to accept the injunction and, if necessary, pay damages or refrain from operating in the UK market rather than complying with the court's direction to enter into a worldwide licence. Since SEP holders are not required to match earlier bids, an implementer's main decision may be whether to try to acquire a licence swiftly and at a fair price. It would be advantageous to let the courts decide on FRAND conditions if a SEP holder's demands for a worldwide licence are irrational. Additionally, even if a SEP holder is not required by law to make a FRAND offer before starting legal action, if a SEP holder behaves unreasonably, Competition law defences may still be available. Other national courts are likely to decide that they have the authority to impose worldwide FRAND licence terms in a manner similar to those of the UK courts. In this case, it's possible that SEP holders may engage in some forum shopping. When choosing a proper (EU) court in which to begin proceedings, any divergent interpretations of the CJEU decision in *Huawei v. ZTE* may also be taken into

29 Philips v. Archos, Regional Court Mannheim (7 O 19/16).

30 Koninklijke Philips N.V. v. Wiko SAS, Court of Appeal the Hague, The Netherlands, Case no. 200.219.487/01 (2 juli 2019).

31 UKSC 2018/0214

consideration. The appeal of simply accepting an injunction and paying damages or avoiding that national market may be diminished for implementers if other national courts follow the UK courts' example and issue injunctions preventing infringement of national SEPs absent the entry of a defendant into a global licence.

IV. India

21 In India too, the standard implementers can approach the Competition Commission of India (CCI) for remedies against abuse of dominant position and against anti-competitive agreements. However, most cases involving IPR issues have landed in the High Courts or the Supreme Court pursuant to a challenge to the jurisdiction of the Commission for adjudicating such matters.

22 In March 2013, after Ericsson failed to get mobile companies to discuss in good faith what Ericsson believed was a FRAND offer, it commenced the first of many SEP battles in India. Ericsson, as a member of the European Telecommunication Standard Institute (ETSI)—the European SSO for telecommunication industry—, had patents covering technology adopted as a part of a standard.[32] Ericsson wanted to enter into Ericsson's global patent license agreement (GPLA) while insisting that the mobile companies sign a non-disclosure agreement (NDA). In light of this NDA, Ericsson refused to share the license rates meted out to other licensees. Micromax refused to sign this agreement which led Ericsson to file for an injunction in the Delhi High Court.[33] An injunction was granted to Ericsson, as the single judge held that prima facie case had been made out by the plaintiff. Further, interim arrangement for royalties were made by the Court, additionally with authorization of search and report of consignments imported by Micromax. Similarly, Delhi HC had granted an *ex-parte* injunctive relief in *Vringo v. Xu Dejun*[34] stating that the case satisfied the three conditions for grant of temporary injunction in favour of the plaintiff, i.e., existence of a *prima facie case, balance of convenience and probability for suffering irreparable loss and injury. This was later vacated on multiple grounds, one of them being that ZTE Corporation (Xu* Dejun was the CEO at that time) had been directed to furnish the bank guarantee of Rs. 5 crores in lieu of the same and all relevant accounts of the quantum of CDMA devices sold by them in India and the revenues resulting from them.

23 In the *Micromax* case, following the Delhi High Court order, both the parties approached the court stating that they would start negotiating on a FRAND licence agreement, the failure of which would lead to resorting to mediation. However, the mediation failed and Micromax approached the CCI on grounds that Ericsson was abusing its dominant position.[35] Similarly, Intex too approached the CCI against Ericsson on similar grounds.[36] The Commission assigned the director general to conduct investigation stating clearly that Ericsson was charging royalty not based on FRAND terms. CCI's reasoning for the same was that Micromax in its complaint had stated that Ericsson was abusing its dominant position as the sole possessor of the essential patents by imposing exorbitant royalty rates. Further, these rates were based on the final product, i.e., the phone instead of the patents used.

24 Aggrieved by the CCI's order, Ericsson approached the Delhi High Court for judicial review.[37] The questions raised in this landmark judgment were of high importance as it was the first time such questions on SEP licensing, FRAND terms and jurisdiction of CCI were raised. According to Ericsson's argument before the Delhi High Court, the CCI lacks power to begin any case in connection to a claim of royalties by a patent holder, which is governed under the *Indian Patents Act, 1970*.[38] After a long-ranging discussion on the nature of remedies that are provided for in the *Indian Patents Act, 1970* and the *Competition Act, 2002*, the Delhi High Court observed that, "*if there are irreconcilable differences between the Patents Act and the Competition Act in so far as anti-abuse provisions are concerned, the Patents Act being a special Act shall prevail*."

25 The Delhi High Court, on the other hand, found no irreconcilable discrepancies between the two acts since the remedies available under the *Competition Act, 2002* for abuse of dominant position were fundamentally different from those available under the *Indian Patents Act, 1970*. The Delhi High Court (HC) also observed that it was apparent that the remedies under the two enactments were not mutually exclusive.

32 Telefonaktiebolaget LM Ericsson (PUBL) v. Competition Commission of India and Another (2016) SCC OnLine Del 1951.

33 Telefonaktiebolaget LM Ericsson v. Mercury Electronics (2013) SCC OnLine Del 4934.

34 CS(OS) 2168/2013 and IA 17292/2013 available at http://delhihighcourt.nic.in/dhcqrydisp_o.asp?pn=221627&yr=2013.

35 Micromax Informatics Limited v. Telefonaktiebolaget LM Ericsson (PUBL) (2013) SCC OnLine CCI 78.

36 Intex Technologies (India) Ltd v. Telefonaktiebolaget LM Ericsson (2014) SCC OnLIne CCI 8.

37 *Supra*, note 29.

38 The Patents Act, 1970, No. 39, Acts of Parliament, 1970.

Further, the Court held that Ericsson did stand in a dominant position and abused it, by citing *Huawei* and drawing similarities between *Treaty on the Functioning of the European Union* (TFEU) and the *Competition Act*. Thus, application of Competition Law is not barred in the Indian jurisdiction to IPR cases. From the injunction aspect we see that interim injunctions have been granted by the Delhi High Court in such cases but the court was ready to lift the injunction if the implementers deposited the (court determined) royalty payment with the court during the pendency of the litigation. Thus, in India, there's a possibility that an SEP holder may be able to seek injunctions against implementers.

26 The High Court of Delhi handed down India's first-ever SEP ruling in the joint (similar) cases of *Koninklijke Philips v. Rajesh Bansal* and *Koninklijke Philips v. Bhagirathi Electronics*[39] in July 2018. The defendants in both cases were importers and assemblers of DVD players in India. Philips filed patent infringement lawsuits against both of them, accusing them of importing DVD player parts made using its proprietary technology and putting them together in India without a licence. The implementers maintained that because they got the parts from Philips approved licensees, they had not violated the patent. The Delhi High Court made a decision in Philips' favour. The defendants' failure to obtain a licence from Philips to use its SEP prima facie led to the finding of infringement, the court held, even though the defendants' products complied with the standard. The court held that the defendants failed to prove that the components were imported from Philips' authorised licensees. The defendants were unable to demonstrate that the appropriate licence fee Philips levied was not on FRAND terms. As a result, the court set the requested royalties charged by Philips. Although ground-breaking, this ruling was rather simple and solely concerned itself with domestic matters. There is another dispute on SEP and FRAND which involves an international jurisdiction issue.

27 An anti-enforcement injunction was given by the Delhi High Court in *Interdigital Technology Corporation v. Xiaomi Corporation & Ors.*[40] It was decided that when Indian jurisdiction is the sole venue qualified to hear the claim, a party cannot be prevented from pursuing their case before an Indian court. By affirming and making India's first anti-enforcement injunction ordered in favour of a US technology pioneer, Interdigital, against the Chinese multinational Xiaomi Corporation, the Delhi High Court made legal history. The proceedings before the Wuhan Court involved alleged violation of six particular Indian patents, and the court noticed that the Wuhan Court had neglected to take this into account. The difference between an Anti-Suit injunction, an Anti-Anti-Suit injunction, and an Anti-Enforcement injunction was highlighted by the court. It was determined that the Indian injunction was in the character of an anti-enforcement injunction because the Wuhan anti-suit procedures had already come to a conclusion. The court also noted that any overlap between the proceedings in Wuhan and those in India is minimal, and that there was no justification for the Wuhan Court to have prohibited Interdigital from pursuing its claims for an injunction against Xiaomi in India unless the overlap was such that it rendered the Indian proceedings oppressive and vexatious.

28 Anti-enforcement suit settlements and various later reliefs have established new precedents. For Indian plaintiffs, this is a favourable and welcome development. The Delhi High Court has established new jurisprudential guidelines for the granting of an anti-suit or an anti-enforcement injunction with this ruling. Since there has never been a precedence in Indian law for this element, these principles will undoubtedly provide clarity in this area. The challenged ruling itself was oppressive and did not respect the jurisdiction of an Indian court to decide cases governed by Indian law, thus the court has specifically mentioned the restricted use of the concept of comity of courts. While deciding each case on its own merits, courts must strike a balance between the parties' rights and the need for justice and equality. After this ruling, it is extremely possible that the parties involved in the litigation will start using anti-suit injunction grounds. Therefore, this decision will make a significant contribution to both Indian and global law.

D. Issues with FRAND terms

29 There is a 2019 report[41] published by the Policy Department for Citizens' Rights and Constitutional Affairs of the European Parliament which addresses the conflicts between SEPs, FRAND and competition law. In the case of *Huawei v ZTE*[42], the CJEU laid down certain guidelines with an attempt to satisfy the interests of all stakeholders, i.e., SEP-owners, standard implementers, especially SMEs, and consumers. In a publication, EC Communication of 29th November 2017, recommendations were made to deal with each issue on a case-to-case basis and to leave the matter to the jurisdiction of the national courts to determine what is FRAND. Swift and cost-effective

39 CS(OS) No. 1034/2009 and CS (OS) No.1082/2009

40 8772/2020 in CS(COMM) 295/2020

41 Mcdonagh and Bonadio, *supra* note 12.

42 EU:C:2015:477

alternate dispute mechanisms are encouraged to resolve disputes. SSOs often need SEP-owners to provide an unequivocal declaration that they are willing to award competitors licences on FRAND terms in order to strike a balance between the need for standardisation and the private rights of SEP-owners. However, issues occur when the parties are unable to agree on what constitutes FRAND in a certain situation. If SEP-owners and prospective licensees disagree over the amount of royalties that should be deemed fair and reasonable, or if one party believes that the terms of the licence are discriminatory, or if the parties disagree over the license's territorial scope, this could cause an unfavourable hold-up in the marketing of goods and services as well as the diffusion of technology. The report offers a good suggestion to auctions off different technologies which the patent owners want to be included as or in the standard. The least restrictive and maximum royalty proposal could be accepted. This however, comes with its downsides where only the big and wealthy companies will be able to cherry pick leaving the small, striving companies to die.

30 The report points out the trend of court's interpretation of FRAND in the EU. There is a common principle followed by the courts in a select few countries mentioned in the report where the proprietor of a patent essential to a standard established by a standardisation body, which has given an irrevocable undertaking to that body to grant a licence to third parties on FRAND terms, does not abuse its dominant position by bringing an action for infringement seeking an injunction that prohibits the infringement of its patent or seeking the recall of products for the manufacture of which that patent has been used. Overall, of all the cases mentioned from Germany, The Netherlands, France and the UK, the courts give weight to the Commission's claim that there is legal complexity involved in SEP and FRAND cases. The disputes are 'hard cases' unsuited to a strict, inflexible approach. This is because what one interprets as FRAND is different in different locations and varies for different products, not to mention the change in value over time. How the economic value of a SEP is accessed cannot be put into a 'one-size-fits-all' mould. The discrepancies are inevitable. It should be left to the parties to come into agreement about what best suits them and only when there is a gross disregard to competitive practices, should the courts be involved.

E. Conclusion

31 Seeking injunctions for FRAND-encumbered patents presents the challenge of balancing innovator's intellectual property rights with the implementer's desire for fair access to technology. The analysis of the US, EU, and UK jurisdictions on the availability of injunctions for FRAND-encumbered patents has evidenced a somewhat consistent approach until recently. In the US, the DOJ and the FTC had taken similar approaches in the past. Both agencies had expressed concerns about the competitive implications of patent holders that had made FRAND commitments obtaining injunctive relief to exclude willing licensees. The Courts and authorities have clarified that IPRs holders may find it difficult to seek injunctive relief for patent infringements when they have committed to FRAND terms and the licensees have agreed to pay fair and reasonable royalties. The antitrust aspect thus has been in the picture for SEP holders in the US. However, the DOJ may be digressing from this view on account of its latest statements that injunctions should be available for SEPs on the same terms as for patents generally. Further, their statement also states that FRAND disputes may be kept out of the purview of the Antitrust law. This may put the patent-holders in a very favourable position, potentially leading to an abuse by them of their dominant position. The exact position in US needs to be clarified and the case currently in limelight, i.e., the Qualcomm case, may shed light on this apparent rift.

32 In EU, it has been held that when the implementer has shown itself to be ready, willing and able to enter into a FRAND licensing agreement, then an SEP proprietor who has made a FRAND commitment to license the patent to third parties on fair, reasonable and non-discriminatory terms will be held liable for abusing its dominant position if it takes recourse to injunctive relief. Even though these *Huawei* principles have been universally acknowledged, doubt still prevails as to the interpretation of these principles in the European Union in the light of the diverging opinions in the Philips case in Netherlands and Germany. These tensions may lead to a further reference to the CJEU in order to understand the final position.

33 In India, injunctions have been granted with a caveat that it will be lifted if the implementers deposit court-determined royalty. Such exclusion orders can be allowed if for example, the implementers are unwilling licensees and refuse to accept a FRAND royalty rate, demand royalty rates that are outside the scope of the FRAND commitment, etc. As far as India is concerned, there is also no ban on seeking injunctions with regard to SEP infringement. However, the Indian courts have acknowledged the role of Competition law in IPR cases. How far can Competition

law penetrate FRAND-encumbered patent issues is yet to be decided.

34 The key takeaway from the global conflicts is that it is crucial to encourage the parties, i.e., the SEP holders and the implementers, to engage in good-faith negotiations and induce them to reach mutually agreeable terms in an expedient manner. Thus, the risk of injunctions should be avoided at all cost, as patent litigations are always highly costly and time inefficient. For this it is essential to have a clearer picture of the licensing terms to be applied. The SSOs' FRAND licensing policies are mostly vague and at the root of the problems of the disputes. The conundrum remains as to what exactly are fair and reasonable terms. It is to be noted that the number of patent cases submitted to arbitration is relatively small.[43] Commentators have suggested the use of arbitration to answer this thorny issue. Mark Lemley and Carl Shapiro have proposed best practices for stand-setting bodies based on "baseball-style" or "final offer" arbitration.[44] However, this solution faces the issues of needing adoption by all the members of the SSO. Until then, with regards to seeking and granting injunctions, a balance needs to be created and it should be ensured by the courts and authorities that an approach that skews the process towards any one party unfairly should not be adopted.

43 M.M Lim, "ADR of Patent Disputes: A Customized Prescription, Not an Over-the-Counter Remedy" (2004) 6 Cardozo Journal of Conflict Resolution 155.

44 M.A Lemley and C. Shapiro, *Supra*, note 14.

Transparency as a legal value for patent disclosure

by **Daria Bohatchuk***

Abstract: This paper is dedicated to the assessment of transparency as a legal value in patent law, as well as in other areas of information flows. It outlines the essence and functions of transparency and, on this basis, proposes a genuinely new conception for assessing transparency. This conception is then applied to the patent system, more particularly to patent disclosure. It sheds new light on disputed issues such as the sufficiency of patent disclosure, the best mode requirement, and the disclosure of training data when patenting AI inventions.

Keywords: Transparency; patent disclosure; legal value; information

Recommended citation: Daria Bohatchuk, Transparency as a legal value for patent disclosure, 14 (2023) JIPITEC 190 para 1.

A. Introduction

1 The era of innovations associated with computers has been christened the "Information Age" and has been made possible by a so-called "digital revolution".[1] Modern technologies have increased availability and accessibility of information, but have made the information more vulnerable towards potential infringements. The new ease with which information can be processed has significantly influenced the intellectual property (IP) sphere. Scientific and technological development keeps constantly challenging the established foundations of IP law.[2] Nowadays, the legal environment urgently needs the tools guaranteeing the quality of disseminated information and the legal foundations adjusted to modern reality.

2 This paper aims to look at transparency as a legal value that should ensure the quality of information and to consider the implementation of this value in patent law through patent disclosure. I first characterize transparency and propose a conception that allows one to assess implementation of transparency. This builds a foundation to consider patent disclosure in the light of transparency and suggests the means to strengthen the quality and availability of patent information. The paper outlines possible solutions to the issues of the best mode requirement and the requirement of disclosing training data when patenting artificial intelligence (AI). In general, legal research regarding transparency contributes to transformation of the said legal value into a principle of law, building the legal foundations in the areas of information flows.

* Postdoctoral Research Fellow, Faculty of Law, Center for Life Sciences Law, University of Basel; e-mail: daria.bohatchuk@unibas.ch.

1 Helen Gubby, *Developing a Legal Paradigm for Patents* (Eleven International Publishing 2012) 295.

2 William Van Caenegem, *Intellectual Property Law and Innovation* (Cambridge University Press 2007) 22.

B. Essence and Functions of Transparency as a Legal Value

3 Legal responses to technological changes have a significant impact on the economy, the development of technologies, and social welfare.[3] Transparency requirements can be considered one of the responses to the challenges of the information age, when increase of accessibility and availability of information does not guarantee the quality thereof. This response shall be duly consolidated and integrated in law.

4 The scientific literature proposes different definitions and different approaches to understanding transparency.[4] However, the meaning of transparency depicted in the literature seems to be vague and unclear. It is admitted that transparency constitutes "a mental representation of a general idea"[5], which is difficult to define.[6] Although the notion of transparency is neither obvious, nor easy to access, the current state of critical transparency studies does not contribute much to the implementation thereof.[7]

5 In the literature, transparency is more and more often referred to as a legal principle[8] and even considered as a legal norm applied, in particular, by the EU institutions.[9] It is said that at the European level the transparency principle has developed from the principle of contract law into a general legal principle.[10] Transparency is sometimes qualified as a general principle of law under Article 38(1)(c) of the Statute of the International Court of Justice, although such qualification faces difficulties in reasoning.[11] Some authors consider transparency as a principle of specific branches of law, for example, as "an interpretative principle of international economic law".[12]

6 There are different views on the notion of "principles" in the literature. In a general sense, a principle is a beginning, a basis, a basic rule, a starting point, etc.[13] Black's Law Dictionary generally defines the "principle" as "a basic rule, law, or doctrine".[14] Ronald Dworkin proposes to perceive a principle as "a standard that is to be observed, not because it will advance or secure an economic, political, or social situation deemed desirable, but because it is a requirement of justice or fairness or some other dimension of morality".[15] Various opinions also exist concerning definition of the principles of law. The Legal Encyclopedia of the National Academy of Sciences of Ukraine defines the principles of law as "guiding foundations (ideas) that determine the content and direction of legal regulation of social relations".[16] The Ukrainian scholar Olga F. Skakun offers the following definition of the principles of law:

3 Roger Brownsword, *The Oxford Handbook of Law, Regulation, and Technology* (1st edn, Oxford University Press 2017) 225.

4 Black's Law Dictionary proposes the following definition of transparency: "Transparency. Openness; clarity; lack of guile and attempts to hide damaging information. The word is used of financial disclosures, organizational policies and practices, lawmaking, and other activities where organizations interaction with the public", Henry Campbell Black and Bryan A Garner, *Black's Law Dictionary* (8th edn, Thomson West 2004) 1537.

5 Andrea Bianchi and Anne Peters, *Transparency in International Law* (Cambridge University Press 2013) 6.

6 ibid 7, 8.

7 See Christopher Hood and David Heald, *Transparency: The Key to Better Governance?* (Oxford University Press 2006); Emmanuel Alloa and Dieter Thomä, 'Transparency: Thinking Through an Opaque Concept' in Emmanuel Alloa and Dieter Thomä, *Transparency, Society and Subjectivity: Critical Perspectives* (1st edn, Springer International Publishing 2018).

8 Anoeska Buijze, *The Principle of Transparency in EU Law* (Utrecht University, Uitgeverij BOXPress 2013) 73 <www.researchgate.net/publication/316284186_The_Principle_of_Transparency_in_EU_Law> accessed 11 November 2022.

9 ibid 264.

10 GH Addink, 'The Transparency Principle in the Framework of the WTO' (2009) 6(2) *Indonesian Journal of International Law* 232, 237, 239.

11 Bianchi, Peters (n 5) 5.

12 Carl-Sebastian Zoellner, 'Transparency: An Analysis of an Evolving Fundamental Principle in International Economic Law'(2006) 27(2) MICH J INT'L L 579, 627.

13 Дар'я Богатчук, 'Принцип Добросовісного Виконання Міжнародних Зобов'язань' (Дисертація на здобуття наукового ступеня кандидата юридичних наук, Інститут законодавства Верховної Ради України 2018) 55 (Daria Bohatchuk, 'Principle of Fulfilment in Good Faith of International Obligations' (DLaw thesis, Institute of Legislation of the Verkhovna Rada of Ukraine 2018) 55).

14 Henry Campbell Black and Bryan A Garner, *Black's Law Dictionary* (8th edn, Thomson West 2004) 1231.

15 Ronald Dworkin, *Taking Rights Seriously* (Harvard University Press 1977) 22.

16 Юридична Енциклопедія (ЮС Шемшученко голов ред, Інститут держави і права ім ВМ Корецького 2003) т 5, 128 (*Legal Encyclopedia* (YS Shemshuchenko ed, VM Koretsky Institute of State and Law 2003) vol 5, 128).

"generally accepted norms-ideas of the highest authority, which serve as the main foundations of legal regulation of social relations, direct their participants to establish social compromise and order".[17] The Ukrainian scholars Leonid D. Tymchenko and Valerii P. Kononenko point out that the basic principles of international law are universally recognized norms of the highest order, which form the foundation of international law and should ensure the effective and stable functioning of the international system.[18] The need to recognize certain provisions as principles is inherent in both national and international law.[19] The basic principles of international law are the foundational elements in the structure of international law. Some authors propose to see the purpose of Art. 38(1)(c) of the Statute of the International Court of Justice in ensuring that international law includes rules and principles common to all legal systems, as they form a part of the structure of "the law".[20]

7 Despite of the value-based character of the principles of law, these principles constitute basic legal rules and thus possess normative power. While transparency is considered a principle in some legal acts[21], it cannot be concluded that transparency, today, is an established principle of law that serves as a basic legal rule. Rather, transparency is seen as "developing" or "emerging" and is "usually described as if it were in statu nascendi, a potential that has not yet turned into actuality".[22] Indeed, transparency is in the process of development and transformation into a principle of law. The legal consolidation and scientific attention to transparency contribute to its establishment as a legal principle. At that, the need for transparency can be legally justified and legitimized.

8 The philosophy of law is a part of a tradition of inquiry that began with Socrates and that is characterized by a desire to understand human values.[23] Nowadays, transparency is considered as a significant public good and as an universally recognized value in the modern society (the so called "zeitgeist"[24]). A value may be defined as "a moral or ethical proposition: an abstraction, an ideal which we may believe in".[25] In general, values have a complicated relationship with virtues, which relate to personal traits and may be characterized as an "operative habit" in the language of Aquinas and a "disposition to act" in the language of Aristotle.[26] In order to show the distinction between the values and virtues authors propose the following example of dual questions: "do you believe in honesty?" (for honesty as one of the societal values) and "are you honest?" (for a virtue).[27] It may be said that it is one of the functions of law to incentivize that the virtues, i.e. the practice, correspond to the values.

9 Against this background, we can understand transparency as a value of the modern information world, a legal value in the fields of law that are directly connected with information. The legal values can

17 Ольга Ф Скакун, Теорія Права і Держави (4 вид, Правова єдність, Алерта 2014) 242 (Olga F Skakun, *Theory of Law and State* (4th edn, Pravova Yednist, Alerta 2014) 242).

18 Леонід Д Тимченко, Валерій П Кононенко, Міжнародне Право (Знання 2012) 89 (Leonid D Tymchenko, Valerii P Kononenko, *International Law* (Znannia 2012) 89).

19 Bohatchuk (n 13) 56.

20 Martin Dixon, *Textbook on International Law* (7th edn, Oxford University Press 2013) 43.

21 Under the General Data Protection Regulation (GDPR), which lays down the EU rules relating to the protection of natural persons with regard to processing of personal data, the principle of transparency is one of the basic data processing principles. Recital 58 of the GDPR explains: "The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. Such information could be provided in electronic form, for example, when addressed to the public, through a website (...)", Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1. Also in some other legal acts, transparency is considered as a principle, for example in Article 76 of the Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC, stating that "Member States shall put in place national rules (...) in order to ensure contracting authorities comply with the principles of transparency and equal treatment of economic operators", Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC [2014] OJ L094/65.

22 Bianchi, Peters (n 5) 6.

23 George Duke, *The Cambridge Companion to Natural Law Jurisprudence* (Cambridge University Press 2017) 256.

24 Bianchi, Peters (n 5) 595.

25 Rainer Hofmann, *Law Beyond the State: Pasts and Futures* (Campus Verlag 2016) 107.

26 ibid.

27 ibid.

be considered as the benchmarks or the ideals that law seeks to serve (for example, peace and security, good governance).[28] Transparency may also be a virtue, a qualitative characteristic of the information. What is so interesting about transparency is that, being a value, it is also a tool which contributes to guaranteeing adherence to other values and purposes of society.

10 Transparency is said to be subservient and instrumentally rational towards other values.[29] Transparency is a tool for the efficiency and effectiveness of the democratic legal order. It is considered as a tool for such basic legal values as participatory democracy, accountability of public authorities, good governance, the legitimacy of decision-making[30] and for the rule of law principle. Transparency is called "an indispensable element of any accountability framework".[31] At the same time, taking into consideration the circle interconnections within the legal field, transparency finds its own application through the basic values, which are needed for the effective implementation of transparency. Transparency finds its application through the human right to information, access to justice and other legal aspects. In the patent sphere, transparency may be considered as a driving force in the functioning of the patent market. At the same time, transparency is being promoted by patent rights themselves (for example, disclosing information about inventions is encouraged by patent protection).

11 Although the legal nature and functions of transparency should become an object of scientific attention in a separate work, this paper would like to contribute to the general understanding of transparency as a legal value and to assessing implementation of transparency. The following conception of transparency is, therefore, proposed.

C. Assessing Transparency

12 First of all, it is important to define what should be transparent, i.e. what is the object of transparency. Although the term "transparency" is often used with respect to institutions, procedures, facts, etc., transparency essentially aims at information. Therefore, it finds application in the areas of information flows (different data, personal and non-personal; public and private information). Transparency with respect to institutions, procedures (public authorities, decision-making), etc. also means assessing the information aspect.

13 Further, I depict the elements that allow an assessment of transparency from the theoretical point of view, as well as to gauge the implementation of transparency in practical cases.

I. Alignment with the Purposes

14 Taking into consideration the subservient character of transparency, this legal value should guarantee non-violation of the purposes of the law within the information flows. Therefore, transparency has to lead to or needs to be aligned with the purpose of the respective legal system or legal area (the main aims of the legal regulation which depend on the area; for example, in patent law that will be the purpose of the patent system). The question to be asked is whether information has been impacted by the respective subjects in a way that precludes achievement of the purpose of the legal system/area (for example, insufficient disclosure with respect to the patented invention). When dealing with the intersections of the purposes of different legal systems or legal areas involved in regulation of the relations towards information, one should aim at establishing the balance between the said purposes and should resort to the principles of law, in particular, to the so-called peremptory "jus cogens" norms that are hierarchically superior. Therefore, the implementation of transparency in respect of information should be carried out taking into account, for example, the privacy requirements applicable to such information.

15 Transparency aims at establishing a "fair balance" in the information field, in particular, through reduction of the information asymmetries between obligees and beneficiaries of information. The necessity of balancing arises from a conflict between competing rights, interests, principles, values[32] or purposes. For example, full and correct information provided by a licensee and a licensor within the license transaction reduces the information asymmetry between them.

28 Definition of the legal values has not received proper scientific attention. For consideration of the notion of the legal values, see Georg Meggle, *Actions, Norms, Values: Discussions with Georg Henrik von Wright* (De Gruyter 2011); Peter Stein, John Shand, *Legal Values in Western Society* (Edinburgh Univ Press 1974).

29 Bianchi, Peters (n 5) 5, 225.

30 ibid 8.

31 Timo Rademacher and Thomas Wischmeyer, *Regulating Artificial Intelligence* (Springer 2020) 77.

32 Massimo Durante, 'Dealing with Legal Conflicts in the Information Society. An Informational Understanding of Balancing Competing Interests' (2013) 26 Philos Technol 437, 440 <https://doi.org/10.1007/s13347-013-0105-z> accessed 11 November 2022.

Patent information, which is sufficiently disclosed in a patent application in line with transparency, also constitutes an example of reduction of the information asymmetries. The transparency obligees have a certain level of control over the relevant information.[33] The beneficiaries of transparency are the recipients/potential recipients of information who either receive information or seek it (in fact or potentially).

16 For reduction of the information asymmetries between the parties, more information may be needed. However, transparency does not automatically require greater amount of information (unless there are legislative provisions thereon), it puts forward the qualitative characteristics of information, depending on the respective legal environment. The need in reduction of the information asymmetries is not absolute and the benchmark for the extent of such reduction can again be found in the purposes of the legal systems / areas. Herewith, this benchmark serves not only for the aim of achievement of the purposes, but also for preventing requirements of disclosure of too much of information, which is not needed for achievement of these purposes.

17 Transparency, which contributes to the realization of the purposes of the legal systems and to the establishing balance, should be an essential element of all legal relations in connection to information.

II. Good Faith

18 Assessing transparency of information includes the detection of the abuse of rights, unfair practice, creating any "smoke screens", and other actions or omissions that can preclude achievement of the purposes of the legal systems. This aspect is tightly connected with good faith in behavior towards information.

19 Good faith in behavior constitutes a qualitative characteristic of the way of fulfilment of the respective obligations. Black's Law Dictionary defines "good faith" as follows: "A state of mind consisting in (1) honesty in belief or purpose, (2) faithfulness to one's duty or obligation, (3) observance of reasonable commercial standards of fair dealing in a given trade or business, or (4) absence of intent to defraud or to seek unconscionable advantage".[34] The said dictionary also proposes the definition of "bona fide": "[Latin 'in good faith'] 1. Made in good faith; without fraud or deceit. 2. Sincere; genuine".[35]

20 Good faith anticipates that the respective obligations should be performed "to the best of the ability of the party"[36], not only in accordance with the letter of the relevant stipulations, but also in accordance with their spirit.[37] Furthermore, the behavior of the obligees aimed at fulfilment of their obligations must not defeat the purpose of the legal rules stipulating these obligations.[38] Thus, for assessing the good faith aspect of transparency, it should be considered, in particular, whether the respective obligations of the transparency obligee concerning information are fulfilled at the obligee's best.

21 As a tool that ensures the quality of the respective information, transparency should be a guarantee of a good faith environment in the information world, where the choices are often made quickly based on the respective information. Transparency may be even considered as the informational dimension of bona fide, as the dimension of good faith in the sphere of information.

III. Legal Requirements of Transparency

22 A crucial role in the implementation of transparency is played by consolidation of the respective requirements in legal acts. The following legal prescriptions should be considered as the legal requirements regarding transparency:

- clearness, completeness and comprehensibility of information;
- availability and accessibility of information.

23 If the mentioned requirements are enshrined in

33 A state seems to be a classical obligee in respect of transparency. The behavior of the representatives of a state should be well regulated within the legal norms containing the levers for balancing the state powers (in particular, the transparency rules) and should be aimed, inter alia, on fulfilment of the public interest (in particular, implementation of transparency). However, the private actors can also be the transparency obligees, when they have control over information and when there are / is the recipients / recipient or the potential recipients / recipient of such information.

34 Campbell Black, Garner (n 14) 713.

35 ibid 186.

36 'Article 20. Pacta sunt servanda' (1935) 29 The American Journal of International Law 977, 981.

37 ibid.

38 II Lukashuk, 'The Principle Pacta Sunt Servanda and the Nature of Obligation Under International Law' (1989) 83(3) The American Journal of International Law 513, 515.

law, transparency should be assessed, in particular, through establishing whether the respective information fulfills these requirements.

24 In cases when the need of transparency may be assumed according to the spirit of the legal regulation or due to the peculiarities of the respective legal area, the amendments establishing the legal requirements on clearness, completeness, comprehensibility, availability and accessibility of information should be proposed.

25 Taking into consideration the important functions of transparency in the areas of information flows, further consolidation of the respective legal rules on transparency in the legal framework need to be suggested. Recognition and greater integration of transparency in legislation will effectively promote implementation of the said value.

26 Implementation of transparency, as proposed in this paper, will, of course, require additional effort and cost on the part of the transparency obligees. However, taking into account the value-based nature of transparency and its fundamental role for the realization of other societal values, the practical measures to increase transparency discussed further in the paper seem reasonable and feasible. Transparency is beneficial both to the transparency beneficiaries and the transparency obligees, as well as to society as a whole. Patent disclosure is an example of how the additional costs and efforts required from the transparency obligee (in particular, the patent applicant) for the sake of transparency of patent information result in mutual benefit to the parties. Although the patent applicant incurs additional time and resources to provide patent information that is of quality and availability consistent with transparency, the applicant also benefits from such good faith behavior, in particular from a clear establishment of the subject matter of the patent, and, therefore, a clear and reliable scope of patent protection. In turn, the transparency beneficiaries in the patent system gain access to truly valuable technological information that can be used for further innovation. All of society benefits from an environment favorable for further technological progress and good faith relations within the patent system.

D. Assessing Transparency of Disclosed Patent Information

27 The legal system of intellectual property rights allows market and non-market forces to operate for informational goods.[39] Intellectual property rights modify knowledge flows and persuade individual actors not to hide and not to deny access to knowledge.[40] Patents, for example, give the incentive to share technical knowledge with the public through filing for a patent instead of keeping it secret.[41] Disclosure of the invention to the public is a condition for obtaining a patent which grants the rights to exclusively make, use and sell the invention for a certain period of time.[42] Due to the public disclosure of the content of a patent,[43] other innovators obtain access to the most recent advances in technology and, therefore, can contribute to further improvements,[44] design around or be inspired by the invention during the patent term and use it fruitfully after the patent term expires.[45] Patent disclosure, therefore, constitutes a core tool for legal modification of information sharing within the patent system.

28 The patentee discloses the invention and the respective technical information with the legal instrument called "patent application".[46] In general, a patent application contains a request for the grant of a patent, one or more claims, a description of the invention, one or more drawings (if necessary) and an abstract,[47] but national patent laws may also

39 Dominique Guellec and Bruno van Pottelsberghe de la Potterie, *The Economics of the European Patent System: IP Policy for Innovation and Competition* (Oxford University Press 2011) 2.

40 Van Caenegem (n 2) 6.

41 Henrik Timmann and Maximilian Haedicke, *Patent Law: a Handbook on European and German Patent Law* (CH Beck 2014) 5.

42 Carlos María Correa, Peter Drahos, and Frederick M Abbott, *Emerging Markets and the World Patent Order* (Edward Elgar 2013) 62.

43 Toshiko Takenaka, *Patent Law and Theory: a Handbook of Contemporary Research* (Elgar 2008) 144-45.

44 Martin J Adelman, Randall R Rader, and Gordon P Klancnik, *Patent Law in a Nutshell* (Thomson/West 2008) 6, 189.

45 Jeanne C Fromer, 'Patent Disclosure' (2009) 94 Iowa Law Review 539, 541 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1116020> accessed 11 November 2022.

46 Nefissa Chakroun, *Patents for Development: Improved Patent Information Disclosure and Access for Incremental Innovation* (Edward Elgar Publishing 2016) 15.

47 World Intellectual Property Organization, Standing Committee on the Law of Patents, 'Dissemination of Patent Information' (SCP/13/5 2009) 2, 11 <www.wipo.int/edocs/mdocs/scp/en/scp_13/scp_13_5.pdf> accessed 11 November 2022.

contain some other requirements[48] (for example, some countries require an applicant to submit prior art information known to the applicant or to submit the information concerning the applicant's corresponding foreign applications and grants).[49] Other information relating to the patent application, for example, power of attorney, a priority claim, a declaration of inventorship, a non-prejudicial disclosure statement or a document regarding the applicant's entitlement, may be filed with the request or submitted separately, depending on the applicable law.[50] The terms used in legal acts concerning patent disclosure may differ: description, specification, claims or patent application in general. For the purposes of this paper, the term "patent information" is used for information disclosing the invention within the patenting procedure. Patent information has dual nature, being not just technical information, but also legal information about the applicable territory, the term and the scope of protection, the ownership of rights,[51] etc.

29 Published patents (and patent applications in many countries) constitute an important source of technical information.[52] However, valuable information about the inventions can also be effectively disclosed in other ways than through patents.[53] According to a theory of peripheral disclosure, technical information about the inventions can be disclosed not only in the patent document itself, but also outside the confines of the patent.[54] An author of this theory, Professor Jason Rantanen, recognizes that patents free (rather than force) inventors to share technical information and that the latter willingly share such information, but might not provide it in the absence of a patent system that retains the ability to monetize the invention.[55] In this context, patents are said to serve a crucial role in facilitating contracting[56] and provide a solution to the Arrow information paradox,[57] according to which in the absence of special legal protection, an owner cannot sell information on the open market, because the disclosure of such information within the selling process the purchaser can destroy the monopoly and reproduce the information at little or no cost.[58] Taking into consideration the criticism that relates to patents concerning their lack of useful information and their failure to transfer tacit knowledge, technological information shared about the inventions in a form other than the patent document (for example, scientific publications by patenting inventors, information shared for marketing purposes or revealed within commercialization of the invention and licensing transactions, self-disclosing inventions)[59] can form an effective supplement for promoting the progress and reinvigorating the disclosure function of the patent system.[60] Professor Colleen V. Chien argues that we need to rethink and broaden the concept of patent disclosure in order to encompass not only the content of the patent, but also its contextual information.[61] The proposed conception of transparency should cover not only patent information disclosed in the patent document, but also peripheral disclosure and disclosure of the contextual information. At the same time, the subject of this paper covers mainly patent disclosure as a part of the patenting procedure.

48 Chakroun (n 46) 15.

49 WIPO, 'Dissemination of Patent Information' (n 47) 12.

50 ibid 11.

51 WIPO, 'Dissemination of Patent Information' (n 47) 2.

52 ibid.

53 Jason Rantanen, 'Peripheral Disclosure' (2012) 74 U Pitt L Rev 1, 16.

54 ibid 6, 7, 15, 16.

55 ibid 7, 15, 16, 19.

56 Robert Merges, 'A Transactional View of Property Rights' (2005) 20 Berkeley Tech L J 1477, 1504, 1519.

57 Colleen V Chien, 'Contextualizing Patent Disclosure' (2019) 69 Vanderbilt Law Review 1849, 1871.

58 Kenneth J Arrow, 'Economic Welfare and the Allocation of Resources for Invention' in National Bureau of Economic Research, *The Rate and Direction of Inventive Activity: Economic and Social Factors* (Princeton University Press 1962) 615.

59 Rantanen (n 53) 13, 14, 16, 19, 20, 21, 23.

60 Chien (n 57) 1876.

61 ibid 1849, 1853, 1867; as Professor Colleen V. Chien states, contextual information includes (a) intrinistic characteristics of a patent regarding the number of claims, the prior art citations, the time spent in prosecution, the original owner of record, and related patents; (b) "acquired" characteristics of the patent concerning changes in patent ownership, size and other traits of the owner that entitle to pay reduced fees, investments in the patent, correction, reissue or re-examination of the patent, financing events involving the patent, citation to the patent, post-grant challenges to the patent, and licensing of the patent; (c) disclosures outside of the patent office: court disclosures, regulatory disclosures, and marking disclosures; (d) information within the international patent system, in particular, regarding where else in the world the patent is filed; (e) information outside the patent but still associated with the patent: standards that the patent is included in, commitments to license patents on royalty-free or RAND terms, patent pledges, etc., ibid 1876, 1877, 1878, 1879, 1890.

30 The patent system induces transparency through patent disclosure. Patent law then protects this transparency, as patents can be used for the legal protection of highly transparent and easy-to-comprehend subject matter.[62] The general trend of demanding greater transparency in different spheres, including the financial system, will push innovations into patenting and will increase the demand for patents.[63] At the same time, many practical problems of the patent system are connected with transparency, such as the issues of sufficiency of patent disclosure, availability of patent information in patent registers, determining inventors, etc. These controversial issues of patent law indicate that there is a lack of solid theoretical foundation for solution.

31 This paper contributes to theoretical consideration of transparency as a legal value with the purpose of improvement of its practical implementation within patent disclosure. I believe that the enhanced integration of this value into patent law will facilitate establishing due balance and finding adequate solutions to existing problems. I start by considering the purpose of the patent system as a benchmark for assessing transparency.

I. Alignment with the Purpose of the Patent System

1. Purpose of the Patent System and the Scope of Patent Disclosure

32 There are various approaches to justification of the patent system and establishing its purposes, in particular the natural rights and utilitarian theories.[64] According to the disclosure theory, which is one of the variations of the utilitarian argument, the patent system is justified on the ground that it encourages the disclosure of information about the invention in the patent document[65] by imposing a requirement of patent disclosure in exchange for the temporary monopoly (patent) granted to the inventor.[66] According to this theory, the patent system encourages the disclosure of technical information that would otherwise be kept secret.[67] At the same time, patent disclosure stimulates future innovation.[68] According to the theory of the incentive to invent justification[69], patents can be seen as a very special type of "contract", or a promise of society to inventors to grant them some exclusive patent rights if they come up with inventions[70], which would likely never have been created or would have been created at a much later time but for existence of the patent system.[71] Within the patent system, the inventor obtains control over the economic benefits from the invention and may recover research costs and accumulate funds for other innovation projects.[72] Thus, patents give the incentive for inventors and companies to invest in acquisition of inventions and to share knowledge with the public through filing for a patent.[73] The thesis that the patent system spurs investment in research[74], produces effective incentives for inventing and thereby stimulate technological progress forms the core of one of the foundational theories of the patent system and is often regarded as the fundamental economic justification of patents.[75] Fostering innovation and growth[76], encouraging the diffusion of technology through an economic mechanism can be regarded as a purpose of the patent system.[77]

33 Patent disclosure is a central tool of the patent system for encouraging further innovation. Under patent law, the scope of exclusive rights and legal protection of invention should correspond to the

62 John F Duffy and John A Squires, 'Disclosure and Financial Patents: Revealing the Invisible Hand' (Suomen Pankki 2008) 23 <www.suomenpankki.fi/globalassets/en/research/seminars-and-conferences/conferences-and-workshops/documents/cepr2008/cepr2008_duffysquires_paper.pdf> accessed 11 November 2022.

63 ibid 4, 33.

64 Guellec, Van Pottelsberghe de la Potterie (n 39) 46.

65 Rantanen (n 53) 4.

66 Guellec, Van Pottelsberghe de la Potterie (n 39) 50-51.

67 Chien (n 57) 1851.

68 Fromer (n 45) 541.

69 Rantanen (n 53) 10.

70 Guellec, Van Pottelsberghe de la Potterie (n 39) 51.

71 Rantanen (n 53) 10.

72 Adelman, Rader, Klancnik (n 44) 4.

73 Timmann, Haedicke (n 41) 5.

74 Rantanen (n 53) 10.

75 Fritz Machlup, 'An Economic Review of the Patent System' (Study of the Subcommittee on Patents, Trademarks, and Copyrights of the Committee on the Judiciary, United States Senate, US Government Printing Office 1958) 33.

76 Guellec, Van Pottelsberghe de la Potterie (n 39) 3.

77 ibid 3, 42.

scope of patent disclosure[78] and should be justified by the technical contribution to the art.[79] Pursuant to the Guidelines for Examination in the European Patent Office,"[a] fair statement of claim is one which is not so broad that it goes beyond the invention nor yet so narrow as to deprive the applicant of a just reward for the disclosure of his invention".[80] Thus, defining the minimum inventive content that justifies the grant of a patent[81] is a key issue of patent law. The conception of transparency, proposed in this paper, may contribute to solution of this issue.

34 Transparency defines the quality of the disclosed patent information. Pursuant to the transparency conception, which links disclosure of information and the purposes of the legal systems (see above)[82], the scope of patent disclosure should be such that it achieves the incentive purpose of the patent system. Therefore, the grant of a patent in exchange for the disclosure of patent information that is not sufficient to use it for further innovative activity does not correspond to transparency. The practical question of the sufficient inventive content justifying the grant of a patent[83] can also be the following: how to define the scope of disclosure that corresponds to transparency?

35 Patent information, which is sufficiently disclosed in a patent application, constitutes an example of reduction of the information asymmetries between patentees and observers[84], as well as between inventors or applicants and the patent office. According to the mentioned transparency conception, more information may be required for mitigation of the information asymmetries between the parties (see above).[85] However, increasing the quantity of the disclosed patent information does not automatically induce transparency of that information, as it does not mean that this information can be effectively used for further innovative development. Mere disclosure of the patent information does not justify the social bargain, as society shall receive something useful from the point of view of further technological progress.

36 According to the proposed transparency conception (see above),[86] information asymmetries regarding patent disclosure need to be reduced as long as this is in line with the purpose of the patent system, which is incentivizing innovations. Patent disclosure should be such that this purpose can be achieved, but there is no need in disclosure of "too much" of information. From this point of view, for example, introduction of the legal requirement of "economic enablement"[87] can't be justified by the purpose of encouraging innovations, as such requirement anticipates the scope of disclosure, which exceeds the extent that is sufficient for achievement of this purpose. Under the "economic enablement" requirement, proposed in the literature in a parallel to the technical enablement requirement, patent disclosure should include sufficient minimum of information for economical exploitation of the invention upon expiration of the patent term.[88] The said scope of disclosure, when required, may reduce innovation incentives[89] and does not seem to be suitable for incorporation in patent law.

37 Patents not only contain valuable technical information about inventions, but also cause and encourage peripheral disclosure or disclosure of contextual information shared in other ways than through patents.[90] The amount and availability of information disseminated within such non-patent sharing should be determined by the purposes of the respective legal systems or legal areas involved in regulation of the relations towards such information.

78 Adelman, Rader, Klancnik (n 44) 7.

79 T 435/91 *Detergents* [1995] OJ EPO 188, para 2.2.1; EPO, *Guidelines for Examination in the European Patent Office* (EPO 2022) pt F, ch IV, para 6.1 <www.epo.org/law-practice/legal-texts/html/guidelines/e/f_iv_6_1.htm> accessed 14 November 2011.

80 EPO, *Guidelines for Examination in the European Patent Office* (EPO 2022) pt F, ch IV, para 6.2 <www.epo.org/law-practice/legal-texts/html/guidelines/e/f_iv_6_2.htm> accessed 14 November 2011.

81 William Cornish and others, *Intellectual Property: Patents, Copyright, Trademarks and Allied Rights* (7th edn, Sweet & Maxwell 2010) 148.

82 para 14.

83 Cornish and others (n 81) 148.

84 Clarisa Long, 'Patent Signals' (2002) 69(2) *University of Chicago Law Review 625,* 627-28.

85 para 16.

86 para 16.

87 W Nicholson Price II, 'Expired Patents, Trade Secrets, and Stymied Competition' (2017) 92 Notre Dame L Rev 1611, 1613.

88 ibid 1611, 1613, 1614.

89 ibid 1632, 1633.

90 Rantanen (n 53) 6, 7, 16, 34; Chien (n 57) 1849.

2. Purpose of the Patent System and Patent Disclosure of AI

38 An alignment with the purposes in practice may be considered on the example of AI[91] being patented. AI-related inventions can be classified to the following types: (1) inventions of AI technologies that are created by humans for improvement of AI technologies themselves; (2) AI-generated inventions that are created by humans with the help of AI as a tool; (3) AI-assisted inventions that are generated by AI with possible human contribution.[92] For the purpose of this paper, I will focus on the first type of the inventions and will use the term "AI inventions" to refer to them.

39 AI systems[93] have an increasing impact on our lives, but also cause unsolved challenges to transparency and disclosure in patent law.[94] The disclosure challenge and the lack of transparency of AI is particularly connected with the difficulties to interpret and explain how AI systems operate.[95] Increasing complexity of AI models urgently raises the issue of sufficiency of disclosure of the AI inventions,[96] which anticipates the problems of unclear and incomplete disclosure of AI in patent applications, as well as the problems of very broad patent claims. In addition, more and more inventions are based on AI-generated output produced with the use of AI-based tools, but the assistance of AI in the invention process is not disclosed and due to the lack of transparency it is difficult to understand what method produced the particular output, and it may appear that it was invented by humans.[97] At that, the patent disclosure requirements also constitute challenges to innovators wishing to obtain a patent regarding AI, as within the patent prosecution process they need to disclose important details which otherwise could have been kept secret.[98]

40 In view of the social and ethical reasons for the need of more transparency in AI, the special relevance is assigned to the research for creating AI models that are able to explain themselves, or to take decisions that can be explained to people ("explainable AI").[99] In general, it should be mentioned that the patent system encourages the creation of self-disclosing inventions[100] and therefore anticipates incentives for investment in the development of explainable AI.

41 Today, the requirements within the examination of patent applications related to AI inventions differ in different jurisdictions, such as the USPTO and the European Patent Office (EPO).[101] Generally speaking, AI inventions may be patented in the EPO[102] and in the USPTO if the respective requirements are met. According to the EPO, an AI invention can be patentable in case the claimed technical features are inventive, in case AI technology is used for a technical purpose.[103] At that, the claimed AI-related features as such are not deemed to be technical (being mathematical in nature) and are considered for an inventive step only if they support a technical effect

91 In simple words, AI may be defined as "the ability of a machine to display human-like capabilities such as reasoning, learning, planning and creativity", 'What is Artificial Intelligence and How Is It Used?' (*European Parliament*, 29 March 2021) <www.europarl.europa.eu/news/en/headlines/society/20200827STO85804/what-is-artificial-intelligence-and-how-is-it-used> accessed 12 November 2022.

92 Jyh-An Lee, Reto M Hilty, and Kung-Chung Liu, *Artificial Intelligence and Intellectual Property* (1st edn, Oxford University Press 2021) 100.

93 An "AI System" can be defined as a computer environment applying AI and can also be described as "a structured contextualized combination of 'AI techniques' with the goal of attaining artificial intelligence", Alfred Früh and Dario Haux, 'Foundations of Artificial Intelligence and Machine Learning' (2022) 29 Weizenbaum Series 1, 4, 5 <https://edoc.unibas.ch/89766/1/20220912105400_631ef3a8beb27.pdf> accessed 21 November 2022.

94 Tabrez Y Ebrahim, 'Artificial Intelligence Inventions & Patent Disclosure' (2020) 125 Penn St L Rev 147, 148, 150, 153, 155, 157.

95 ibid 170, 174, 179.

96 Harm van der Heijden, 'AI Inventions and Sufficiency of Disclosure – When Enough Is Enough' (*IAM*, 3 October 2019) <www.iam-media.com/global-guide/iam-yearbook/2020/article/ai-inventions-and-sufficiency-of-disclosure-when-enough-enough> accessed 11 November 2022.

97 Ebrahim (n 94) 161, 170.

98 Clark D Asay, '*Artificial Stupidity*' (2020) 61(5) Wm & Mary L Rev 1187, 1207, 1209, 1222.

99 Matt Hervey and Matthew Lavy, *The Law of Artificial Intelligence* (1st edn, Sweet & Maxwell 2021) 297.

100 Rantanen (n 53) 31, 32.

101 Ryan N Phelan, 'A Tale of Two Jurisdictions: Sufficiency of Disclosure for Artificial Intelligence (AI) Patents in the U.S. and the EPO' (*PatentNext*, 1 November 2021) <www.patentnext.com/2021/11/a-tale-of-two-jurisdictions-sufficiency-of-disclosure-for-artificial-intelligence-patents-in-the-u-s-and-the-epo/> accessed 11 November 2022.

102 ibid.

103 Van der Heijden (n 96).

or technical goal.[104] The USPTO classifies patents relating to AI in the USPC generic class 706 "Data Processing – Artificial Intelligence".[105] The Alice/Mayo test[106], which is extensively applied in the United States, requires determination of whether (1) a fundamental AI algorithm, being a mathematical concept, can be considered as an abstract idea, which is not eligible for patenting, and then whether (2) the respective claim can still be eligible for patenting[107] in case "the claim, as a whole, integrates the recited judicial exception into a practical application of that exception".[108] In the recent report "Public Views on Artificial Intelligence and Intellectual Property Policy", the USPTO emphasizes that three disclosure requirements[109] envisaged by 35 U.S.C. § 112(a) "apply to all applications examined before the USPTO, including those directed to AI inventions".[110]

42 Under the provisions of patent law, it is necessary to disclose sufficient details[111] of the claimed AI invention, so that it can be repeatedly implemented by a person skilled in the art.[112] In view of the necessity of alignment with the purposes of the legal systems or areas under the above conception of transparency, the patent disclosure of the AI inventions should be sufficient for the potential usage of the disclosed data for further innovations. This means that the expression of AI within the patent system should adhere to the purpose of this system. Such an approach should define the vector of legislative development and the fundamental basis for an environment which is constantly challenged by new technologies. Hence, the legal requirements on the increased disclosure of AI in patents should serve the purpose of incentivizing innovations. At the same time, for example, very abstract description of the AI-related process in the patent claims may bring about very broad protection by the patent granted for such claims and, thus, stifle innovation by blocking any other use of the said process even for a different purpose.[113]

43 The following threshold of patent disclosure regarding the AI inventions may be suggested: in addition to an adequate and clear description of the basic model, either (1) a description of the method of training of the model, including a reference to the training data, or (2) every learned coefficient or weight of the trained model need to be disclosed.[114] The second option might be enough for reproducing a particular embodiment of the invention by the skilled person, however it is not enough for its improvement.[115] Thus, in order to reach the incentive purpose of the patent system, disclosure of the method of training and the training data is recommended.[116] However, disclosure of the training data of an AI invention may be complicated by the following issues: (1) very large amount of data (for example, thousands or even millions of images), which makes a proposition to include the respective datasets to the patent applications not workable; (2) a significant effort needed from an applicant to gather and (for example, in case of supervised learning) to label the training data; (3) unwillingness of the applicant to make the training data publicly available because they are deemed trade secrets and their use by competitors would be detrimental to the applicant[117]; (4) no consent to make the training data publicly available from the third parties that hold

104 ibid.

105 Lee, Hilty, Liu (n 92) 79.

106 USPTO, *2019 Revised Patent Subject Matter Eligibility Guidance* [2019] 84 FR 50 <www.govinfo.gov/content/pkg/FR-2019-01-07/pdf/2018-28282.pdf> accessed 11 November 2022 (USPTO, *Patent Eligibility Guidance*).

107 Van der Heijden (n 96).

108 USPTO, *Patent Eligibility Guidance* (n 106) 50.

109 Edwin D Garlepp, 'Disclosing AI Inventions - Part I: Identifying the Unique Disclosure Issues' (*Oblon*, 9 April 2021) <www.oblon.com/disclosing-ai-inventions-part-i-identifying-the-unique-disclosure-issues> accessed 11 November 2022.

110 USPTO, 'Public Views on Artificial Intelligence and Intellectual Property Policy' (2020) 9 <www.uspto.gov/sites/default/files/documents/USPTO_AI-Report_2020-10-07.pdf> accessed 11 November 2022.

111 According to the recent decisions of the European Patent Office's Boards of Appeal (T161/18 from May 2020, T1191/19 from May 2022), a lack of details in the description of the AI inventions as to how to carry out the invention and how AI Systems solve the respective problem, may lead to a finding of insufficient disclosure and lack of inventive step, Christopher Smith, 'Artificial Intelligence, Insufficiency and Inventive Step: Detailed Disclosure Needed at the EPO' (*Reddie&Grose*, 19 May 2022) <www.reddie.co.uk/2022/05/19/artificial-intelligence-insufficiency-and-inventive-step-detailed-disclosure-needed-at-the-epo/> accessed 13 November 2022.

112 Hervey, Lavy (n 99) 294.

113 Lee, Hilty, Liu (n 92) 353-54.

114 Van der Heijden (n 96).

115 ibid.

116 ibid.

117 ibid.

rights to such data. All these reasons contribute to the fact that patent applicants prefer to provide a description of the training method, while omitting the training data.[118]

44 There are proposals for legislative amendments envisaging a data deposit requirement or a publicly accessible repository as part of the applicant's disclosure of AI (similar to the respective legal requirements for plant seeds).[119] In this vein, the developers of machine learning products could be required not only to provide the detailed description of the training process but also to put the training data and/or the trained machine learning models into a dedicated repository.[120] Building and maintaining such training data or model repositories within the patent offices may, however, not only be difficult from a technical point of view but also be challenging because of the unwillingness of the patent applicants to give away valuable data.

45 This calls for an alternative. A patent applicant could be obliged to grant to interested third parties access to the AI's training data stored within the applicant's system, without being able to read the data in plain text, extract or copy it. The researchers, who receive access to the training data via the applicant's system, could be required to provide proper identifying information, including the identity documents and the proofs of the innovation purpose of the need in the data. Such systems for storage of the training data could base on various privacy-preserving machine learning (PPML) solutions that provide machine learning (ML) systems with privacy protection[121] and prevent data leakage in ML algorithms.[122] The recent achievements of PPML research integrate existing anonymization mechanisms into ML pipelines or design innovative new methods and architectures for preserving privacy in ML systems.[123] Further development of PPML techniques should take into account the need of data protection systems for the purpose of patent disclosure of the AI inventions. The depicted procedure for storage and usage of the AI training data[124] could balance the interests of the patent applicants with other researchers or interested third parties and satisfy the incentivizing purpose of the patent system.

II. Good Faith in Patent Disclosure

46 The requirements for disclosure of the invention are not prescribed in specific details, which allows flexibility in adaptation of patent disclosure to the nature of the invention and the needs of the technical field.[125] Thus, good faith in fulfilment of the obligations by the patent applicants and in performance of the duties by the patent examiners has a great significance in ensuring sufficient patent disclosure and the implementation of transparency in the patent system. The principle of good faith in disclosing patent information is tightly connected with transparency.

47 In particular, the following question may be considered in this context: shall the patentee bound by obligations of good faith reveal the best way of performing the respective invention at the time of a patent application?[126] The European legislation allows the patentee to provide the description which leads to a perfectly acceptable, but not necessarily optimal, version of the invention, even if the patentee knew this at the date of the application.[127] Article 29 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (the TRIPS Agreement) indicates the best mode for carrying out the invention only as a non-mandatory condition.[128] At the same time, US patent law contains an obligatory best mode requirement. This requirement prescribes dis-

118 ibid.

119 Ebrahim (n 94) 215-17.

120 W Nicholson Price II and Arti K Rai, 'Clearing Opacity Through Machine Learning' (2021) 106 Iowa L Rev 775, 800, 802 <https://ilr.law.uiowa.edu/print/volume-106-issue-2/clearing-opacity-through-machine-learning> accessed 11 November 2022.

121 Runhua Xu, Nathalie Baracaldo, and James Joshi, 'Privacy-Preserving Machine Learning: Methods, Challenges and Directions' (*arXiv*, 2021) 26 <https://arxiv.org/pdf/2108.04417.pdf> accessed 22 November 2022.

122 Dulari Bhatt, 'Privacy-Preserving in Machine Learning (PPML)' (*Analytics Vidhya*, 2022) <www.analyticsvidhya.com/blog/2022/02/privacy-preserving-in-machine-learning-ppml/> accessed 22 November 2022.

123 Xu, Baracaldo, Joshi (n 121) 3.

124 Discussion with Professor Dr. iur. Alfred Früh, Faculty of Law, University of Basel (Basel, Switzerland, 10 November 2022).

125 Tim Roberts, 'Sufficiency of Disclosure (Enabling Disclosure, Disclosure of Prior Art, Best Mode)' (*WIPO*) 5 <www.wipo.int/export/sites/www/meetings/en/2006/scp_of_ge_06/presentations/scp_of_ge_06_roberts.pdf> accessed 11 November 2022.

126 Cornish and others (n 81) 249.

127 ibid 253.

128 Chakroun (n 46) 69.

closure in the patent specification of any instrumentalities or techniques that the inventor recognized as the best way of carrying out the invention according to the inventor's subjective perception and knowledge at the filing date.[129] However, the invalidity and cancellation means of enforcement of the best mode requirement have been removed from US patent legislation.[130]

48 There has been vast critique of the best mode requirement, with the reference to the following reasons: (1) the enablement requirement already compels a full and fair disclosure of an invention; (2) the inequitable conduct doctrine already imposes penalties on a patentee for intentional concealment of material information; (3) according to the best mode requirement inventor just has to disclose the best mode known to him at the time of the application without any duty to seek out the best mode; and (4) the best mode requirement does not provide for the information on the subsequent improvements after the time of filing.[131] Other critical arguments point out that (5) the best mode requirement is an obstacle to international harmonization in the patent system and that (6) the cost of this requirement exceeds its value.[132]

49 I would argue that the disclosure of the best mode of carrying out the invention corresponds to the good faith aspect of the transparency conception, as good faith anticipates performance at one's best (see above).[133] Furthermore, the disclosure of the best way of performing the respective invention (even if it is only from the inventor's point of view) fits the purpose of the patent system. The best mode requirement, if widely accepted and implemented, will extend the predictive capacity of a person having ordinary skill in an art and innovators will need to reach farther for the next patentable invention.[134] Thus, the best mode could contribute to establishment of the level of "inventiveness" necessary for an optimal patent system which effectively incentivizes further innovations.[135]

50 The best mode disclosure seems to be a necessity, which can ensure that the patentee holds their end of the quid pro quo bargain.[136] In turn, a patentee, that does not disclose the best mode contemplated by the inventor for carrying out the invention, could obtain the exclusive patent rights while keeping a part of valuable technical information regarding the invention in secret. This does not correspond to good faith in behaviour and to the purpose of the patent system.

51 Introducing the requirements on disclosing the best method known to the inventor for performing the invention should be further considered on the international level. The best mode requirement, if implemented in a reasonable manner, helps to ensure the adequacy of the disclosure of patent information and the quality of such information.[137] Disclosing the best mode of carrying out the invention ensures the proper establishment of the patent boundaries and promotes transparency in the patent system. Based on transparency, the patent system, which functions for material expression of immaterial goods, should be able to ensure the proper expression, which does not distort the initial source and the boundaries of the patented subject matters.

52 Other examples of incentivizing good faith in behaviour of patent applicants could be mentioned. Thus, some jurisdictions (in particular, Mexico, Spain and Uruguay) require the patent applicant to provide information on known prior art in connection to necessity to understand the invention or to examine the patent claims.[138] In the USA, this obligation is described with a direct reference to good faith: "Each individual associated with the filing and prosecution of a patent application has a duty of candor and good faith in dealing with the Office, which includes a duty to disclose to the Office all information known to that individual to be material to patentability (...)".[139]

129 Adelman, Rader, Klancnik (n 44) 191, 211-12.

130 Chakroun (n 46) 89.

131 Adelman, Rader, Klancnik (n 44) 217, citing Advisory Commission on Patent Law Reform, *A Report to the Secretary of Commerce* (US 1992) 102-03.

132 Bingbin Lu, 'Best Mode Disclosure for Patent Applications: An International and Comparative Perspective' (2011) 16 J Intellec Prop Rights 409, 414.

133 para 20.

134 Lee Petherbridge and Jason Rantanen, 'In Memoriam Best Mode' (2012) 64 Stan L Rev Online 125, 129 <www.stanfordlawreview.org/wp-content/uploads/sites/3/2012/04/64-SLRO-125.pdf> accessed 24 November 2022.

135 ibid 129.

136 Alfred Früh, 'Transparency in the Patent System' in Rafał Sikorski, *Patents as an Incentive for Innovation* (Kluwer Law International 2021) 7.

137 Chakroun (n 46) 70.

138 World Intellectual Property Organization, 'WIPO Technical Study on Patent Disclosure Requirements Related to Genetic Resources and Traditional Knowledge' (UNEP/CBD/COP/7/INF/17 2004) 20 <www.wipo.int/edocs/pubdocs/en/tk/786/wipo_pub_786.pdf> accessed 28 November 2022.

139 ibid, citing 37 CFR, 1.56.

The problem to be solved is that patent examiners at the patent office do not always see and consider all of the relevant prior art.[140] For mitigation of this information asymmetry between the patentee and the patent office regarding the prior art, some authors propose to add the option of disclosing all relevant prior art in a special expanded prior art information disclosure statement that could be provided to the patent office by a patentee in exchange for a specific presumption of validity attached to the disclosed prior art (including the information on how the filed claims relate to the disclosed prior art).[141] If the patentee chooses this proposed option, a court will not invalidate the respective patent unless it is proved that no reasonable examiner would have allowed the patent in light of the disclosed prior art.[142] If the patentee does not choose the said option, the presumption of validity of the patent should be eliminated[143] and the patent office would retain the respective rights to invalidate the patent in the case of post-issuance litigation.[144]

53 In general, greater integration of the requirements on good faith in patent law will constitute an additional guarantee of achievement of the purpose of the patent system through transparency of patent information.

III. Legal Requirements to Transparency of Patent Information

1. Clearness, Completeness and Comprehensibility Requirements

54 After discussing the foundational issues regarding the patent scope in view of the purpose of the patent system and good faith aspect, it is necessary to consider the legal regulation in respect of patent disclosure as an essential element for assessing transparency of patent information. Let's consider the legal requirements of clearness, completeness, and comprehensibility of the disclosed patent information.

55 The disclosure requirement exists in the patent legislation of both the US system and the legislation of the member states of the Convention on the Grant of European Patents (European Patent Convention, EPC).

56 The European Patent Convention states as follows:

> The European patent application shall disclose the invention in a manner sufficiently clear and complete for it to be carried out by a person skilled in the art.[145]
>
> The claims shall define the matter for which protection is sought. They shall be clear and concise and be supported by the description.[146]

57 The mentioned Convention provides for the remedies to insufficient disclosure[147]:

> If the Examining Division is of the opinion that the European patent application or the invention to which it relates does not meet the requirements of this Convention, it shall refuse the application unless this Convention provides for a different legal consequence.[148]
>
> Opposition may only be filed on the grounds that: (...) the European patent does not disclose the invention in a manner sufficiently clear and complete for it to be carried out by a person skilled in the art;[149]
>
> a European patent may be revoked (...) on the grounds that: (...) the European patent does not disclose the invention in a manner sufficiently clear and complete for it to be carried out by a person skilled in the art.[150]

58 The formal requirements regarding the form and substance of the patent claims are stipulated by Rule 43[151] of the Implementing Regulations to the Convention on the Grant of European Patents.[152]

140 'Peer-to-Patent Begins Expanded Pilot' (*PatentlyJobs*, 19 October 2010) <https://patentlyo.com/jobs/2010/10/peer-to-patent-begins-expanded-pilot.html> accessed 11 November 2022.

141 Jay P Kesan, 'Carrots and Sticks to Create a Better Patent System' (2002) Illinois Law and Economics Working Papers Series 3/2002, 145, 149, 151, 155-56 <https://ssrn.com/abstract=305999> accessed 11 November 2022.

142 ibid 156.

143 ibid 151.

144 Chakroun (n 46) 73.

145 Convention on the Grant of European Patents of 5 October 1973, as revised [2001] OJ EPO 4/55, art 83 (EPC).

146 ibid art 84.

147 Früh (n 136) 3.

148 EPC, art 97(2).

149 ibid art 100(b).

150 ibid art 138(1)(b).

151 Timmann, Haedicke (n 41) 356.

152 EPO, *Implementing Regulations to the Convention on the Grant of European Patents of 5 October 1973*, as amended (EPO 2022) <www.epo.org/law-practice/legal-texts/html/

The sufficiency of disclosure is also defined in the Guidelines for Examination in the European Patent Office.[153]

59 The provisions regarding patent disclosure are also stipulated by other international legal acts, such as the Patent Cooperation Treaty (PCT), the TRIPS Agreement, the Convention on the Unification of Certain Points of Substantive Law on Patents for Invention (Strasbourg Convention).[154] The disclosure requirements are included into the national legislation. For example, the patent acts of Switzerland, Germany and the United Kingdom contain similar provisions which envisage that the patent application shall disclose the invention in a manner sufficiently clear and complete for the invention to be performed by a person skilled in the art.[155] The requirements for disclosure in the USA and in Japan[156] are stricter than the requirements under the European Patent Convention.[157] Thus, the US patent legislation stipulates the following requirements to the specification:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor or joint inventor of carrying out the invention.[158]

60 Further let's have a closer look on the rules and requirements around the patent disclosure, based on the European Patent Convention and the established practice.

61 The clearness and completeness requirements, which are envisaged in the legal provisions on patent disclosure, must ensure the ability to carry out the invention without undue experimentation by a person of ordinary skill in the art.[159] The skilled person may use the common general knowledge in the specific technical field to cure insufficiencies and errors in the disclosure in order to carry out

epc/2020/e/ma2.html> accessed 14 November 2022.

153 EPO, *Guidelines for Examination in the European Patent Office* (EPO 2022) pt F, ch III, para 1 <www.epo.org/law-practice/legal-texts/html/guidelines/e/f_iii_1.htm> accessed 14 November 2022.

154 The Patent Cooperation Treaty (PCT) sets up the following rules: "The description shall disclose the invention in a manner sufficiently clear and complete for the invention to be carried out by a person skilled in the art. (...) The claim or claims shall define the matter for which protection is sought. Claims shall be clear and concise. They shall be fully supported by the description" (arts 5, 6). Article 29 of the TRIPS Agreement envisages: "Members shall require that an applicant for a patent shall disclose the invention in a manner sufficiently clear and complete for the invention to be carried out by a person skilled in the art and may require the applicant to indicate the best mode for carrying out the invention known to the inventor at the filing date or, where priority is claimed, at the priority date of the application". The Convention on the Unification of Certain Points of Substantive Law on Patents for Invention (Strasbourg Convention) contains the following statements: "1. The patent application shall contain a description of the invention with the necessary drawings referred to therein and one or more claims defining the protection applied for. 2. The description must disclose the invention in a manner sufficiently clear and complete for it to be carried out by a person skilled in the art. 3. The extent of the protection conferred by the patent shall be determined by the terms of the claims. Nevertheless, the description and drawings shall be used to interpret the claims" (art 8).

155 In the United Kingdom, the Patents Act 1977 establishes: "The specification of an application shall disclose the invention in a manner which is clear enough and complete enough for the invention to be performed by a person skilled in the art" (s 14). Pursuant to the Swiss Federal Act on Patents for Inventions of 25 June 1954, "The invention must be described in the patent application in such a manner that it can be carried out by a person skilled in the art" (art 50, para 1). The German Patent Act (Patentgesetz, as published on 16 December 1980, as amended) contains the similar provision: "The application shall disclose the invention in a manner sufficiently clear and complete for it to be carried out by a person skilled in the art" (s 34).

156 Article 36 of the Japanese Patent Act No. 121 of 13 April 1959 contains rather broad requirements: "(...) The statement of the detailed explanation of the invention (...) must comply with each of the following items: (i) as provided by Order of the Ministry of Economy, Trade and Industry, it is clear and sufficient to enable a person ordinarily skilled in the art of the invention to work the invention; (...) The statement of the claims (...) must comply with each of the following items: (i) the invention for which the patent is sought is stated in the detailed explanation of the invention; (ii) the invention for which a patent is sought is clear; (iii) the statement for each claim is concise; and (iv) the statement is composed in accordance with Order of the Ministry of Economy, Trade and Industry", 'Patent Act' (*Japanese Law Translation*) <www.japaneselawtranslation.go.jp/en/laws/view/4097#je_ch2at13>) accessed 12 November 2022.

157 Laurence Lai and others, *Visser's Annotated European Patent Convention* (2021 edn, Wolters Kluwer 2021) 183.

158 United States Code (July 19, 1952, ch 950, 66 Stat 798; Pub L 89-83, §9, July 24, 1965, 79 Stat 261; Pub L 94-131, §7, Nov 14, 1975, 89 Stat 691; Pub L 112-29, §4(c), Sept 16, 2011, 125 Stat 296) title 35, pt II, ch 11, s 112.

159 Timmann, Haedicke (n 41) 219-20, 222-23, 232.

the invention,[160] however without an undue effort[161] and without using the documents not belonging to the common general knowledge and not referred to in the application as filed.[162]

62 As the legal provisions do not explicitly define the point(s) in time when it shall be possible for the skilled person to carry out the invention, there are continuous debates on this issue: whether it means the filing/priority date, application date, date of disclosure, date of grant or even a later point in time.[163] The legal view, according to which the disclosure of the patent application and the patent must be measured in terms of realisability at the filing/priority date,[164] seems to be well-grounded, as orientation on other point in time may cause strange situations from the resulting break in the uniform notion of disclosure.[165]

63 The sufficiency of patent disclosure depends on the claims, which define the matter for which protection is sought.[166] The clarity requirement shall ensure that a claim defines the protected subject-matter in such an accurate way that a person skilled in the art is able without any unreasonable effort, safely and clearly define what the protected subject-matter is and whether a certain embodiment falls under the claim or not.[167] The subject-matter protected by patent must be described as precisely as possible, which means that the claim's respective category shall be indicated clearly, the claim shall not contain any contradictions in terms or regarding the description, the meaning of the terms shall be clear at least from the context, and the claims shall be technically comprehensible in themselves.[168] At the same time, neither the complexity of a claim means lack of clarity, nor its simplicity is a self-contained requirement for the granting of a patent.[169]

64 The invention is disclosed sufficiently and completely, if the skilled person is able to obtain substantially all embodiments falling within the scope of the claims.[170] Sufficiency of disclosure requires that a broad claim includes in general the disclosure of a number of alternatives over the range of the claim, however, the only disclosed embodiment may be sufficient if it has the technical advantages of the invention as stated in the application and the skilled person is able to perform the invention over the whole claimed range.[171] When assessing sufficiency of disclosure, a feature of an embodiment must receive an interpretation that is meaningful for the function of the said feature to be performed, whether other interpretations shall be excluded by the skilled person as being irrelevant for working the invention.[172] In general, the claim may be considered as insufficiently disclosed, if a technical effect expressed in the claim is not achieved.[173]

65 The claims must be supported by the description[174], which typically outlines the technical field of the invention, elaborates on the background art of the invention and sets out the detailed features of the invention.[175] The description shall contain a basis for

160 Laurence Lai and others (n 157) 182, citing T 206/83 *Herbicides* [1987] OJ EPO 5, para 5.

161 Laurence Lai and others (n 157) 182, citing T 171/84 *Redox Catalyst* [1988] OJ EPO 95, para 12.

162 Laurence Lai and others (n 157) 182, citing T 580/88 (Decision of Boards of Appeal of EPO, 25 January 1990), para 2.3.

163 Timmann, Haedicke (n 41) 223-25.

164 ibid 224-25.

165 ibid 225-26.

166 EPO, *Guidelines for Examination in the European Patent Office* (EPO 2022) pt F, ch IV, para 4.1 <www.epo.org/law-practice/legal-texts/html/guidelines/e/f_iv_4_1.htm> accessed 14 November 2022.

167 Timmann, Haedicke (n 41) 356, 358.

168 ibid 357.

169 T 1020/98 *Safeners/BAYER* [2003] OJ EPO 533, hn I, para 3.5.2.

170 Laurence Lai and others (n 157) 194, citing T 226/85 *Stable Bleaches* [1988] OJ EPO 336.

171 Laurence Lai and others (n 157) 183, 194, citing EPO, *Guidelines for Examination in the European Patent Office* (EPO 2022) pt F, ch III, para 1 <www.epo.org/law-practice/legal-texts/html/guidelines/e/f_iii_1.htm> accessed 14 November 2022; EPO, *Guidelines for Examination in the European Patent Office* (EPO 2022) pt F, ch IV, para 6.3 <https://www.epo.org/law-practice/legal-texts/html/guidelines/e/f_iv_6_3.htm> accessed 14 November 2022; T 435/91 *Detergents* [1995] OJ EPO 188, para 2.2.3; T 1173/00 *Transformer with High-Temperature Superconductor for Locomotives* [2004] OJ EPO 16, para 3.1; T 409/91 *Fuel Oils* [1994] OJ EPO 653, hn, para 3; T 0595/90 *Grain Oriented Silicon Sheet* [1994] OJ EPO 695, hn II.

172 Laurence Lai and others (n 157) 182, citing T 0521/12 *Graphical Interface for Information Retrieval and Simulation/BOEING* (Decision of Boards of Appeal of EPO, 2 June 2016) para 9.

173 Laurence Lai and others (n 157) 185.

174 Cornish and others (n 81) 253.

175 WIPO, 'Dissemination of Patent Information' (n 47) 12.

the subject-matter of every claim.[176] The claims must not be broader than is justified by the extent of the description and drawings and also the contribution to the art.[177] Drawings are not always necessary for sufficient and complete disclosure of the claimed invention, but they are useful to illustrate, for example, a map of the invented object, an electronic circuit or a chemical formula.[178] An abstract, which also forms a part of a patent application, provides a concise summary of the disclosure for understanding of the general gist of the invention and is not taken into account for the purpose of interpreting the claims or determining the sufficiency of the disclosure.[179]

66 As it may be seen from the above-mentioned, both national laws and international multilateral treaties establish a set of requirements to patent disclosure. The clearness and completeness requirements to patent disclosure are directly established by the legal norms. The legal provisions regarding the sufficient scope for the implementation of the invention by a person skilled in the art can be considered as the requirement of comprehensibility. Thus, when assessing transparency of patent information, correspondence with the requirements of clearness, completeness and comprehensibility of such information should be considered.

2. Availability and Accessibility Requirements

67 According to the conception proposed in this paper, availability and accessibility of information, if enshrined in law, are among the requirements for its transparency. Patent offices, which maintain the patent registers with valuable patent information, play a crucial rule in satisfaction of these requirements within the patent system. The primary role of the patent offices is to ensure that reliable information is available in a timely manner in a usable format.[180] The availability of information, which may be found and accessed in the patent registries, supports transparency within the technology-based market and transactions in the sphere of intellectual property.[181]

68 Article 12 of the Paris Convention for the Protection of Industrial Property states that each country of the Paris Union undertakes to establish a special industrial property service and a central office for the communication to the public of patents, utility models, industrial designs, and trademarks.[182] This service shall publish an official periodical journal and shall publish regularly the names of the proprietors of patents granted, with a brief designation of the inventions patented.[183]

69 The European Patent Convention includes the following regulation concerning the European Patent Register:

> The European Patent Office shall keep a European Patent Register, in which the particulars specified in the Implementing Regulations shall be recorded. No entry shall be made in the European Patent Register before the publication of the European patent application. The European Patent Register shall be open to public inspection.[184]

70 The Implementing Regulations to the Convention on the Grant of European Patents establish data, which the European Patent Register shall contain.[185] The peculiarities of maintaining local patent registers are established on the national level in the national legal regulation and practice. In providing patent information, the patent offices follow patent information dissemination policies which differ from country to country.[186] Many national offices officially publish the bibliographic data, including name(s) and address(es) of inventor(s) and applicant(s), date and number of application(s), date and number of publication, patent classification, the title of the invention and the full text of the claims, description and abstract.[187] However, in some countries, only limited information, such as the date of the grants,

176 EPO, *Guidelines for Examination in the European Patent Office* (EPO 2022) pt F, ch IV, para 6.1 <www.epo.org/law-practice/legal-texts/html/guidelines/e/f_iv_6_1.htm> accessed 14 November 2022. See also T 409/91 *Fuel oils* [1994] OJ EPO 653, para 3.3.

177 ibid.

178 WIPO, 'Dissemination of Patent Information' (n 47) 12.

179 ibid.

180 ibid 17.

181 ibid 2, 9.

182 Paris Convention for the Protection of Industrial Property, as amended on 28 September 1979.

183 ibid art 12(2).

184 Convention on the Grant of European Patents of 5 October 1973, as revised [2001] OJ EPO 4/55, art 127.

185 EPO, *Implementing Regulations to the Convention on the Grant of European Patents of 5 October 1973*, as amended (EPO 2022) pt VII, ch IX, r 143 <www.epo.org/law-practice/legal-texts/html/epc/2020/e/ma2.html> accessed 14 November 2022.

186 WIPO, 'Dissemination of Patent Information' (n 47) 16.

187 ibid 13.

the date of filing, the names of the applicants and the title of the inventions, is published in the official publication, whereas other information, such as the full text of the claims and the description is laid open for public inspection in the patent offices.[188]

71 Difficulties in access to patent information are listed among the main problems of the patent system.[189] Authors often note that the existing public patent registers are not as helpful as they could and should be.[190] In particular, storage of patent collections only in paper form[191] instead of their availability in electronic format creates obstacles to accessibility of patent information. It can be difficult to access the information on the technical contents of patents and the status of such patents (and patent applications), particularly from abroad.[192]

72 Taking into consideration not only the letter, but also the spirit of the respective legal regulation, it can be concluded that availability and accessibility of patent information are prescribed by patent law. Hence, the respective requirements of availability and accessibility should be considered for assessing transparency of patent information in the patent registers. In turn, the necessity of alignment with the purpose of the patent system determines that the patent information stored in the patent registers should be sufficient for its usage for further innovative activity.

3. Means to Improve the Quality and Availability of Patent Information

73 One of the problems of the patent system is that the interested readers of the patent documents are often not able to obtain truly useful information from them[193] and to exploit this information for further development of innovations.[194] In practice, there are frequent cases of the abuse of the patent monopoly, when patents are granted in exchange for incomplete disclosure.[195] There are surveys, according to which the patent system and patent disclosure make hardly any positive contribution to innovation and very few innovative companies attach any value to the patent system as a source of technical information.[196] Thus, the ways of general improvement of the respective rules and practice with the aim of strengthening the quality and availability of patent information need to be considered.

74 On the whole, establishing stronger limits against vague or overly abstract claims, including the patents in software and other technologies, should be proposed.[197] The strong limits should cover the patent applications with the broadest scopes aiming at making it difficult to invent around, as well as the abuse of rights in the form of "continuing" applications, keeping claims hidden[198], and the so-called "submarine patents" (very large applications making the actual invention virtually invisible and almost unsearchable).[199]

75 There are various suggestions for incentivizing the patentees to disclose clearer and more practical patent information: (1) sending patent applications for additional "peer review", which is something similar to the procedure of getting a paper published in a scientific journal[200]; (2) involvement of experts in the relevant fields for technical comments to some parts of patent application (if such comments are required by the patent office)[201]; (3) envisaging an obligation of a patentee to respond to the good-faith questions regarding the reproducibility of the invention asked by an ordinary person (similar to the questions that could be stated to the author of the published scientific paper).[202]

76 Separate attention should be paid to the patent claim language, which should not be vague. According to the relevant European case law, "a claim cannot be

188 ibid.

189 Chakroun (n 46) 23.

190 David Vaver, 'Sprucing Up Patent Law' (2011) 23 Intellectual Property Journal 63, 70.

191 World Intellectual Property Organization, Standing Committee on the Law of Patents, 'Technical Solutions to Improve Access to, and Dissemination of, Patent Information' (SCP/14/3 2009) 12 <www.wipo.int/edocs/mdocs/scp/en/scp_14/scp_14_3.pdf> accessed 11 November 2022.

192 WIPO, 'Dissemination of Patent Information' (n 47) 3.

193 Fromer (n 45) 543.

194 Chakroun (n 46) 5.

195 Machlup (75) 32.

196 Chakroun (n 46) 22, 24.

197 James Bessen and Michael James Meurer, *Patent Failure: How Judges, Bureaucrats, and Lawyers Put Innovators at Risk* (Princeton University Press 2008) 26.

198 ibid 62.

199 Guellec, Van Pottelsberghe de la Potterie (n 39) 88.

200 Chakroun (n 46) 78.

201 ibid.

202 ibid 79.

considered clear [...] if it comprises an unclear technical feature [...] for which no unequivocal generally accepted meaning exists in the relevant art".[203] For achieving some progress on clarity of the patent claim language, the patent offices could establish glossaries of commonly used terms of claims, or specify references as authoritative sources of definitions[204] or establish a code of best practices.[205] Such a code should include definitions of the key concepts connected to patent information and explanations on the terminology for each section of the patent application.[206] AI-enabled drafting assistance software[207] could also be very helpful for clarity of patent language and for sufficiency of patent disclosure.

77 The use of blockchain, AI and other modern technologies within the patent prosecution process could contribute to transparency of the respective patent information. The researchers expect the wide use of the digitalized representation of inventions in future.[208] There are also futuristic suggestions that sufficiency of patent disclosure may be tested by or with the help of the AI tools, being fed with the patent description for further performing the claimed invention.[209] When some of the patent prosecution tests could be efficiently conducted by machines, the inventors (applicants) will be able to check the sufficiency of the claimed inventions on the stage of patent drafting and to respectively correct the draft.[210]

78 Patent offices possess the examination tools which can induce transparency in patent disclosure. There is a need of adequate disclosure review within the patent examination procedure by the examiners of the patent offices.[211] Patent attorneys, when drafting patent applications, first of all, aim at securing maximum protection and interests of their clients.[212] On one hand, full information needs to be disclosed, as the scope of disclosure defines the scope of patent protection. On the other hand, keeping some information secret or even adding misleading details may help to erect barriers for easy copying of the invention by the competitors.[213] So it is the task of the patent office to ensure transparency of the disclosed patent information according to the public interests. That is why, "[i]t is highly desirable that the principles governing disclosure should be uniform for all Patent Offices".[214] That is why it is so important to talk about transparency as a value in patent law. The special trainings for the experts of the patent offices should include values alignment and should effectively serve to improvement of the respective examination practice according to good faith. The means for incentivizing the good faith approach of the patent applicants have already been outlined in this paper (see above).[215]

79 The good governance approach of patent offices plays a prominent role also in implementation of availability and accessibility of information. For instance, the Swiss Federal Institute of Intellectual Property (IPI) on the official web-site, mentions transparency as a hallmark for its practice[216] and provides for the useful list of free online databases, where one can search for patent information as a source of inspiration (e.g., Swissreg, Espacenet, PATENTSCOPE, Patent Lens, DEPATISnet, USPTO, UK IPO, JPO database, CNIPA database, KIPO Datenbank, International Patent Classification, Cooperative Patent Classification, etc.).[217] This is a good collection of the respective sources, supported by short explanations for an average user. The Ukrainian special information system also currently provides the claims, descriptions, drawings and abstracts to the inventions online.[218]

80 Digitization of national patent collections and patent information is very much needed, as it makes possible to search and process raw data from millions of patent documents.[219] It may be suggested to establish international legal regulation, obliging

203 T 728/98 *Pure terfenadine/ALBANY* [2001] OJ EPO 319.

204 Bessen, Meurer (n 197) 239.

205 Chakroun (n 46) 82.

206 ibid 212-13.

207 Lee, Hilty, Liu (n 92) 135.

208 ibid 122.

209 Hervey, Lavy (n 99) 293.

210 Lee, Hilty, Liu (n 92) 133.

211 Fromer (n 45) 591.

212 Chakroun (n 46) 145.

213 ibid 145, 157.

214 Roberts (n 125) 5.

215 paras 49-53.

216 'The History of the IPI' (*IGE/IPI*) <www.ige.ch/en/about-us/the-history-of-the-ipi> accessed 17 November 2022.

217 'Searching for Patents Yourself' (*IGE/IPI*) <www.ige.ch/en/services/searches/patent-searches-in-general/searching-for-patents-yourself> accessed 13 November 2022.

218 See 'UANIPIO Special Information System' (*SIS*) <https://sis.ukrpatent.org/en/search/simple/> accessed 2 November 2022.

219 WIPO, 'Dissemination of Patent Information' (n 47) 7, 17.

the states to ensure online availability of the claims, descriptions, drawings and abstracts in the national patent registers.

81 There are also proposals on improvement of patent information classification (for example, classification of patent information on the basis of patent families), as well as on improvement of indexing of patent information (in particular, locating the index within the general technical databases).[220] The global application of common classification for basic legal events and setting up a minimum set of legal status data may be substantial to secure transparency of patent information.[221]

82 AI, if applied by the patent offices, could become a very helpful tool for restoring the readability of the patent registers and for transformation of the respective storages into full human inventiveness repositories.[222] There is also a need in a cross-language tool that could, with the aid of specialized dictionaries, provide the translation of patent information into different languages, as well as provide synonyms, for any keyword which has been input as a criterion for search.[223] Establishing electronic links between the patent registers and the court systems containing information on the court judgements, by which the respective administrative decisions of the patent offices are reviewed, is also desirable. Therefore, the patent information databases should be synchronized with the modern information and data processing technologies, which would increase transparency of the respective technical information.[224]

83 There are also suggestions regarding increase of availability and accessibility of contextual information (see above)[225] about the patents for promoting the technological progress—in many cases, using already existing information.[226] In particular, the accurate and up-to-date information about applicants and owners—which is recorded in the national patent registry and is available to the public—increases transparency regarding the actual ownership of patents, makes it easier to contact right holders[227] and can be helpful for technical learning from the patent.[228] However, this information is not always properly available. In fact, it is sometimes impossible to know with certainty who owns a patent.[229] This gap in patent ownership information[230] should be addressed, perhaps by introducing the respective legal requirement. Availability of, and accessibility to, the court decisions, by which the respective administrative decisions of the patent offices are reviewed, may also increase transparency and legal certainty.[231] Knowing if a patent has been previously litigated clearly has significance for the dissemination of the invention.[232] However, this information is often not properly reported.[233] Further use of modern technologies may be suggested for establishing links between the patent registers and the court systems containing information on the patent cases.

E. Conclusion and Outlook

84 Transparency constitutes a legal value, which ensures the quality of information, and may also be considered as a virtue, as a qualitative characteristic of the respective data. Transparency creates the legal environment suitable for realization of other values and purposes of the legal systems. This suitable legal environment is created by transparency, in particular, with reduction of the information asymmetries in legal relations.

85 The conception of transparency, proposed in this paper, allows one to access the content of transparency, as well as to gauge the implementation of transparency in practical cases through the following elements: (1) alignment with the purpose (assessment whether information has been impacted by the respective subjects in a way that precludes achievement of the purpose of the legal system/area); (2) good faith in fulfilment of obligations concerning information; and (3) correspondence to the legal re-

220 Fromer (n 45) 585-86; Chakroun (n 46) 124, 126-27.

221 Chakroun (n 46) 134.

222 Früh (n 136) 14.

223 WIPO, 'Dissemination of Patent Information' (n 47) 21.

224 Mindaugas Kiskis, 'Transparency for Efficiency of the International Patent System' (2014) 3(2) NTUT J of Intell Prop L and Mgmt 118, 132 <https://iip.ntut.edu.tw/var/file/92/1092/img/2036/NTUTJournal-2014-v3i2-2-Kiskis.pdf> accessed 11 November 2022.

225 para 29.

226 Chien (n 57) 1890.

227 WIPO, 'Dissemination of Patent Information' (n 47) 3, 15.

228 Chien (n 57) 1880.

229 ibid.

230 ibid.

231 WIPO, 'Dissemination of Patent Information' (n 47) 3.

232 Chien (n 57) 1881.

233 ibid.

quirements regarding transparency, which imply clearness, completeness and comprehensibility of information, as well as availability and accessibility of information.

86 The theoretical consideration of transparency as a legal value in patent law sheds new light on disputed issues of patent disclosure, such as the sufficiency of patent disclosure, the best mode requirement and the disclosure of training data when patenting AI inventions. According to the vision of transparency proposed in this paper, the scope of patent disclosure shall be determined by the purpose of the patent system, which is stimulating further innovations (and not the mere disclosure of technical information). Consequently, patent disclosure should be sufficient to be used by the inventors for further technological development. In view of this, consideration of a special system for depositing the AI's training data is suggested. Thus, a patent applicant could be obliged to grant to interested third parties access to the AI's training data stored within the applicant's system based on the PPML solutions, without being able to read the data in plain text, extract or copy it. Patent law envisages a set of requirements to the sufficiency of patent disclosure, which includes the requirements of clearness, completeness and comprehensibility, as well as the requirements of availability and accessibility of information. However, taking into consideration the general character of the legal provisions concerning patent disclosure, good faith in fulfilment of the respective obligations regarding information plays a crucial role for proper implementation of these provisions in line with transparency. Good faith anticipates, inter alia, that the respective subjects must fulfil the obligations at their best. This builds foundations for justification of the best mode requirement to disclosure of carrying out the invention, as this scope of disclosure corresponds to the good faith aspect of the transparency conception and fits the purpose of the patent system.

87 Transparency does not automatically require greater amount of information (unless there are legislative provisions), it puts forward the qualitative characteristics of information, depending on the respective legal environment. Therefore, increasing the quantity of the disclosed patent information does not automatically imply transparency of that information, as it does not mean that this information can be effectively used for further innovative activity. At the same time, patent disclosure should be minimum sufficient for the achievement of the purpose of incentivizing innovations, but there is no need in disclosure of "too much" of information. From this point of view, for example, introduction of the economic enablement requirement can't be justified, as such requirement anticipates the scope of disclosure which exceeds the extent thatis sufficient for achievement of the purpose of the patent system.

88 This paper contains various suggestions for improvement of the quality and availability of patent information with the aim of implementing transparency within the patent system. It may be concluded that transparency should be an essential element of all the legal relations in connection to information. Consolidation of the legal provisions on transparency and scientific attention to this legal value will promote its implementation and transformation into the well-established principle of law.

Platform regulation, content moderation, and AI-based filtering tools

Some reflections from the European Union

by **María Barral Martínez***

Abstract: Online platforms have voluntarily relied on screening tools for content moderation purposes for quite some time now. They do so to deal with the problems of scale and the speed content is shared online. Currently, the efforts of online platforms to fight illegal and harmful content are continuously focusing on innovative AI-based solutions for better performance of their content moderation systems. At the same time, in the EU, new rules on content moderation are entering the arena. These rules may require a more active role of online intermediaries to detect and remove illegal content in their sites. This begs the question whether we are moving towards a filtering obligation in disguise on online intermediaries. If that is the case, are AI-based filtering systems fit to avoid blocking lawful content? What safeguards should be taken at regulatory level to ensure the protection of fundamental rights of online users?

Keywords: content moderation; artificial intelligence; filtering tools; platform regulation; DSA; EU law

Recommended citation: María Barral Martínez, Platform regulation, content moderation, and AI-based filtering tools: some reflections from the European Union, 14 (2023) JIPITEC 211 para 1.

A. Introduction

1 The vast amount of digital content being uploaded and posted by users of online platforms—such as Meta, Twitter, or YouTube—is leading these companies to invest in better technologies to efficiently track and block illegal and harmful content. Until now, this has been a self-governance voluntary effort from online platforms.[1] However, in the EU, a wave of new regulatory instruments to tackle online illegal content may put service providers between a rock and a hard space.

2 Are we moving towards a *de facto* obligation on online platforms to use filtering systems in the EU? If so, are AI-based filtering systems fit to avoid blocking lawful content? What safeguards should be taken at regulatory level? In light of the EU current legal developments, this paper analyses the technological limitations and legal challenges arising from the use of AI based filtering tools in content moderation. Despite the progress made by Digital Services Act Regulation setting up transparency and accountability requirements for online platforms, there are still a few issues that deserve regulatory attention. The paper is divided as follows: the second part provides background on content moderation and algorithmic screening tools. Part C analyses the EU legal landscape impacting content moderation from current rules to future measures. In part D, the article explores the technological concerns of AI based filtering tools in an EU context-specific assessment. Finally, part E takes stock on the implications of imposing

* María Barral Martínez, Legal Counsel, LuxTust S.A., LL.M International and EU Law University of Amsterdam.

1 The term online platform is used in a broad sense to capture the different categories of internet intermediaries under the scope of analysis of the present article.

filters on online intermediaries and calls for further regulatory responses.

B. Facts and technology

3 Next to the traditional hashing, watermarking, and fingerprinting technologies for automated content recognition (ACR)[2], online service providers like Meta[3] or YouTube[4] are relying on new artificial intelligence (AI) enhanced solutions to deploy content moderation screening tools in a more efficient manner. Content moderation is the organized practice of screening user-generated content (UGC) posted to Internet sites, social media, and other online outlets, to determine the appropriateness of the content for a given site, locality, or jurisdiction[5]. In broad terms, content can be illegal, lawful but harmful—the so-called "lawful but awful" content—or go against the terms of use or community guidelines of the online service provider.

4 While moderation has traditionally been a job for humans, for reasons of scale and costs, artificial intelligence tools have been developed to help with the task. Algorithmic content moderation techniques aim at identifying, matching, predicting some piece of content on the basis of its exact properties or general features.[6] Within this context, companies usually use matching or predictive models.[7] Matching algorithms require a manual process of collating and curating individual examples of the content to be matched. Classification algorithms predict the likelihood that a previously unseen piece of content violates a rule.[8] When a piece of content is a match or is classified as content that violates a rule, the content can be flagged for review, deleted, or prevented from going online.[9]

5 Last year, YouTube released its first Copyright Transparency report providing some insight in their platform copyright enforcement actions.[10] In Meta;s latest community standards enforcement report, the social media online platform highlighted the better performance in detecting harmful content thanks to proactive detection technologies based on AI.[11]

6 Figures speak by themselves: YouTube processed 729.3 million copyright actions in the first quarter of 2021[12], Meta has acted against 905,000 pieces of content related to terrorism only over the last quarter of 2021, and Twitter removed in the first half of 2021 5.9 million pieces for violating Twitter rules.[13] According to the World Economic forum, by 2025 the amount of data created globally by humans each day will reach 463 exabytes.[14] Against this background, reliance, and investment on these technologies to detect illegal and harmful content seems the way forward to tackle such a massive amount of online content.

2 European Union Intellectual Property Office Automated content recognition: discussion paper. Phase 1, Existing technologies and their impact on IP, 2020 p. 5 <https://data.europa.eu/doi/10.2814/52085>.

3 https://ai.facebook.com/blog/the-shift-to-generalized-ai-to-better-identify-violating-content

4 Julia Alexander, "Youtube can now warn creators about copyright issues before videos are posted" *The Verge* (17 March 2021) <YouTube's new tool will warn creators if they're using copyrighted content - The Verge> accessed 08 April 2022

5 See definition at Roberts, S.T. (2022). Content Moderation. In: Schintler, L.A., McNeely, C.L. (eds) Encyclopaedia of Big Data. Springer, Cham. <https://doi-org.proxy.bnl.lu/10.1007/978-3-319-32010-6_44>.

6 Robert Gorwa et al., Algorithmic content moderation: Technical and political challenges in the automation of platform governance, Big Data & Society 2020, p.3. <https://doi.org/10.1177/2053951719897945>.

7 Nafia Chowdhury, Daphne Keller, Automated Content Moderation: A Primer, Stanford Cyber Policy Center, 2022, p.2. < FSI | Cyber - Automated Content Moderation: A Primer (stanford.edu)>.

8 Ibid, p.2.

9 Gorwa (n 6) p.6.

10 YouTube Copyright Transparency Report H1 2021 <YouTube Copyright Transparency Report H1 2021 (storage.googleapis.com)>.

11 Guy Rosen "Community Standards Enforcement Report, Fourth Quarter 2021" Meta news room (1st March 2021) <https://about.fb.com/news/2022/03/community-standards-enforcement-report-q4-2021/> accessed 8 March 2022.

12 Paul Keller "Youtube copyright transparency report: Overblocking is real" (Kluwer Copyright blog 9 December 2021) <YouTube Copyright Transparency Report: Overblocking is real - Kluwer Copyright Blog (kluweriplaw.com)> accessed 8 March 2022.

13 Twitter Transparency Report published in January 2022 available at Rules Enforcement - Twitter Transparency Center. accessed 8 March 2022.

14 Rem Darbinyan "The growing role of AI in content moderation" *Forbes* (14 June 2022) https://www.forbes.com/sites/forbestechcouncil/2022/06/14/the-growing-role-of-ai-in-content-moderation/ accessed 10 August 2022.

C. The EU legal landscape

7 Before delving into the challenges of automated filters applied to the content moderation scene in the EU, it is helpful to briefly go through the rules on illegal content online. In the EU, illegal content online is subject to two layers of regulation: at EU level, a horizontal framework and sectoral regulation for specific types of content, and then Member State national laws. Until now, the horizontal rules were set by the e-Commerce Directive, but soon the Digital Services Act (DSA)[15] will be the central piece of legislation. Sectoral rules are for example the Audiovisual Media Services Directive[16], the Directive on Copyright in a Digital Single Market (DSM Directive)[17] or the Terrorism Online Content Regulation (TERREG).[18]

I. The current horizontal framework

8 Articles 14 and 15 are the e-Commerce Directive key provisions for intermediaries' liability and content monitoring.[19] Pursuant to Article 14, intermediaries of online services are exempt from liability for content stored in their services by its users, subject to not being aware of illegal activity or information in their services, or if made aware, for example, through an injunction ordered by a Court, to expeditiously remove or to disable access to the content. Article 15 prohibits Member states to impose a general obligation on providers [...] to monitor information which they transmit or store, or actively seek facts or circumstances indicating illegal activity. In the case *Poland v Parliament*[20], Advocate General (AG) Saugmansgaard Øe regarded the prohibition enshrined in Article 15 as a general principle of law governing the internet.[21]

9 What constitutes general monitoring against specific monitoring has not been determined by the e-Commerce Directive.[22] The European Court of Justice (ECJ) explored the subject in judgments like *L'Oreal vs Ebay*[23] and *Scarlet Extended v SABAM et al.*[24], and provided some sort of guidance on what kind of content screening is allowed under Article 15 in *SABAM vs Netlog*[25] and *Glawischnig-Piesczek*[26].

10 In *SABAM vs Netlog*, SABAM—a Belgium private collective rights management organisation—sought through an injunction against Netlog, that the latter install a filtering system at their own cost to prevent copyright infringements of their repertoire. The ECJ found that preventive monitoring not compatible with Article 15.[27] The deployment of such a system, would require the social media company Netlog to carry an active monitoring of almost all the data stored relating to all of its service users.[28] In this case, the obligation to monitor was broad and too burdensome for Netlog, and it would be at odds with Netlog's freedom to conduct a business and its users right to personal data and freedom of information.[29]

15 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 (The DSA).

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

17 Directive (EU) 2019/790 of the European Parliament and of the Council 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. (*DSM Directive*).

18 Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online (*TERREG*).

19 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,2000 O.J. (L 178) 1-16 (*e-Commerce Directive*).

20 C-401/19 Republic Poland v European Parliament and of the Council of the European Union[2022] ECLI:EU:C:2022:297 (hereinafter *Poland v Parliament*).

21 C-401/19 Republic Poland v European Parliament and of the Council of the European Union [2022] ECLI:EU:C:2021:613,Opinion AG Saugmansgaard Øe, point 106.

22 Folkert Wilman, The responsibility of online intermediaries for illegal user content in the EU and the US (Edward Elgar Publishing Limited 2020).

23 C-324/09, L'Oreal v Ebay, [2011] ECLI:EU:C:2011:474

24 C-70/10 Scarlet Extended SA v SABAM [2011] ECLI:EU:C:2011:771.

25 C-360/10, Sabam v Netlog [2012] ECLI:EU:C:2012:85 (*SABAM v Netlog*)

26 C-18/18 Eva Glawischnig-Piesczek v Facebook Ireland Ltd [2019] ECLI:EU:C:2019:821 (*Glawischnig-Piesczek*)

27 Ibid 25 C-360/10, para 38.

28 Ibid.

29 Ibid paras 47-48.

11 In *Glawischnig-Piesczek*, an Austrian Court was concerned with whether an interim injunction against a host provider (Facebook), to remove a post previously declared defamatory could also extend to other posts of identical or equivalent content. Here, the Court held that the measure did not impose a general obligation to monitor within the meaning of Article 15. However, the national court order for removal of identical or equivalent defamatory content should contain "specific elements" to identify the content—targeted monitoring one could say—and in any event, it should not require an independent assessment of the content by the host provider because it will make use of automated tools.

II. New EU rules striving for a safer online environment in the Digital Single Market

12 The DSA seeks to contribute to the proper functioning of the internal market by harmonising the rules for intermediary services, such as social media networks or marketplaces, to tackle the spread of illegal content, address online disinformation, and other societal risks.

13 Articles 7 and 8 are of special interest: Article 7 shields against liability those intermediary services which in good faith and diligently [...] take measures aimed at detecting, identifying, and removing, or disabling of access to illegal content or take the necessary measures to comply with the requirements of national law, in compliance with Union law, including the requirements set out in this Regulation.

14 Article 8 contains the prohibition on general monitoring and active fact-finding, replicating the wording of Article 15 e-Commerce Directive. It is worth mentioning that throughout the legislative process, the European Parliament (EP) made an amendment to Article 8 by clarifying that there is no general obligation to screen information providers transmit and store *neither the jure nor the facto through automated or non-automated means*.[30] In addition, the EP also introduced a new limb to Article 8 stating providers of intermediary services should not be obligated to use automated tools for content moderation [...]. Both amendments, however, did not make it to the final version of the text just approved at time of writing. Article 8 now reads as follows: "no general obligation to monitor the information which providers of intermediary services transmit or store, nor actively to seek facts or circumstances indicating illegal activity shall be imposed on those providers".[31]

III. Current sectoral measures

15 In recent years, on the online content sector-specific front, several legal instruments have been passed and others are now in the pipeline of the EU legislature. These measures can target specific types of online service providers or particular categories of illegal content harmonised under EU law.[32]

16 Under the Audiovisual Media Services Directive, Article 28b requires Member States to ensure video-sharing platforms providers (VSPPs) take appropriate measures against illegal and harmful content. These measures, however, should not lead to any ex-ante control measure or upload-filtering of content contrary to Article 15 of the e-Commerce Directive.

17 The DSM Directive ignited a heated debate around its Article 17. The lengthy provision on the use of protected works by online content-sharing services providers (OCSSPs), sets out a specific liability regime for OCSSPs departing from the principle under Article 14 of the e-Commerce Directive.[33] OCSPPs can be liable for the content uploaded by its users to their services when such content infringes copyright-protected works. To escape liability for acts of communication to the public and make available to the public copyright-protected works, OCSSPs shall obtain licenses for these works or make best efforts to obtain them. In the event of no licensing agreements, OCSSPs are subject to the obligation to prevent the availability of those works in their services and to the take down and stay down of that content.[34]

18 Poland challenged the legality of Article 17 before the ECJ.[35] It argued the obligations arising from Article

30 Amendments adopted by the European Parliament on 20 January 2022 on the proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC(COM(2020)0825 – C9-0418/2020 – 2020/0361(COD))1, amendment 139-140 Article 7 of the proposal corresponding to Article 8 of the final version. Emphasis added.

31 DSA Regulation.

32 De Streel, A. et al. (2020) p.15.

33 See Recital 65 DSM Directive.

34 Article 17(4) letters (a), (b),(c) DSM Directive.

35 Ibid (n 20) Case C-401/19.

17.4[36] on OCSSPS implicitly require the use of filtering technologies to monitor content uploaded by users to prevent the infringement of copyright. In the view of the Polish government, deploying automatic filters is a serious interference on the users right to freedom of expression and information. The Court dismissed Poland's action and reasoned that even though Article 17.4 liability regime indeed imposes a limitation on the exercise of freedom of expression and information of users, Article 17 provides appropriate safeguards to preserve the essence of that right as guaranteed by Article 11 of the Charter of Fundamental Rights (CFR). Furthermore, the ECJ agreed that some filtering will be needed to comply with the mandates of Article 17.[37] Yet, as long as these filters do not screen and block lawful content when uploaded by users, their use is compatible with Article 11 CFR.

19 Since June 7, 2022, the TERREG is in force. Hosting service provides are obligated to remove or disable access to terrorist content at least within one hour of receipt of a removal order from a competent authority of any Member State.[38] Pursuant to Article 5.8, hosting service providers, when implementing specific measures[39] to address the dissemination of terrorist content in their services, are under no obligation to use automated tools. However, Recital 25 clarifies that providers should have recourse to automated tools if they consider them appropriate and necessary to address the dissemination of terrorist content online. When using automated means, providers should take appropriate measures through human oversight and verification and ensure accuracy to avoid blocking or removing content that is not terrorist related.[40]

IV. Future sectoral measures

20 More controversial is the new proposal for a Regulation fighting child sexual abuse published in early May of 2022.[41]The Regulation seeks to harmonize the requirements imposed on online services providers removing the divergences from Member States rules to prevent and combat child sexual abuse.[42] It complements the general framework of the DSA and among others, it introduces an obligation on providers to detect, report, remove and block child sexual abuse material (CSAM). Apart from the privacy and mass surveillance concerns voiced[43], the Article 10 mandate is of interest. Online service providers shall execute detection orders by national authorities by installing and operating technologies—AI systems—to detect the dissemination of CSAM, favouring systems which have been vetted by a new coordination authority, the EU Centre on Child Sexual Abuse.[44] Although the proposal explains these orders will be specific and targeted, it is not yet clear how the screening would be performed and if the current tools are effective. Some commentators warned there are no technologies available that can safely scan people's messages or discern what is abusive from what is not.[45]

D. AI-based filtering for content moderation: technological concerns

21 Online platforms are filters only in the way that trawler fishing boats "filter" the ocean: they do not monitor what goes into the ocean, they can only sift through small parts at a time, and they cannot guarantee that they are catching everything, or that they are not filtering out what should stay.[46]

36 Ibid para 24.

37 Ibid para 54.

38 Article 3(3) TERREG

39 Article 5 TERREG.

40 Article 5(3) and Recital 24 TERREG.

41 Proposal for a regulation to prevent and combat child sexual abuse (COM (2022) 209 2022/0155 (COD) (*CSAM proposal)*

42 Both providers of hosting services and providers of interpersonal communication services.

43 James Vicent "New Eu rules would require chat apps to scan private messages for child abuse" (The Verge 11 May 2022) <https://www.theverge.com/2022/5/11/23066683/eu-child-abuse-grooming-scanning-messaging-apps-break-encryption-fearsv > and Mathieu Pollet "children first, privacy second" (Euroactiv 270502022) <https://www.euractiv.com/section/digital/podcast/csam-proposal-children-first-privacy-second/>.

44 Ibid 28 Article 10 CSAM proposal.

45 Mathieu Pollet "CSAM proposal: children first, privacy second?" *Euroactiv* (27 May 2002) <https://www.euractiv.com/section/digital/podcast/csam-proposal-children-first-privacy-second/> (accessed 09 September 2022) and https://edri.org/our-work/private-and-secure-communications-put-at-risk-by-european-commissions-latest-proposal/.

46 Gillespie Tarleton, Custodians of the internet: Platforms, content moderation, and the hidden decisions that shape social media (Yale University Press 2018) p.87.

22 The use of filtering solutions can lead to over-blocking patterns by online service providers. In other words, lawful content which should in principle be allowed online, can risk being caught by a filter, be flagged or removed. Some authors have already signalled the limits of automated systems and the challenges posed by false positives.[47] Others argued there will always be a need for human intervention for the content to be appropriately screened.[48] This is partly because filtering technologies have a problem with content contextualization, they are able to detect certain content but not infringing content *per se*.[49] As a result, a piece of content that can be illegal in certain circumstances, may not be if used in a different context.[50]

I. Training the algorithm: context, human bias, and accuracy challenges

23 For the efficient deployment of a filtering system in content moderation, the premise is that the system will work with clear and defined parameters of what constitutes illegal or harmful content. The first challenge in this respect is to define the nature of the content and work backwards—i.e., why a post can be labelled as hate speech, or what is hate speech for that matter. In AI terms, this would consist in training the model with data sets to teach the system to recognize on its own the targeted illegal content. In this process, the quality of the data fed to the system will be key. Automatic detection can assess only what it can know and what can be represented as data, but limited to the data it has.[51] In addition, algorithms can be subject to human bias during the AI training process. Human bias can take place in both machine-supervised learning and non-supervised learning processes. In the former, human intervention is needed to evaluate data examples and select the appropriate labels or to evaluate an automatically applied labels.[52] In the later, hidden biases could arise from the dataset itself.[53]

24 Further, considering these technologies are context insensitive and unable to make subjective decisions[54] there are certain bars at technical level. Although some context can be incorporated in a tool, historical, political, and cultural context are more difficult for an AI system to be trained to detect.[55] As Spoerri points out, the state-of-the-art of filtering technologies is quite limited as tools are only capable of matching content, but it is not yet possible to determine whether the use of a file—be it music, text or image—constitutes an infringement.[56] Despite this situation, the EU legislator seems to assume that online service providers can employ intelligent filters that identify infringing content while enabling the upload and making available of lawful content.[57]

25 Against this background, the ECJ in C-401/19 warned that where a filtering system does not adequately distinguish between lawful and unlawful content, leading to blocking of lawful content, the system is not compatible with the right to freedom of expression in Article 11 CFR.[58]

26 Yet, there is no infallible filtering system able to make such a clear distinction.[59] For that reason, the focus should be put on the accuracy of these tools. Accuracy in this context can be defined as the rate

47 Christophe Geiger and Bernd Justin Jütte, Platform Liability Under Article 17 of the Copyright in the Digital Single Market Directive, Automated Filtering and Fundamental Rights: An Impossible Match, PIJIP/TLS Research Paper Series no. 64, 2021 p.36.

48 Sarah T Roberts, Behind the screen: Content moderation in the shadows of social media. (Yale University Press 2019) p. 35.

49 Ibid 21 AG Saugmansgaard Øe Opinion in *Poland v Parliament* at point 148.

50 Giovanni Sartor,Andrea Loreggia, The impact of algorithms for online content filtering or moderation: upload filters. European Parliament, Directorate-General for Internal Policies of the Union, (2020) p.46. <https://data.europa.eu/doi/10.2861/824506p>.

51 Gillespie, (n 46) p.105.

52 Emma Llansó et Al., Artificial intelligence,content moderation,and Freedom of expression, Working, Transatlantic working group, paper series, 2020, p.8 <doi:https://doi.org/10.1177/2053951720920686>.

53 Althaf Marsoof, Andrés Luco, Harry Tan & Shafiq Joty, Content-filtering AI systems–limitations, challenges and regulatory approaches, Information & Communications Technology Law, 2022 p.16.

54 Geiger and Jutte, (n 47) p.36 and Santa Clara Principles 2.0 Open Consultation Report (accesed 24 August 2022)

55 Ibid 52 Llansó.

56 Thomas Spoerri, On Upload-Filters and other Competitive Advantages for Big Tech Companies under Article 17 of the Directive on Copyright in the Digital Single Market, 10, JIPITEC, 2019 pp 173-186, p.182 at 35.

57 Ibid Geiger and Jutte (no 47) p.36.

58 Ibid (n 20) *Poland v Parliament* para 86.

59 Spoerri (note 56) p.182 at 34.

at which the tool's evaluation of content matches a human's evaluation of the same content.[60] The results can be divided into four categories: true positives, true negatives, false positives, and false negatives.[61] This begs for the question how many false positives or false negatives are acceptable to not fall in over-blocking patterns threatening users' rights. Perhaps, certain standards should be set for the development and use of filtering technologies within this sphere, and improvements of filtering tools should focus on bringing these mistakes within an acceptable range.[62] What is acceptable would depend on analysing the content and harm at stake. Trade-offs in this regard are unavoidable[63]—a balance between leaving false negatives online and blocking lawful content should be achieved. At any rate, predictability of the systems should be guaranteed as well as mechanisms to correct the potential mistakes.

27 In the EU, another layer of complexity exists; the regulation of illegal content categories is not entirely harmonized at Union level[64] so the same type of content may be considered illegal, legal but harmful, or legal and not harmful across the 27 Member States.[65] This is reflected in the broad definition of illegal content enshrined in the DSA[66] "illegal content means any information, which, in itself or in relation to an activity, including the sale of products or the provision of services, is not in compliance with Union law or the law of any Member State, irrespective of the precise subject matter or nature of that law".

28 Therefore, online service providers deploying filtering systems need to consider that for those categories of illegal content not harmonized at EU level, tailor-made filters for specific jurisdictions within the EU need to be implemented. For larger online services providers operating worldwide, having to deal with different degrees of requirements across the globe or even with conflicting rules is already the case. This forces them to operate their compliance content policy and enforcement programmes based on global rules and adjust them through a risk-level approach. One should question then, if the risk of non-compliance comports fines as those established by the DSA[67], online service providers would not be prone to self-censorship/over-removal for the sake of compliance, paying little heed to the fundamental rights of its users.

II. The need for human review

29 The difficulties of screening tools to consider language and social/cultural context evidences the gap between the capabilities of a human and that of machines. The high rate of false positives and the removal of lawful content resulting from automated screening emphasize the added value of human moderation. It is for this reason that the inclusion of human review at some stage of the moderation chain should be a requirement to safeguard users' fundamental rights. Typically, human review can take place when content is reported by a user and a decision needs to be made by the online service provider on the content flagged. Similarly, filters can serve to flag content by the platform own initiative and subsequently be reviewed by a moderator. Moreover, although most online platforms follow a "publish-then-filter approach"[68] human review can happen either before the content is online or after it is published.[69]

30 If human content moderators are excluded entirely from the screening process, it will be the automated system deciding which content stays online or is taken down. Still, reviewing every piece of content caught by a filter as a potential infraction of the law or from the online service provider TOUs, would defeat the purpose of using content screening systems by the online service providers, rendering the content moderation exercise not feasible.

60 Emma Llansó, No amount of "AI" in content moderation will solve filtering's prior-restraint problem. Big Data & Society, 7(1) 2020, p.4.<doi:https://doi.org/10.1177/2053951720920686p4>.

61 Sartor and Loreggia (n 50) p. 45.

62 Llansó, (n 60) p 4.

63 Federal Trade Commission Report to Congress: Combatting Online Harms Through Innovation, June 2022 available at Combatting Online Harms Through Innovation; Federal Trade Commission Report to Congress (ftc.gov) p. 41.

64 De Streel, A. et al., Online Platforms' Moderation of Illegal Content Online, Study for the committee on Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg, 2020. <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652718/IPOL_STU(2020)652718_EN.pdf> p.16.

65 See Ibid De Steel, p.16. and for example The German law on Hate Speech, NetzDG (2017) < BMJ | Netzwerkdurchsetzungsgesetz>.

66 Article (3)(g) DSA.

67 See Article 52.3 and 74 DSA.

68 ibid 51 p.75.

69 Roberts (n 48) 33.

31 To that extent, the ELI principles on automated decision making[70] proposed an ex-post content human review after a decision has been taken by automated means and challenged by the user. To put it simply, users who posted/uploaded a piece of content which was afterwards blocked or removed should have access to a redress mechanism to challenge the decision requiring human review. In that sense, human review guarantees full compliance with applicable law without relinquishing the benefits of automation.[71] However, such an approach does not resolve the issue of users being at the mercy of online platforms and their internal dispute settlement mechanisms at first instance, forcing them to rely on them regardless the content disputed was lawful from the outset. An issue that fuels the debate on the role of these platforms acting as delegated enforcers of public powers vis-à-vis online users' freedom of expression and due process rights.[72]

32 But what is EU law position on human review? Although the outcomes of non-compliance with a human review requirement remain to be seen, references to human review or human intervention can be found in different EU legal acts.[73] As an illustration, under the General Data Protection Regulation (GDPR)[74], data subjects have the right not to be subject to a decision based solely on automated processing without human intervention.[75]

33 Some of the above-mentioned new rules introduce provisions on the inclusion of human review when using filtering technologies. The TERREG mandates hosting service providers to include human oversight and **verification safeguards** when using technological measures to protect its services against the dissemination to the public of terrorist content, to ensure accuracy and to avoid the removal of material that is not terrorist content.[76] In the same fashion, the proposal on CSAM establishes that providers should ensure regular human oversight and where necessary, **intervention**, to ensure technologies operate in a sufficiently reliable manner. Even more, when detecting potential errors and potential solicitation of children.[77] In the case of the DSA Regulation, Article 20(6) requires that decisions on removal/block of allegedly illegal content or content incompatible with the platform T&Cs, are reviewed by qualified staff and are not solely taken on the basis of automated means.[78]Therefore, the human review requirement comes within the context of the complaint handling system. This is, ex post, when the online service provider receives a complaint by a user of the platform.

34 Lastly, the ECJ had the opportunity to provide some precisions on human review while using automated filters through *Glawischnig-Piesczek* and *Poland v Parliament*. In the first judgement, the Court was of the view that a hosting service provider is not under the obligation to include human review—"an independent assessment" in the Court's words—when using automated filtering technologies to comply with a removal order by a national court. In the second case, the Court held in similar terms that OCSSPs are not obliged to conduct an independent assessment of the content uploaded by their users to prevent the uploading or making available to the public of copyright-protected works, in the light of the information provided by the rightsholders and of any exceptions and limitations to copyright.[79]

35 This approach, however, seems difficult to conjugate with the rules discussed above and creates different standards for human review depending on the type of content at stake and on the subject requesting the removal. Even if human review in such situations

70 De las Heras Ballell, Teresa, ELI Innovation Paper on Guiding Principles for Automated Decision-Making in the EU, European Law Institute (2022). < ELI Innovation Paper on Guiding Principles for Automated Decision-Making in the EU by European Law Institute, TERESA RODRIGUEZ DE LAS HERAS BALLELL:: SSRN>.

71 Ibid.

72 For a more detailed discussion see Martin Husovec, Ir) Responsible Legislature? Speech Risks under the EU's Rules on Delegated Digital Enforcement (2021) <https://dx.doi.org/10.2139/ssrn.3784149> and Víctor Javier Vázquez Alonso, The «private» censorship of large digital corporations and the emerging system of freedom of expression, Teoría y Derecho, no 32, Tirant, (2022) pp 108-129.

73 Codagnone, C. et Al., Identification and assessment of existing and draft EU legislation in the digital field, Study for the special committee on Artificial Intelligence in a Digital Age (AIDA), Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg (2022) p.61.

74 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC O.J. L 119 1-88. (*GDPR*).

75 Article 22 and to Recital 71 GDPR.

76 Article 5(3) (d) *in fine* TERREG.

77 Article 10(4) (c) and Recital 28 CSAM proposal.

78 Article 20(6) and Recital 45 DSA.

79 Ibid 20 case Poland v Parliament para 90.

is not required by law, in all likelihood AI based filters will match/block ambiguous content or lawful content when searching for the objectionable content. This is particularly relevant in the case of the copyright exceptions and the rights of content creators to use protected works without the prior authorisation of rightsholders. Essentially, this implies that someone whose lawful content was removed due to a filter mistake would have to go through the complaint handling system of the provider to challenge the removal. Only then human review would be required per Article 17(9) DSM. With this set up by default, the balance tilts towards the right to intellectual property vis-à-vis the freedom of expression and creation of users, placing a heavy burden on non-professional creators and user-generated content.[80]

36 Although online service providers could of course still decide to rely on human review[81] for those cases, even platforms that use filters and human review are incentivized to remove legal "grey area" content.[82]

E. AI based filters for content moderation are here to stay, so what is next?

I. Towards a filtering obligation on online intermediaries?

37 For reasons of scalability, speed, and cost-efficiency, online service providers will keep relying on AI based filtering solutions on voluntarily basis to tackle illegal or harmful content.[83] Thus, the key question is no longer whether to rely on AI based systems to screen content, but whether automated content screening is turning into an obligation in disguise for online platforms and if so, how could it be articulated with online intermediaries' liability exemption and their fundamental rights, namely, their freedom to conduct a business.

38 Looking at Article 7 DSA and other sector-specific rules, one observes a trend of the EU legislator to require a more active role of online service providers to tackle illegal content.[84] In fact, the use of automated filtering systems seems a *de facto* must for online intermediaries to escape liability, especially in cases where short removal time is required. Recital 26 of the DSA sheds light on the scope of Article 7 DSA voluntary measures of providers to conduct investigations and actions for the detection, identification, removal or disable access to illegal content. It clarifies the requirements of conducting such activities "in good faith" and "in a diligent manner" by also stating that if the provider uses automated tools for those purposes, it should take reasonable measures to ensure the technology is sufficiently reliable to limit to the maximum extent possible the rate of errors. There are still some open questions, how the error rate could be measured, if a threshold should be established, or what happens if the filter fails to detect illegal content despite the intermediary voluntary actions. Would this "bad" filter engage the liability of a provider conducting voluntary measures to fight illegal content? A reading of Recital 22 tells us that to benefit from the exemption of liability, the provider, upon obtaining actual knowledge or awareness of illegal content, needs to act expeditiously to remove or to disable access to that content, and that knowledge of the illegal nature of the content can be obtained through own-initiative investigations.

39 In this regard, the case *Delfi AS v. Estonia*[85] of the European Court of Human Rights (ECtHR) is quite insightful. This Court found the liability imposed by the Estonian Supreme Court to an online news portal operator for defamatory comments made in their site by third parties, did not violate the applicant freedom of expression. The Court noted that Delfi's filtering system in question failed to detect the harmful comment and left it online for some weeks.[86] This amounted to not having taken reasonable measures to remove the comments without delay. In such a circumstance, the Court found the liability on the online news operator to be a proportionate restriction on the applicant`s right to freedom of expression.

40 Looking at the case from another perspective, one could also ask if requiring an online service provider to deploy a filtering system to look for

80 Giancarlo Frosio and Sunimal Mendis, Monitoring and Filtering European Reform or Global Trend? in Giancarlo Frosio (ed), The Oxford Handbook of Online Intermediary Liability (Oxford University Press 2020) p.28.

81 Daphne Keller, Facebook Filters, Fundamental Rights, and the CJEU's Glawischnig-Piesczek Ruling, GRUR International, June 2020 Volume 69, Issue 6, pp 616–623 p.621.

82 Ibid.

83 See for example, Meta transparency statement on how Meta prioritises content for review at: < https://transparency.fb.com/en-gb/policies/improving/prioritizing-content-review/>(accessed 15 July 2022)

84 Ibid (n 50) p.59.

85 Delfi A S v. Estonia App no. 64569/09 (EctHR, 16 06 2015).

86 Ibid para. 156 - 159.

illegal content or manifestly illegal content is a proportionate restriction to its freedom to conduct a business under Article 16 of the CFR. The answer would depend among other things, on the size of the internet intermediary and its resources. Thus, a liability obligation of that sort would create differences between the market players. As Frosio and Geiger flagged, the economic impact of enforcing filtering and monitoring obligations on online service providers has been discussed in the case-law of the ECJ, in particular, in *Netlog v. SABAM* where the Court held that imposing a monitoring obligation on Netlog to screen all works uploaded would burden the online service provider with the requirement of installing at its own expense filtering technologies.[87]

II. What regulation?

41 The DSA renders online services providers accountable through algorithmic transparency and reporting obligations including disclosure obligations on metrics for notices processed by automated means, any use of automated means for the purpose of content moderation, and information on the type of content moderation engaged by providers of online services.[88] Furthermore, the Regulation provides for procedural measures for users to dispute content blocking or removals of information labelled as illegal content or against the ToUs of the platform.[89]

42 While these measures purport a robust layer of protection for online users' fundamental rights, the fact remains that AI based filtering tools are far from being perfect and the technical challenges of these tools cannot be resolved only with transparency obligations on online intermediaries. There are issues that are yet to be addressed: the algorithmic fairness and human bias on data sets, accuracy standards since for certain type of content, a higher rate of accuracy may be easier to achieve[90], although that would not be the case when context is an intrinsic factor for determining illegality of a piece of content. In addition, it should not be assumed that online intermediaries are best placed to assess the legality or illegality of content, and they should not be seen as neutral when making such decisions.[91] With that in mind, there will always be "grey zone" cases which would require human judgement rather than an AI based system taking a decision.[92] It is particularly in those situations where online intermediaries may feel compelled to over-block to not risk liability.

43 If despite the flaws, we take AI based filters as a "necessary evil" for content moderation, then, closer regulatory scrutiny should be paid to their design, implementation, and the consequences of their use on public speech and the fundamental rights of online users but also the role and responsibilities of online intermediaries. To that end, data sets to build automated AI systems should be documented and traceable.[93] Guidelines on content moderation automated systems, including accuracy and error thresholds could be adopted to complement the DSA. Human review should continue to be an essential component of moderating with filters. Some authors postulate that automated decision-making processes should be subject to the "human-in-command" principle, namely, human intervention to supervise the overall activity of the AI system, its impact, and the ability to decide when and how to use the system.[94] By the same token, there should be clear accountability, liability, and redress mechanisms to deal with potential harm resulting from using applications, automated decision-making and machine learning tools.[95] Other propositions advocate for AI ethical principles specific for content filtering[96] which could form part of a regulatory framework to ensure compliance and enforceability. Such a framework should include the setting up of

87 Giancarlo Frosio, and Christophe Geiger, Taking Fundamental Rights Seriously in the Digital Services Act's Platform Liability Regime. European Law Journal (forthcoming 2022) p.30 <http://dx.doi.org/10.2139/ssrn.3747756>.

88 Article 15, 24, and the provisions addressed to very large platforms (VLOPs) read in conjunction with Recital 39.

89 Articles 20 & 21 DSA.

90 Sartor and Loreggia (n 50) p.56.

91 Guidance note on content moderation, adopted by the Steering Committee for Media and Information Society (CDMSI) at its 19th plenary meeting, Council of Europe 19-21 May 2021 p.13.

92 Ibid (n 90) p.57.

93 André Tambiama Madiega, EU guidelines on ethics in artificial intelligence: Context and implementation, European Parliamentary Research Service, (2019) p.4. < EU guidelines on ethics in artificial intelligence: Context and implementation (europa.eu)>.

94 Frosio and Geiger (n 87) p.43.

95 Ibid. Moreover, with the new proposal for an AI liability Directive, it is to be seen how this liability regime could apply to the use AI tools in the context of content moderation. See Proposal for a Directive of the European Parliament and the Council on adapting civil liability rules to artificial intelligence.<IMMC.COM%282022%29496%20final.ENG.xhtml.1_EN_ACT_part1_v10.docx (europa.eu)>

96 Marsoof et al. (n 53) p.22.

mandatory certification standards for testing AI systems to ensure they meet minimal safety and accuracy requirements.[97] This is in line with the approach of the EU Artificial intelligence Act (AIA).[98] The proposal sets a horizontal legal framework for the development, placement on the market, and use of AI applications in the Union, based on a risk-based approach. Under the current form of the proposal, there is no specific reference to AI systems for content moderation purposes. However, it has been argued that the AIA could be the right place to regulate the use of upload filters.[99]

44 As a closing remark, one should also not lose sight of technological innovation to question if other options to automated tools managed by online platforms are possible. In its report on combating online harms through innovation, the American Federal Trade Commission listed user tools in its recommendations to tackle harmful content.[100] These tools could help users to control what content they see on the internet, shifting the content moderation effort from private platforms towards users. This is the idea of the so-called middleware for content moderation services. Middleware in this context, is a software program that rides on top of an existing internet or social media platform such as Google, Facebook or Twitter and can modify the presentation of underlying data.[101] Middleware can be understood as a layer between the user and the online platform. By relying on this software, users could control their experience in a relevant platform but at the same time have the option to interact with other users of the online platform.[102] The development of these tools is still at a very early stage, and for now aimed mainly to the specifics of legal but harmful content. Nevertheless, there is room to consider if similar AI initiatives could provide effective alternatives to automated filters for fighting illegal content.

F. Conclusion

45 AI based filtering tools have become an integral part of content moderation. Although these technologies have been used until now as voluntary measure to fight illegal and harmful content, the new EU regulatory framework may be implicitly requiring online platforms to rely on them to escape liability. The EU legislator should not ignore the technical developments in the field and the current practices in content moderation carried out by online intermediaries, albeit regulatory efforts must ensure that the benefits of deploying and using these technologies to fight illegal and harmful content are not hampering the fundamental rights of online users. Accordingly, further guidance on human intervention and what entails human review should be provided. AI-based filtering tools should be designed, developed, and deployed when they meet certain safety and quality performance criteria. Accuracy standards and error rate thresholds must be established to ensure predictability and most importantly, a clear role responsibility and a reparation framework should be established to enable online users to seek redress from harms arising from the malfunction of filters.

97 Ibid p.28.

98 Proposal for a Regulation laying down harmonised rules on artificial intelligence, COM/21/206 FINAL (2021/0106(COD))

99 See for example Martin Husovec, *Euroactiv* "Internet filters do not infringe freedom of expression if they work well. But will they?" (2 May 2022) <Internet filters do not infringe freedom of expression if they work well. But will they? – EURACTIV.com> accessed 14July 2022.

100 Federal Trade Commission Report to Congress: Combatting Online Harms Through Innovation, June 2022 <Combatting Online Harms Through Innovation; Federal Trade Commission Report to Congress (ftc.gov)>.

101 Katharine Miller "Radical proposal:,Middleware could give consumers choices over what they see online" Stanford University (20 October 2021) <https://hai.stanford.edu/news/radical-proposal-middleware-could-give-consumers-choices-over-what-they-see-online> accessed 24 August 2022.

102 Daphne Keller (Blogpost The University of Chicago Law Review Online. 28 07 2022) Lawful but Awful? Control over Legal Speech by Platforms, Governments, and Internet Users – The University of Chicago Law Review Online (uchicago.edu).

ALLEA Statement on Open Access Publication Under "Big Deals" and the new Copyright Rules

by **The European Federation of Academies of Sciences and Humanities***

Recommended citation: ALLEA, Statement on Open Access Publication Under "Big Deals" and the new Copyright Rules, 17 (2023) JIPITEC 222 para 1.

A. The increasing costs of publication under the Gold Open Access model and "Big Deals"

1 The European Federation of Academies of Sciences and Humanities (ALLEA) has for many years supported the move away from proprietary models of scientific publishing towards Open Access (OA).[1] OA publication of publicly funded scientific research bears the triple promise of (1) fostering access to published research and knowledge by researchers, and the general public, all over the world; (2) recognising that outputs derived from publicly funded research are essentially a public good; and (3) reducing the mounting costs of accessing published research for universities and other academic institutions.

2 ALLEA, therefore, welcomes recent studies showing that OA publication in scientific journals is on the rise.[2] An important driver of this development is the so-called "Big Deals"; "read and publish agreements" that have been negotiated in recent years between (consortia of) research libraries, institutions, and universities on the one hand, and scientific publishers on the other. These agreements, also known as "transformative agreements", have replaced the subscription deals that were previously agreed between research libraries and publishers, and which provided for large bundles of subscriptions to proprietary journals to be made available electronically to libraries and their affiliated researchers.[3]

3 The new generation of deals is "transformative" in that they additionally allow for OA publication under the "Gold" standard of (usually a finite number of) research articles by institution-affiliated researchers in return for payment of substantial "article processing charges" (APCs)[3] that allow publishers to recoup their investment in OA publication.

* short: ALLEA; This statement was originally published on ALLEA's website on 12 December 2022 (doi.org/10.26356/BIGDEALS).

1 See, for example: https://allea.org/portfolio-item/allea-response-to-plan-s/; https://allea.org/portfolio-item/ethical-aspects-of-open-access-a-windy-road/; https://allea.org/portfolio-item/allea-statement-on-enhancement-of-open-access-to-scientific-publications-in-europe/

2 Zhang, L., Wei, Y., Huang, Y. et al. "Should open access lead to closed research? The trends towards paying to perform research". Scientometrics (2022): https://doi.org/10.1007/s11192-022-04407-5.

3 European University Association "2019 Big Deals Survey Report - An Updated Mapping of Major Scholarly Publishing Contracts in Europe" (2019): https://eua.eu/downloads/content/2019%20big%20deals%20report%20v2.pdf

4 As a recent study demonstrates, commercial publishers currently derive more than two billion USD annually from Author Processing Charges (APCs).[2] Despite gradually decreasing subscription revenues, the commercial publishers have managed to embrace the Gold OA model without compromising their total revenues and enormous profit margins. Evidently, Gold OA publishing has become a new, highly profitable business model in and of itself,[2] in addition to the subscription model which has remained partially intact. Incorporating Gold OA publication into all-encompassing read and publish agreements has thus allowed the major commercial publishers to effectively consolidate and enhance their already dominant position in the field of scholarly publishing,[4] solidifying their role as the gatekeepers of publicly funded research.[5]

5 While the rising number of Gold OA publications facilitated by these deals is to be applauded, they do not deliver on the triple promise of OA. In particular, they have not led to a reduction in the exorbitant costs to the academic community incurred in the process of research publication. While the downstream costs of journal subscriptions are gradually falling, the upstream costs of publication, made up of the APCs, have risen sharply.

6 Concomitantly, the imposition of APCs has created new, and sometimes insurmountable, barriers to publication for researchers that are not affiliated to a contracting institution.[6] In addition, as already underlined in previous ALLEA Statements,[6,7] the Gold OA model creates a disadvantage for those coming from less wealthy countries and institutions, under-funded researchers in the social sciences and humanities, and early career researchers, among others. For these academics, OA of published research comes at the expense of closure of first-tier publication fora.

7 In addition, ALLEA is concerned that the conditions of the "Big Deals" that drive these developments do not adequately reflect the rules on copyright law in the European Union (EU) and fail to fairly value the creative and research endeavours of researchers and their institutions, as well as their investment and efforts over time to generate research results and publications to the benefit of the public.

B. The new copyright rules relevant to "Big Deals"

8 Under the law of copyright, the authors of works of science are the copyright owners of their published articles. Unless these rights are contractually assigned or licensed, it is for the authors, and the institutions that employ them (not for the publishers), to determine the conditions under which their works are to be published, reproduced, and otherwise used (including by way of OA).

9 In current practice, authors are expected to assign or exclusively license their copyright to publishers. Under the new rules of the 2019 Directive on Copyright in the Digital Single Market, which have been recently implemented in most EU Member States, authors that license or assign their rights "for the exploitation of their works" are entitled to receive appropriate and proportionate remuneration,[8a] except where they have granted OA licences.[8b] Ordinary publishing contracts between authors and publishers on which the "Big Deals" largely rely, however, rarely, if ever, provide for such remuneration. To the contrary, researchers or their institutions are expected to remunerate the publishers through APCs for having their scientific research published.

10 In addition, various EU Directives allow Member States to provide for limitations and exceptions to copyright for the purpose of scientific research. For example, EU law allows Member States to exempt the reproduction and making available of works "for the sole purpose of illustration for teaching or scientific research, as long as the source, including the author's name, is indicated, unless this turns out to be impossible and to the extent justified by the non-commercial purpose to be achieved".[9a] While not all Member States have implemented this provision, and modalities of implementation

4 Frontiers. "It is not transformation if nothing changes" (2022): https://blog.frontiersin.org/wp-content/uploads/2022/06/Frontiers_transformative_agreements_whitepaper_2022.pdf.

5 European Commission - DG for Research and Innovation "Study on EU copyright and related rights and access to and reuse of scientific publications, including open access" (2022): https://op.europa.eu/en/publication-detail/-/publication/884062d5-1145-11ed-8fa0-01aa75ed71a1/.

6 ALLEA "Statement on Equity in Open Access" (2021): https://allea.org/portfolio-item/equity-in-open-access/.

7 ALLEA "Statement on Enhancement of Open Access to Scientific Publications in Europe" (2013): https://allea.org/portfolio-item/allea-statement-on-enhancement-of-open-access-to-scientific-publications-in-europe/.

8 (a) Art. 18, (b) Recital 74 and (c) Art.3 of the Directive on Copyright in the Digital Single Market, 2019/790: https://eur-lex.europa.eu/eli/dir/2019/790/oj.

9 (a) Art. 5(3)a, (b) Art. 5(3)d and (c) Art. 5(3)n of the Information Society Directive, 2001/29/EC: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32001L0029.

vary,[5,10] downloading and sharing of articles for the purpose of conducting or producing scientific research is permitted without authorisation in many EU Member States. Where such limitations and exceptions exist, publishers that have acquired the copyrights may not subject the downloading of articles by researchers to licensing conditions and payment of licence fees, as the European Court of Justice (ECJ) has clarified in its case law.[11]

11 Other relevant limitations and exceptions in EU law permit the use of "quotations for purposes such as criticism or review"[9b] and the making available of articles on dedicated terminals in library networks.[5,9c] Moreover, the 2019 Directive on Copyright in the Digital Single Market requires EU Member States to grant non-profit research institutions broad freedoms to reproduce works for the purpose of "text and data mining".[8c] Accordingly, publishers may not restrict or condition text and data mining from scientific journals to which the researchers have lawful access.

12 Additionally, an increasing number of Member States (e.g., Germany, Netherlands, Austria, France, and Belgium) have introduced special rules permitting researchers to reproduce and make available published articles in non-profit repositories, regardless of having transferred their rights to publishers.[12] These so-called Secondary Publication Rights allow authors of scientific works that are the product of fully or partially publicly funded research to provide Open Access to their articles, following the expiry of a variable embargo period set by national legislation or good practices.[5] National rules vary as well in respect of the version of the article that is subject to the Secondary Publication Right. While some countries limit the right to the Author Accepted Manuscript, the law in other countries seems to extend the right to the printed version, the so-called Version of Record. In all countries, the right is limited to articles; entire monographs and other scholarly books are therefore excluded.[5]

13 While ALLEA applauds the introduction of these new rights, we believe that, with the accelerated pace of scientific output and the need to adequately respond to today's societal challenges, embargo periods are unnecessary impediments to the timely dissemination of publicly funded research. Today, as recently underlined in a Guidance of the White House Office of Science and Technology Policy (OSTP) of 25 August 2022,[13] research that is made "widely available to other researchers and the public (...) can save lives, provide policymakers with the tools to make critical decisions, and drive more equitable outcomes", and therefore "there should be no delay or barrier" for the research outcomes to be made available to the public which has funded this research. ALLEA agrees, and therefore favours copyright rules that allow for OA publication of (partially) publicly funded research with immediate access and no embargo.

14 While EU and national copyright laws provide for a variety of rules intended to facilitate the free use and sharing of scientific works, without the need to compensate copyright holders, the current "Big Deals" do not generally factor in these statutory free uses.

15 Admittedly, the value added to the scientific article during its journey from submission to final publication is the result of a review and editing process that deserves financial reward. However, much if not most of this work (such as peer-reviewing and journal editing) is outsourced by the publishers to members of the academic community directly affiliated to institutions that are also parties to the agreements. To better judge the added value provided by publishers, there is a need for greater transparency on the pricing of journal publishing services and fees, and developments like the cOAlition S "Journal Comparison Service" are to be welcomed.[14]

16 All in all, it is difficult to see why an overall licensing agreement between research institutions representing the authors of thousands of publicly funded works, allowing affiliated researchers to publish and access the products of their own research or their fellow researchers' endeavours, would justify payment of "read and publish" fees in the order of magnitude of the present "Big Deals".

10 Knowledge Rights 21 "A Position Statement from Knowledge Rights 21 on Secondary Publishing Rights" (2022): https://www.knowledgerights21.org/wp-content/uploads/2022/10/Secondary-Publishing-Rights-Position-Paper.pdf.

11 Court of Justice of the European Union: Judgement of 27 June 2013, C-457/11 (VG Wort), ECLI:EU:C:2013:426. https://ipcuria.eu/case?reference=C-457/11.

12 ALLEA "Supplementary Statement on Enhancement of Open Access to Scientific Publications in Europe" (2015): https://allea.org/portfolio-item/supplementary-statement-on-enhancement-of-open-access-to-scientific-publications-in-europe/.

13 OSTP Issues Guidance to Make Federally Funded Research Freely Available Without Delay: https://www.whitehouse.gov/ostp/news-updates/2022/08/25/ostp-issues-guidance-to-make-federally-funded-research-freely-available-without-delay/.

14 cOAlition S - Journal Comparison Service: https://www.coalition-s.org/journal-comparison-service/.

C. Recommendations

1. Negotiate future deals considering national and EU copyright law.

17 Now that the first generation of "Big Deals" is soon to expire, ALLEA recommends that research institutes and affiliated authors reconsider the terms of these agreements. In particular, ALLEA advises negotiators on the part of the research community to better leverage the rights and limitations accorded to authors and research institutions under national and EU copyright law, in order to further enhance the possibilities of (immediate) OA publication and substantially reduce the costs of APCs and journal subscriptions. ALLEA is concerned that if researchers perceive present and future "Big Deals" as vehicles that further strengthen and enrich the scientific publishing oligopoly, their willingness to permit OA publishing will dissipate.

2. Move away from the current rights assignment models.

18 Future "Big Deals" should pave the way for a future of scientific publishing where publicly funded research is freely available from multiple competing platforms, whether operated for profit or not-for-profit, including platforms operated by the research community itself.[15] Therefore, future deals with scientific publishers should depart from the rights assignment model that still prevails today. Rather than forcing authors to individually negotiate with publishers, universities, and other research institutions might consider reserving certain rights in employee-produced publications to themselves, for example, by way of (collectively bargained) labour agreements. In addition, funding organisations should ensure that all researchers participating in the research they fund commit to publishing the research outcomes under an OA model that does not impose APCs or embargos.

3. Harmonise EU legislation to allow publication of post-print versions without embargo.

19 ALLEA recommends that national legislatures follow the example of an increasing number of European states in providing for Secondary Publication Rights that give researchers the right to make the post-print version (i.e., the Version of Record) of articles that are the product of fully and partially publicly funded research available in public repositories without embargo. Authors of scholarly books, scholarly book chapters, and edited research books should also be encouraged to publish their work in OA where reasonably possible. Ideally, such Secondary Publication Rights should be harmonised and made mandatory at the EU level.[5,10] In doing so, the EU would set an important step towards operationalizing the 2018 European Commission Recommendation, which advised that all scientific publications resulting from publicly funded research be available OA by 2020,[16] while refraining from creating new barriers for authors. Additionally, with a view to international collaborations that go beyond the EU, further efforts should be made to harmonise Secondary Publication Rights globally.

4. Develop a sustainable non-profit publishing ecosystem.

20 Finally, ALLEA recommends that research institutions and funding organisations prioritise the development of a sustainable non-profit publishing ecosystem that allows for OA of scientific publications without imposing undue financial barriers to publication, and that prevents scarce financial resources from being syphoned off by the private sector.[3] The development of community-driven journals that charge no fees to authors and readers (Diamond OA) are an important contribution to a more equitable publishing landscape and an enrichment in bibliodiversity. ALLEA therefore welcomes and supports the Action Plan for Diamond Open Access that was published in March 2022.[17]

About ALLEA

ALLEA is the European Federation of Academies of Sciences and Humanities, representing more than 50 academies from over 40 countries in Europe. Since its foundation in 1994, ALLEA speaks out on behalf of its members on the European and international stages, promotes science as a global public good, and facilitates scientific collaboration across borders and disciplines. Learn more: www.allea.org

About this Statement

This ALLEA statement has been prepared by ALLEA's Permanent Working Group on IPR, with Prof P. Bernt Hugenholtz as principal author. Through its Working and Expert Groups, ALLEA provides input on behalf of European academies to pressing societal, scientific, and science-policy debates

15 For example, Latin America has demonstrated for many years that an OA system based around federated institutional repositories works very well, and inspiration should be drawn from initiatives like Redalyc and SciELO.

16 European Commission Recommendation on access to and preservation of scientific information, 2018/790. https://eur-lex.europa.eu/eli/reco/2018/790/oj.

17 Science Europe, cOAlition S, OPERAS, and the French National Research Agency (ANR). "Action Plan for Diamond Open Access" (2022): https://www.scienceeurope.org/media/t3jgyo3u/202203-diamond-oa-action-plan.pdf.

and their underlying legislations. With its work, ALLEA seeks to ensure that science and research in Europe can excel and serve the interests of society. Read more about the ALLEA Permanent Working Group on IPR and its members: https://allea.org/intellectual-property-rights/

Kai-Niklas Knüppel (ed.), Data financed apps as a matter of data protection law, 2022, 417 p.

by **Oliver Vettermann,** Scientific Co-Worker, FIZ Karlsruhe, Intellectual property rights in distributed information infrastructures

Book Review

Recommended citation: Oliver Vettermann, Data financed apps as a matter of data protection law, 14 (2023) JIPITEC 227 para 1.

I.

The smartphone is now not only the memory and companion of day-to-day activities, but also the main object for datafication of everyday life. It feels like there is an application for every problem in our daily lives, which leads to a large number of installed apps. Most of the apps are free of charge—but at what cost? Usage data is regularly analyzed and sooner or later exploited. Even if the exact value of one's own (personal) data is debatable, it remains obvious when looking at microtargeting and real-time bidding in the advertising sector that free applications are being financed by the usage data or entered data of the users. Knüppel's work—"Data Financed Apps As a Matter of Data Protection Law"—is devoted to a classification of such applications in the applicable data protection law from a legal perspective.

The analysis is divided into three parts. Part 1 defines basic terms such as the property of data financing, followed by a detailed discussion of data protection law *de lege lata* and the classification of data-financed apps in Part 2. Part 3 then takes a look at the conclusions from Part 2 and develops them into reform ideas *de lege ferenda*.

II.

Accordingly, Chapter 1 introduces the methodology and course of the analysis. The existence of the thesis is justified by the fact that there is a lack of consideration of data-financed apps from different perspectives; previous works have only dealt with the topic sporadically. Thus, to a certain extent, the thesis or the editor aims at a meta-analysis of the topic area. Chapter 2 is dedicated to the definition of data-financed services by presenting the process of data financing with examples. This type of financing is dissected based on the value of the data and a legal description of the value in the Digital Content Directive (EU) 2019/770.

Methodologically, the procedure seems comprehensible. The chapter sets the foundation for the further investigation and is intended to introduce readers to the author's understanding of the term. However, it is problematic that the author biases the conceptual definition with his premise: Data is money. For the author, both terms seem almost synonymous, which can be seen in several places in chapter 2. According to the author, the quantity and coding of the data are not relevant; what matters is the content alone (p. 40). This concept overlooks the fact that it is certainly of value for the evaluation whether the data are enriched or simple. Also, whether the information is encrypted can have an impact when trading data. Why individual personal data should have "no separate value" (p. 41) is similarly not clear. These characteristics are relevant at least for the risk assessment in the sense of the risk-based approach of the GDPR, making it interesting to draw a parallel here.

Furthermore, the author attempts to scale possible data protection risks on the basis of his own categories or to prepare them for further investigation. Yet this, too, is only moderately successful and rather superficial. Knüppel apparently tries to separate "free" models from freemium models or even paid applications by means of a clear categorization and a binary approach. In the context of the thesis, data-financed offerings are exclusively applications that "require registration or some other form of personalization" (p. 38). Therefore, he excludes applications without a collection of user data (p. 39). In this way, the author thinks predominantly in binary terms—every free app is a data-funded app, and vice versa. Border cases such as the freemium model, which switches advertising in free mode or is intended to persuade users to buy the upgrade, are omitted by the author. The paid model is also omitted, as the author assumes that every application with a monetary counter value also covers all development and maintenance costs. In practice, however, this already proves to be a misguided approach when the change from one-time financing to the subscription or freemium model tends to increase and successively displaces the one-time payment. In addition, there is the deficient indication that registration is always required: According to the author, the data is of particular relevance when using a search engine (p. 43). However, this regularly functions without registration, so it would not be a "data-financed offer". If other criteria in the chapter are taken into account, such as the type of collection and use, the correlation with Big Data, and the profiling by means of cookies or other identifying parameters, it is precisely such an application in the sense of the doctoral thesis. It is completely incomprehensible why the author does not take the opportunity to confront his thesis of data funding with the Commission's elaborated view in the Digital Content Directive. The author merely states that, according to the Directive, data cannot be equated with money; it is protected by fundamental rights and thus cannot be regarded as a commodity (p. 56). Without criticism, the author continues to adopt and apply his term. Why the Directive assumes that personal data are now "made available" seems not clear to the author. The reason for this is that a few pages earlier, the problem of freedom from costs at the level of awareness of the users is only touched upon. A provision includes that users provide the data voluntarily and self-determined; this presupposes an action in knowledge. Simply treating data as money would neglect the core of human dignity of informational self-determination. Similarly, the European legislator seeks to avoid this (see also Buttarelli, Opinion 4/2017, pp. 3, 6). Chapter 2 thus moves on the surface in terms of content without addressing problematic cornerstones of its own definition. This seems understandable, because otherwise the framework of the work would fall apart. Nevertheless, the definition seems unstable in this respect.

Chapter 3 is primarily concerned with a civil law classification in order to highlight the special features of data-financed apps. The main focus is on the constellation in the triangular relationship between user, app store, and app manufacturer/developer. It is shown that the users regularly conclude the contract with the developers or companies; the respective store is only an intermediary that acts as a commercial agent. This seems to make sense insofar as this could be relevant for the assessment as jointly responsible persons or processors. Nevertheless, the comments on the TMG are not purposeful; references to the TTDSG should have been made sub specie after a classification in the construct of the GDPR. The rejection of the DSA seems reasonable; for the sake of completeness, the DGA could also have been excluded—app stores are not to be understood as intermediary services as defined by the DGA, after all.

Chapter 4, with its rather illustrative nature, introduces Part 2 of the thesis and provides an overview of constitutional or primary as well as secondary data protection law. In addition to the aforementioned detailed overview, the author presents which fundamental rights apply to data processors, i.e., Big Data analysts. In the abstract, he concludes that entrepreneurial freedoms such as fundamental communication rights, in addition to the subsidiary freedom of action, can be considered under both national and Union law. These conclusions are then anchored in a consideration of the constitutional court's assessment through the Right to be Forgotten I and II decisions. The author concludes that the economic and data protection interests are diametrically opposed. This would be reinforced by the privacy paradox.

In chapters 5 and 6, the author focuses on the basic requirements for data processing under the GDPR. Chapter 5 is therefore addressed to the general data protection principles of Article 5 GDPR and applies them steadily to the subject of the analysis: data-financed services. The approach appears differentiated overall, but remains substantively on the surface. The conclusion that there is a close connection between the degree of complexity of data processing and compliance with data protection principles, which becomes more difficult with increasing complexity, follows almost logically from the risk-based approach of the GDPR. Indeed, the author is able to illustrate this in a predominantly comprehensible manner using the object of investigation. In some cases, however, the author draws hasty conclusions. If a processing is incompatible with the purpose of collection, this cannot steadily lead to a change of purpose; if only because it is not intended for all cases according to Article 6 (4) of the GDPR, but only for certain purposes or processing bases of Article 6 (1) of the GDPR. Similarly, a steadily assumed nexus between Big Data and data-funded offerings runs through the work. According to the author, the broad concept of data-financed offerings includes both non-personal and personal data. Big Data—especially the aspect of marketing purposes, which is often used in the thesis—refers to personal data for the purpose of microtargeting or similar methods that lead to real-time bidding. The author does not see the

conclusion that not every data-financed app is part of Big Data and that, as a result, it is not necessary to constantly draw on Big Data. Further, he overlooks the scope of the definition of Big Data by excluding statistical purposes—whereas the cited BITKOM already includes these purposes in 2015. Thus, the chapter predominantly presents itself as a summary of existing teachings and content on the principles of the GDPR.

As mentioned, chapter 6 analyzes the usual legal bases for data-financed offers—namely the contractual basis of Article 6(1)(b) GDPR, the legitimate interest of lit. f and, to a large extent, the consent of lit. a. The contractual basis of Article 6(1)(b) GDPR is the only legal basis for data-financed offers. In this context, Knüppel comes to the conclusion that the contractual basis represents a narrow *synallagma*, since the necessity of the data processing for the fulfillment of the contract ties the framework tightly. Data financing arising from advertising use or the analysis of personality profiles would therefore not be permissible as a direct obligation to perform in order to receive the app use as a service in return. If making the app available free of charge always specified or presupposed the type of service in the form of the data, the necessity principle of Article 6(1)(b) GDPR would be undermined. In terms of content, the contractual use of personal data could relate exclusively to the scope of functions (p. 229). It is fundamentally easier to base data financing on legitimate interests pursuant to Article 6(1)(f) of the GDPR. However, in Knüppel's view, the comprehensive weighing of interests in individual cases leads to a similar result: personal data must be limited to the functional scope for business reasons and in consideration of informational self-determination. For long-term storage, subsequent use or disclosure to third parties, a case-by-case assessment is required, in which the impairment via collection or processing may only be of minor extent. Interestingly, Knüppel brings up informed consent as a subsidiary instrument and examines the justification ground after analyzing potential legitimate interests. In doing so, he recurs to the possible breadth of the object of consent and the independence from a case-by-case examination as in the context of Article 6(1)(f) GDPR. Accordingly, the details of consent (i.e., voluntariness, informedness, etc.) and possible problems due to revocability or in GTC-like data protection declarations are introduced and commented on in detail. In the context of the prohibition of tying, the author concludes, after a detailed analysis of the state of the dispute, to understand the necessity of Art. 7(4) more broadly in terms of content than that of Art. 6(1)(b) GDPR. According to Knüppel, a performance with a contractual character in a consent situation should therefore have a relation to the subject matter of consent to the main performance obligation or consideration (pp. 272, 273). According to this, data financing is possible as a main performance in exchange for consideration; the concepts of necessity for contract and consent are not to be equated (p. 276). In a classic free app situation, however, this conclusion does not seem entirely mature: if the user and the manufacturer of a free app conclude a usage contract, this is probably to be classified as a contract according to lit. b. Knüppel presumes that this is not the case. Rarely—as the author correctly recognizes in the analysis of data protection declarations—will a declaration identify data utilization as a performance. Consent is mostly given later, during or with the start of use, and is located in declarations as a secondary purpose or without a direct link between performance (based on consent) and consideration. Thus, the advertising use and the contractually based exchange of the app are adjacent or superimposed. The two justifications start to blur and it is hardly possible to differentiate. This supports Knüppel's view that, with a view to Section 327q (2) of the German Civil Code (BGB) as the implementation of Directive EU 2019/770, the app manufacturer's obligation to perform also ceases to apply when consent is revoked. Thus, Knüppel elevates the consent relationship to a quasi-*synallagma*. Justification via consent is thus clearly to be read in a liberal context in the context of the thesis.

Part 2 concludes with a presentation of problems arising from the cross-border data processing of data-financed apps, which could occur in all variants of the categories of apps listed by the author. Materially, the legal requirements and the consequences of the *Schrems II* decision are presented in detail. However, with respect to the subject matter of the study, there are no notable differences from the details of the decision.

The previously rather general chapters on general concepts in data privacy law and a classification of data-funded apps *de lege lata* are followed by a consideration *de lege ferenda*. Chapter 8 deals in detail with maintaining the existing level of data protection despite the liberal view taken in the thesis. To this end, legislative as well as practical measures are proposed: one possibility would be to contrast the data-financed usage models with a monetary and collection-free model (p. 348 ff). Even though the author does not name the term, he refers to existing freemium models in terms of the basic idea. Whether this is more likely to be solved by a direct (objective) obligation of the manufacturers or a subjective claim of the users against the manufacturer is left open. However, regulatory implementation seems to be difficult, among other things, and tends to be rejected because it would generate an increasing effort in programming ("considerable additional costs", p. 358). Small and medium-sized companies and app manufacturers would not be able to cope with this (p. 355). Then, however, the question would also have to be asked whether the app manufacturer of the data-financed application did not deliberately overlook the technical reading of data minimization or storage limitation from the very beginning. In addition, the argument of the size of the company hardly holds water, also in view of current plans of the European Union—in such cases, exemptions for small and medium-sized companies are regularly provided for. The author sees the strengthening of transparency as a further point of

contact *de lege ferenda*. It is true that suitable means and approaches are available with the multi-layer approach and mouseover effects. The discussed one-pager solution therefore also seems plausible. In addition, however, explanations could be provided with image icons that pick up on the regulation of Art. 12 (7) GDPR. Various proposals (e.g., EU Parliament, PrimeLife research project) are discussed in detail. As a result, both the picture symbols and structural solution approaches can only be a tool and make existing information obligations from Articles 13 and 14 GDPR more accessible. The fundamental challenge of directing and maintaining awareness to the information remains.

III.

Knüppel succeeds in creating an overview for the data protection law consideration of data-financed apps. The reader is then provided with a mental map for the regulations *de lege lata*, which, however, leaves "white spots" in view of the discussion points mentioned. The potential for more in-depth coverage could be exploited by further work, especially in the consideration *de lege ferenda*.

JIPITEC

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

www.jipitec.eu