jipitec

2 | 2024

Volume 15(2024)
Issue 2 ISSN 2190-3387

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

www.jipitec.eu

2024

jipitec

Journal of Intellectual Property, Information Technology and Electronic Commerce Law

Volume 15 Issue 2 August 2024
www.jipitec.eu
contact@jipitec.eu

A joint publication of:

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

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

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

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

ISSN 2190-3387

Funded by
DGRI Deutsche Gesellschaft für Recht und Informatik e.V.

Table Of Contents

Editorial

Articles

Editorial

by **Karin Sein**

Recommended citation: Karin Sein, Editorial, 15 (2024) JIPITEC 100 para 1.

1 During the preparation of this issue, a legislative cycle has come to an end in the European Union. Recent legislative advances, including the Digital Services Act, the Data Act and the Artificial Intelligence Act, aim to promote a secure, competitive and innovative digital ecosystem in Europe, while seeking to ensure that technological progress is consistent with fundamental rights and ethical standards. The importance of the new rules for the digital economy cannot be overstated: companies operating in digital sectors must comply with new transparency and accountability measures, facilitate data sharing, and implement risk assessment and management processes.

2 JIPITEC tries to keep pace with these rapid legislative changes, and this issue will provide insights into several highly topical legal issues. We start with the latest legislative milestone: very recently, on 1 August 2024, the world's first comprehensive regulation of artificial intelligence - the Artificial Intelligence Act - came into force. While legal issues related to AI have been explored several times in JIPITEC, in this issue Hanjo Hamann looks at web-scraping for AI training, providing an interdisciplinary insight into human-machine communication protocols. He argues that only some of these protocols qualify as "machine-readable" under Article 4(3) of the DSM Copyright Directive, which governs the text and data mining exception.

3 The following two articles identify different shortcomings in the new Data Act that will become applicable only in a year. First, Daniel Gill argues that the Data Act fails to open up the automotive aftermarket to innovative third-party services due to a number of general and sector-specific application problems and offers policy recommendations for a sectoral data access regime. Second, Daria Kim and Man Wai Kwok focus on data usability as a legal parameter delineating the scope of data access rights and show that different concepts used for the technical state of data are too vague and lead to uncertainties regarding the scope of data-sharing obligations.

4 Next, Matteo Frigeri, Martin Kretschmer, and Péter Mezei tackle the (lack of) digital exhaustion in the context of eLending by public libraries and assess that there are few lawful avenues to obtain access to digital copies for eLending purposes. To meet the informational needs of modern societies, they propose several alternatives, ranging from judicial intervention to the introduction of the concept of book altruism.

5 The last two articles offer a critical analysis of the judgments of the Court of Justice of the European Union concerning digitalisation from the perspective of fundamental rights. Valentina Golunova and Mariolina Eliantonio ask about the role of civil society actors as enforcers of the GDPR in the proceedings before the Court and regret their limited influence. Finally, Evangelia Psychogiopoulou examines the development of the Court's case law on data retention, describing the Court's sophisticated attempts to strike a balance between citizens' fundamental rights and the protection of national security in the absence of EU legislative intervention.

6 “A rolling stone gathers no moss”. JIPITEC is indeed rolling, as we have launched a new channel for interacting with our readers. On 15 May, we hosted the first joint DGRI-JIPITEC webinar on the transatlantic perspective of the Data Act, with speakers providing insights into the legal landscape of data sharing in the EU, US and Canada. The fact that we ran out of time before the flow of questions was over shows the continued interest in digital law and the need to meet again. In the meantime, enjoy reading this summer edition!

Karin Sein

Tallinn, 2024

Artificial Intelligence and the Law of Machine-Readability

A Review of Human-to-Machine Communication Protocols and their (In)Compatibility with Article 4(3) of the Copyright DSM Directive

by **Hanjo Hamann** *

Abstract: Many legal scholars critique the supposed ineffectiveness of European copyright regulation regarding commercial text and data mining. At the same time, tech-savvy entrepreneurs keep proposing new standards to effectuate them at a rate that has been described as "exponential". The present paper reconciles these complementary perspectives. In the first (doctrinal) part, it develops a framework for article 4(3) of the Copyright DSM Directive by arguing that: (1) Web-scraping for AI training is a use case of TDM. (2) European TDM regulation seeks to protect fundamental rights and to uphold incentives of both AI developers and rightholders. (3) To ensure balanced protection, the legislator provided for a "reservation of rights" as an exception similar to one found in the Berne Convention. (4) This reservation instrument gets criticized on account of being either unduly effective or largely ineffective – a tie that can only be broken by clarifying the doctrinal hurdles raised by the Directive. (5) The Directive establishes two standards that reservations need to fulfil simultaneously: They must be explicit (specific for a given content and use) and automatable (employing a well-defined technical protocol). In the second half of the paper, it uses these standards to assess seven communication protocols commonly proposed to reserve TDM rights. It concludes that only some qualify as "machine-readable" in a legal sense at all, and that the proliferation of standards currently precludes any effective reservation of TDM rights. This may, however, come with a silver lining.

Keywords: AI web-scraping, text and data mining, machine-readability, rights reservation, H2M communication

Recommended citation: Hanjo Hamann, Artificial Intelligence and the Law of Machine-Readability: A Review of Human-to-Machine Communication Protocols and their (In)Compatibility with Article 4(3) of the Copyright DSM Directive, 15 (2024) JIPITEC 102 para 1.

* Prof. Dr. Dr., JSM (Stanford), assistant professor for civil law, commercial and intellectual property law, in particular the law of digitalisation and legal linguistics, at the Wiesbaden University of Business and Law (EBS Law School). The basic argument of this paper was presented at Humboldt University in Berlin (19 June 2023) and at a conference on "Generative AI Through the Lens of Copyright Law" that I co-hosted with Katharina de la Durantaye, Franz Hofmann and Benjamin Raue in Berlin (23 Feb 2024). Besides these colleagues, I thank Emre Bayamlıoğlu, Anna Bernzen, Péter Mezei, Alexander Peukert, Jonathan Pukas, Eleonora Rosati, Alain Strowel, and Maren Wöbbeking for feedback and helpful suggestions on various drafts for this paper, as well as Simon Weyhofen for editorial assistance.

A. The Little Spider who tried to Save the Web

1 The following story is based on true events.[1]

2 Once upon a time in Europe, there was a small computer program. It got sent on a mission to collect text so that its master's could train a Large Language Model. It was told to follow a simple protocol: Go to a website on the Internet, copy its contents into a database, then follow each hyperlink to other websites, and start over. Since the program "crawled" the web in this manner, some called it a "spider". (Others admired its robot-like discipline and called it a "bot".) The crawling spider did a good job, although its mission protocol was not as simple as it appeared at first:

3 Whenever the spider approached a website that it sought to enter, it had to identify itself to the virtual butler ("server") by telling him its name. For instance, our spider might have called itself "CCbot" or "GPTBot" or "anthropic-ai". One beautiful morning, the spider approached a server and (following good old robot-spider manners) started by asking for the rules of the house. The server responded that he knew them and was ready to hand them to the spider, which in machine language sounded like this:[2]

```
4  HTTP/2 200
   server: myracloud
   date: Mon, 04 Mar 2024 02:01:00 GMT
   accept-ranges: bytes
   tdm-policy: https://rsw.beck.de/beck-online-service/tdm-
   vorbehalt
   tdm-reservation: 1
   content-security-policy: […] etag: […] x-content-type-
   options: […] X-Firefox-Spdy: h2
```

5 Along with this response, the server delivered the requested list of rules as a text file ("robots.txt"), which our spider instantly read. It said:[3]

```
6  User-agent: CCBot
   User-agent: GPTBot
   User-agent: ChatGPT-User
   Disallow: /
```

7 The spider already knew this text because two out of every five news portals worldwide (40.7 %) feature the same house rules.[4] This time, the file contained two additional lines of text,[5] but being prepended by hashtag characters (#), our spider knew they were meant to be read by humans and incomprehensible to machines.

8 Next, the little spider requested the landing page from the server. This would usually be called index.html or something to that effect; here, it was simply "/Home". The server knew what to deliver, and sent our spider a file that it devoured eagerly. Some eighty lines at the start of this file were written in machine language, opening with:[6]

1 The following is adapted from a German long-form article from which this paper derives: *Hanjo Hamann*, 'Nutzungsvorbehalte für KI-Training in der Rechtsgeschäftslehre der Maschinenkommunikation' (2024) 16 ZGE/IPJ 113.

2 HTTP Response Header of <beck-online.beck.de/robots.txt> (accessed 4 Mar 2024). See *infra*, section C.IV.

3 File contents of <beck-online.beck.de/robots.txt> (accessed 4 Mar 2024) See *infra*, section C.II.

4 Data and sources *infra* (n. 98).

5 Literally: „# Legal notice: Verlag C.H.BECK oHG expressly reserves the right to use its content for commercial text and data mining (§ 44b Urheberrechtsgesetz). – # The use of robots or other automated means to access our websites or collect or mine data without the express permission of Verlag C.H.BECK oHG is strictly prohibited."

6 File contents of <beck-online.beck.de/Home> (accessed 4 Mar 2024). See *infra*, section C.V.

9 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html lang="de" class="">
<head>[…]
<title>Homepage - beck-online</title>
<meta name="format-detection" content="telephone=no" /> […]
<meta http-equiv="content-type" content="text/html;charset=utf-8" />
<meta http-equiv=”Content-Style-Type" content="text/css" />
<meta name="tdm-reservation" content="1">
<meta name="tdm-policy" content="https://rsw.beck.de/beck-online-service/tdm-vorbehalt">
<meta name="robots" content="noai, noimageai">

10 Our spider copied the contents of this file into her database and proceeded to follow each of the file's hyperlinks. One of them was labelled "AGB" and pointed to a file on a different subdomain. The spider requested to read it. This file, too, began in machine language, but continued as a garbled mix of human- and machine-readable text. For instance, the spider found this string of characters:[7]

11 […]<h4>9. Schutzrechte</h4> […]
9.2 Der Verlag behält sich gemäß § 44b Abs. 3 UrhG das Recht vor, Vervielfältigungen […] zum Zwecke des Text und Data Mining vorzunehmen.

12 The spider could not make sense of this, as it did not speak human language, let alone German.[8] All it could do was to use the interspersed bits of machine language to display a well-formatted text for humans to read. But there was no human wanting to read it, so the spider, following its protocol, saved the file's contents, and proceeded to visit the next hyperlink. This one was labelled "These General Terms and Conditions in English (PDF)", and it pointed to a binary-encoded file[9] rather than plain text that the spider might have saved. Another file that the spider did save that day (called "/Impressum") contained a string of characters not unlike the one cited above:[10]

13 […] Text and Data Mining according to § 44b UrhG
[…]
The publisher reserves the right to reproduce for text and data mining according to § 44b UrhG.

14 Little did the spider know that this was in a different language than the one in the previous quote – it was still human language. The most the spider could have determined, based on a statistical comparison of both strings and their overlapping use of bigrams like "data mining" and "44b UrhG", was that both files were surely dealing with similar issues. But no one had told (or taught) the spider to do this, so it continued to visit the next batch of hyperlinks. Most of them pointed at files of about 10 kilobytes in size, which for a human would have looked something like this:

15 "You can access the requested file only if you are logged in. If you do not have personal login data, you can subscribe to one of the database modules mentioned above."[11]

16 Our spider diligently saved each of these error messages, and continued to visit many other websites that day. All of them were saved in the same manner: File by file, link by link. Soon the spider had gathered billions of texts in its database. And since robot-spiders never die, it continued to crawl and save the web happily ever after.

17 What is the moral of our story? Did the spying spider violate European copyright law?

B. Copyright Reservations against AI Web-Scraping

18 Legal debate about artificial intelligence is ubiquitous. So, too, in copyright law. Yet, although much has been written and discussed about protecting the output of AI (i.e., the "downstream" of digital value-creation), this paper is concerned with its inputs, i.e., "the upstream side, which might be slightly less aesthetic, but from a practical point of view [.] far more pressing. Surprisingly, to date these questions have attracted little academic attention."[12]

7 Quote from <rsw.beck.de/beck-online-service/agb-beck-online> (accessed 4 Mar 2024). See *infra*, section C.I.

8 Or else it would have read, "9. Protected rights, 9.2 The publisher reserves the right under Sec. 44b(3) German Copyright Code to reproduce contents for purposes of text and data mining."

9 Namely <rsw.beck.de/docs/librariesprovider138/kam-support-dokumente/general_terms_and_conditions_beck_online_2023_08_23.pdf> (accessed 4 Mar 2024). See *infra*, section C.I.

10 Quote from <beck-online.beck.de/Impressum> (accessed 4 Mar 2024). See *infra*, section C.I.

11 Quote translated from German ("Sie können das gewünschte Dokument […] nur aufrufen, wenn Sie eingeloggt sind. […] Besitzen Sie kein persönliches Login […], dann können Sie eines der oben genannten Module abonnieren") taken from <beck-online.beck.de/vpath=bibdata%2Fkomm%2FDieNotKosBer%2Ehtm> (accessed 4 Mar 2024). See *infra*, section C.VII.

12 *Daniel Schönberger*, 'Deep Copyright: Up- and Downstream Questions Related to Artificial Intelligence (AI) and Machine Learning (ML)' (2018) 10 ZGE/IPJ 35, 47.

19 The view that questions of input regulation appear "less aesthetic" seems to result, at least in part, from their technicality. As we will see throughout this paper, effective regulation of AI inputs requires diving deep into technical specifications. This lies beyond the comfort zone of most lawyers. What this paper will also show, however, is that lawyers need to get comfortable interpreting technical standards just as they have been interpreting legal jargon. Otherwise, any attempt at governing the digital realm by way of half-understood terms of art (such as "machine-readability") will merely turn the law into a dysfunctional barrier against innovation. Before we turn to such technical aspects, let us first consider the currently applicable laws and their doctrinal structure.

I. AI Web-Scraping as a Use Case of Text and Data Mining (TDM)

20 In order to train algorithms such as large language models ("LLMs"), AI developers require large amounts of textual data. In obtaining such training data, they commonly send spiders to scrape the web and download available online contents. Each download involves copying a file, which infringes upon rightsholders' reproduction right under Article 2 of Directive 2001/29/EC on Copyright and Related Rights in the Information Society ("InfoSocD"),[13] unless AI developers can invoke a copyright exception. Such an exception may be found in the Directive (EU) 2019/790 on Copyright in the Digital Single Market ("CDSMD"), which requires member states to introduce an exception for general-purpose *text and data mining* ("TDM"). This is defined as

21 "any automated analytical technique aimed at analysing text and data in digital form in order to generate information which includes but is not limited to patterns, trends and correlations" – article 2(2) CDSMD

22 In the past, there was considerable uncertainty whether web-scraping for AI training falls under the purview of this definition. Nowhere did the CDSMD refer specifically to artificial intelligence, so "there is no provision in the Directive that expressly deals with the training of AI",[14] which some say "has obviously been overlooked".[15] The Directive merely acknowledged vaguely that "text and data mining technologies are prevalent across the digital economy" (recital 8 CDSMD),[16] and sought to "provide for more legal certainty in such cases and to encourage innovation also in the private sector" (recital 18 subpar. 1 CDSMD).

23 While AI certainly exemplifies innovation in the private sector, there are reasonable doubts whether today's transformer architectures – as black box processes that even AI developers cannot understand or explain intelligibly – are really *aimed at analysing in order to generate information* in the sense of article 2(2) CDSMD. Many authors find it "not without a degree of uncertainty",[17] or outright "unclear whether the exceptions also cover" reproductions "for the development, training, and testing of AI systems".[18] Such reasonable doubts notwithstanding, most copyright scholars agree that "classical TDM and machine learning [...] use the same key algorithms to discover patterns in data",[19] so that the TDM exception "could be invoked, *a priori*, within the framework of any ML project".[20] Some have even

13 This is a simplification. There is more than meets the eye to the question whether AI trainers actually "use copyright protected subject matter" in a legal sense. See *Mezei*, 'A saviour or a dead end? Reservation of rights in the age of generative AI' (2024) 46 Eur. IP Rev. 461, 463.

14 *Jan Bernd Nordemann, Jonathan Pukas*, 'Copyright exceptions for AI training data – will there be an international level playing field?' (2022) 17 J. of IP Law & Pract. 973, 974.

15 *Christophe Geiger*, 'When the Robots (Try to) Take Over: Of Artificial Intelligence, Authors, Creativity and Copyright Protection' in Thouvenin/Peukert/Jaeger/Geiger (eds.), 'Kreation Innovation Märkte – Creation Innovation Markets: Festschrift Reto M. Hilty' (2024), 67, 77, reasoning that the TDM exception was "not designed to cover machine learning by generative AI systems".

16 This seems to be what *Mezei* (n. 13), 465 at fn. 47 refers to as "developments of AI".

17 *Nordemann/Pukas* (n. 14), 974; earlier doubts by *Schönberger* (n. 12), 56: "a relationship might be seen [...] although ML is much further down the line than TDM"; most recently, *Mezei* (n. 13), 465: "even if the TDM exceptions were designed in light of the developments of AI, they were not drafted in light of GenAI."

18 *Peter Georg Picht, Florent Thouvenin*, 'AI and IP: Theory to Policy and Back Again – Policy and Research Recommendations at the Intersection of Artificial Intelligence and Intellectual Property' (2023) 54 IIC 916, 928; similarly undecided *Andres Guadamuz*, 'A Scanner Darkly: Copyright Liability and Exceptions in Artificial Intelligence Inputs and Outputs' (2024) 73 GRUR Int. 111, 120: CDSMD exceptions "should work to allow some machine learning operations to take place legally, but there will be some room for interpretation depending on the particulars of each situation."

19 *Eleonora Rosati*, 'Copyright in the Digital Single Market' (2021), 72, concluding that "TDM plays a significant role in the advancement of AI applications."; similarly, *Séverine Dusollier*, 'The 2019 Directive on Copyright in the digital single market: Some progress, a few bad choices, and an overall failed ambition' (2020) 57 CMLR 979, 984: "artificial intelligence, based on machine-learning, is also deeply reliant on data mining".

20 *Theodoros Chiou*, 'Copyright lessons on Machine Learning: what impact on algorithmic art?' (2019) 10 JIPITEC 398, 409

criticized the TDM exception as being "overly broad" exactly because its definition was construed to encompass "a vast field that includes most forms of modern artificial intelligence applications".[21]

24 The final nail in the coffin[22] of this controversy came, arguably, with the Artificial Intelligence Act recently adopted as Legislative Resolution 2024/138 by the European Parliament ("AI Act"). Recital 105 of the AI Act clearly states that "text and data mining techniques may be used extensively" in the context of "large generative models" for the "retrieval and analysis of such content, which may be protected by copyright and related rights." While one might argue that recitals are not themselves legal acts but merely the "reasons on which they are based" in the sense of article 296(2) TFEU, the proper text of the AI Act also mentions data mining as one of the "procedures for data management [...] performed before and for the purpose of [...] high-risk AI systems" (article 17(1) f AI Act). This makes it abundantly clear that the European legislator has decided to apply the TDM exception in cases of reproduction for purposes of AI web-scraping.[23]

II. Rationales of the TDM Exception: Justifying An Exception-Exception

25 There are at least two rationales for the legislator to let AI developers invoke the TDM exception when reproducing works for inclusion in training datasets. Both conversely justify a critical carve-out to the exception.

26 One rationale is rights-based. Speaking in terms of Charter 2012/C 326/02 of Fundamental Rights of the European Union ("EUCFR"), the right of AI developers to mine text and data is protected by the more general freedoms of scientific research (article 13 EUCFR) and the freedom to conduct a business (article 16 EUCFR). Indirectly, it also protects downstream AI end users' freedom of expression and information (article 11 EUCFR) and freedom of the arts (again, article 13 EUCFR). Conversely, however, the right of AI developers to mine text and data encroaches upon authors' and creators' rights of expression and information (again, article 11 par. 1 EUCFR), and their right to intellectual property (article 17 par. 2 EUCFR). Given this head-on collision of fundamental rights, one objective of (copyright in general and particularly) the CDSM Directive is "to achieve a fair balance between the rights and interests of authors and other rightsholders, on the one hand, and of users on the other" (recital 6 CDSMD). To that end, article 7(2) CDSMD incorporates the three-step test from article 5(5) of the InfoSocD, based on article 9(2) of the Berne Convention.

27 The other rationale is incentive-based. The CDSMD in particular (and copyright in general) seeks to "stimulate innovation, creativity, investment and production of new content" (recital 2 CDSMD). While the TDM exception is meant "to encourage innovation also in the private sector" through incentivizing AI developers, it simultaneously needs to incentivize rightholders by enabling them to "license the uses of their works or other subject matter" (recital 18 CDSMD).

28 Both rationales interlock, and demand a counterbalance for the TDM exception in order to protect and incentivize rightsholders affected by it. This would usually take the form of monetary compensation.[24] The Directive does not prohibit this solution, but does not recommend it either.[25] Instead,

(marginal 22); *Jonathan Griffiths, Tatiana Synodinou, Raquel Xalabarder*, 'Comment of the European Copyright Society Addressing Selected Aspects of the Implementation of Articles 3 to 7 of Directive (EU) 2019/790 on Copyright in the Digital Single Market' (2023) 72 GRUR Int. 22, 25 at fn. 42; *Martin Senftleben*, 'Generative AI and Author Remuneration' (2023) 54 IIC 1535, 1542 at fn. 33; *Juha Vesala*, 'Developing Artificial Intelligence-Based Content Creation: Are EU Copyright and Antitrust Law Fit for Purpose?' (2023) 54 IIC 351, 355; *Katharina de la Durantaye*, 'Garbage In, Garbage Out. Regulating Generative AI Through Copyright Law', translation of a German journal article (ZUM 2023, 645) available through SSRN as of 13 Oct 2023 <doi.org/10.2139/ssrn.4572952>.

21 *Thomas Margoni, Martin Kretschmer*, 'A Deeper Look into the EU Text and Data Mining Exceptions: Harmonisation, Data Ownership, and the Future of Technology' (2022) 71 GRUR Int. 685, 686 – see also ibid. 688: "under the misleading label of TDM, what has been regulated at the EU level in Arts. 3 and 4 goes far beyond a mere copyright exception. In fact, it should be reclassified as [...] a property-right approach to the regulation of AI."

22 *Alexander Peukert,* 'Copyright in the Artificial Intelligence Act – A Primer' (2024) 73 GRUR Int. 497, 503 after fn. 88.

23 *Peukert* (n. 22) 503 at fn. 90: "EU legislator confirmed this prevailing view qua lex posterior"; on the other hand, see *Geiger* (n. 15), 77: "the discussion is not over"; *Guadamuz* (n. 18), 111: "growing debate".

24 For example, see the proposal by *Geiger* (n. 15), 78–81.

25 Recital 17 CDSMD justifies to "not provide for compensation for rightholders" only insofar as "potential harm created to rightholders through this exception would be minimal" because "of the nature and scope of the exception, which is limited to entities carrying out scientific research". This does not apply to commercial TDM, which is justified in Recital 18 CDSMD without reference to compensation at all.

the legislator designed an opt-out process (an *exception-exception* of sorts) whereby rightsholders can unilaterally declare a "reservation" to suspend the TDM exception in particular cases. This mechanism applies to any TDM use including the use for AI training, as the AI Act clarifies:

29 "rightsholders may choose to reserve their rights over their works or other subject matter to prevent text and data mining [...] providers of general-purpose AI models need to obtain an authorisation from rightsholders if they want to carry out text and data mining over such works." (recital 105 AI Act)

30 Despite what the first part of this quote suggests, the reservation instrument is not really designed to "prevent" TDM. Plausible though as this might seem as a means of protecting authors' moral rights (by allowing them to oppose AI training as a matter of principle),[26] the Regulation intends instead – as the second part of the quote shows – to nudge parties into bargaining, thereby instrumentalizing unilateral reservations as a conduit to create a (demand-driven) market for TDM licenses. Such market-creation is the ultimate objective of counterbalancing the TDM exception. Hence its exception-exception (*Rückausnahme*) reads:

31 "The exception or limitation provided for in paragraph 1 shall apply on condition that the use of works and other subject matter referred to in that paragraph has not been expressly reserved by their rightholders [...]" – article 4(3) CDSMD

III. Who's Afraid of Article 4(3) Reservations?

32 If rightsholders can opt out of the TDM exception, some fear that this makes the law ineffective. But, which law? Two camps have expressed diametrically opposing fears:

33 For one camp, "the law" is the TDM exception, and the reservation of rights "a provision that may very well frustrate its efficacy"[27] and "will most likely leave the practice of commercial text and data mining for non-research purposes uncertain".[28] This camp expects that "all relevant providers of content will make such reservations" so that TDM would "become practically impossible" and the "purposes of the exception would get turned on their head".[29] Some authors have even advocated for abolishing article 4(3) to improve effectiveness and economic efficiency of the TDM exception.[30]

34 For another camp, "the law" is the rights reservation, which they fear might be "extremely time-consuming and consequently expensive", hence inoperable in practice.[31] As a case in point, German journalists[32] have expressed concerns that "utilising this option in any given case" will be "difficult in practice" because "very few authors have the requisite skills and knowledge to draft a reservation [...] or to monitor compliance."[33] In addition, "it can also be unclear whether reservations have been made by rightsholders themselves or at their behest, or only by a service provider (in which case they would not prevent mining)."[34] The reservation mechanism may therefore turn out to be have no practical effect at

26 See, e.g., *de la Durantaye* (n. 20), 9 at fn. 57: "Many authors are not exclusively guided by economic interests. Quite a few of them are principally opposed to their works being used for training generative AI."

27 *Margoni/Kretschmer* (n. 21), 695; *Picht/Thouvenin* (n. 18), 928: "The scope of these exceptions is therefore limited."; *Dusollier* (n. 19), 987: "The exception [...] is thus rather precarious"; *Geiger* (n. 15), 76: "usefulness of this provision might be rather limited [...] can make the provision rather ineffective"; *Mezei* (n. 13), 464: "We cannot but agree with the reviewers' frustration with the substance and the practical functionality of these rules.".

28 *Christophe Geiger, Elena Izyumenko*, 'Towards a european "Fair Use" grounded in Freedom of Expression' (2019) 35 Am. U. Int. L. Rev. 1, 18–19.

29 *Matthias Hartmann, Jonas Jacobsen*, '„Maschinenlesbarkeit" des Rechtevorbehalts im neuen § 44b UrhG' [2021] MMR-Aktuell #441332, sub I.: „praktisch unmöglich machen und damit die Ziele der Schranke in ihr Gegenteil verkehren [...] dass alle relevanten Anbieter von Inhalten einen entsprechenden Vorbehalt anbringen".

30 In German, see *Brockmeyer*, 'Text und Data Mining: Eine rechtsökonomische Analyse der neuen Schranken im Urheberrecht' (2022), 166–170; similarly, *Emre Bayamlıoğlu*, 'Machine Learning and the Relevance of IP Rights: An Account of Transparency Requirements for AI' (2023) 31 Eur. Rev. of Priv. Law 329, 346 perceived the reservation mechanism a "major shortcoming of the provision which is likely to render it inefficient"; more cautiously, *Mezei* (n. 13), 468: "whether the CDSM Directive shall be amended, is far from being certain. [...] In general, Article 4(3) CDSM Directive shall be revisited to provide for more certainty [...] With the end of the von der Leyen Commission's tenure in 2024, this time is not 'ideal' for any such updates."

31 *Mezei* (n. 13), 465: "how such a reservation shall operate in real life is far from clear [...] it is a doctrinal and practical minefield."

32 For other voices from the German discussion, see *Hamann* (n. 1), 135–137 (C.IV.).

33 Deutscher Journalisten-Verband, Legislative Amicus Brief of 6 Nov 2020 <t1p.de/1qfzk>, p. 8: „In der Praxis wird es schwierig, von dieser Option im Einzelfall Gebrauch zu machen. Die wenigsten Urheber:innen verfügen über die nötigen Fähigkeiten und Kenntnisse, einen solchen Vorbehalt in einer maschinenlesbaren Form zu verfassen und dessen Einhaltung zu kontrollieren".

34 *Vesala* (n. 20), 357.

all.

35 Both camps' concerns are serious in view of the rationales sketched out earlier (B.II.). Inefficacy of the TDM exception might jeopardize fundamental rights of AI developers and diminish their incentives for innovation – leaving them to train their models on antiquated content in the public domain. Inefficacy of the reservation mechanism might be equally as problematic, potentially jeopardizing fundamental rights of content creators and diminishing their financial incentives for creation. As one author put it,

36 "Article 4(3) CDSM Directive cannot serve the purpose it was designed for – neither for the benefit of authors (who were the targeted beneficiaries of this provision), nor for the AI industry (whose contribution to humankind's development is unquestionable)."[35]

37 We cannot know, of course, which of the two fears is actually warranted unless we first clarify the doctrinal requirements for an effective reservation (in the next two sections) and compare them with the real potentials of current technologies (infra C.).

IV. Opt-Out Reservations in International Copyright Law

38 In order to clarify the doctrinal requirements of the reservation instrument, we need to first understand its context and prefigurations. For instance, some have criticized the opt-out model in general terms as a back-handed way to "subordinate the legislative exception to private will".[36] Yet, this exception/reservation mechanism is hardly unique in copyright law, so earlier models may provide guidance on how to construe its newest instantiation. Consider a long-established provision from the 2001 Directive upon which the CDSMD built:

39 "Member States may provide for exceptions or limitations [... for] reproduction by the press [...] of published articles on current economic, political or religious topics [...] in cases where such use is not expressly reserved" – article 5(3)c InfoSocD

40 This exception had been equally "subordinated" to "private will", allowing the press to protect "current" contents from getting reproduced, by means of reserving such use. This was itself an almost verbatim copy of a much older article in the Berne Convention, which allowed signatories to create such exceptions for "articles published in newspapers or periodicals on current economic, political or religious topics", but limited to cases in which such use was "not expressly reserved." The exact wording of this carve-out had a long and varied history since the Convention first passed in 1886:[37]

41 1886, article 7(1)1: "... unless the authors or publishers have expressly forbidden it."

42 1896, article 7(2)1 amended: "... when the authors or editors shall have expressly declared ... that reproduction is forbidden"

43 1908, article 9(2)1: "... unless the reproduction thereof is expressly forbidden."

44 1928/1948, article 9(2)1: "... unless the reproduction thereof is expressly reserved"

45 1967/1971, article 10bis(1)1: "... in cases in which [... use] is not expressly reserved"

46 As this synopsis shows, the instrument that was later implemented in article 5(3)c InfoSocD started out as a prohibition ("forbidding" users to reproduce contents) but ended up becoming a "reservation" from 1928 onwards. This semantic reorientation is meaningful in view of the purposes of the reservation instrument, and it might help to justify why nowadays, in TDM cases, the *droit moral* tends to take a back seat to market-creating incentive rationales.[38]

47 Another significant parallel with today's TDM exception is that the press exception covered materials that were once "widely believed not to be copyrightable in the first place."[39] Hence the exception could be construed as creating a new penumbra of protection, rather than dutifully protecting natural *a priori* rights. This would mean that no moral standards kept the exception from being "subserv[i]ent to its prohibition by rightholders", as is now the case for the TDM exception.[40]

35 *Mezei* (n. 13), 462.

36 *Rossana Ducato, Alain Strowel*, 'Limitations to Text and Data Mining and Consumer Empowerment: Making the Case for a Right to "Machine Legibility"' (2019) 50 IIC 649, 666.

37 Sources documented as online appendix to *Ricketson/Ginsburg*, 'International Copyright and Neighbouring Rights: The Berne Convention and Beyond', 2nd ed. 2005 <global.oup.com/booksites/content/9780198259466>.

38 See *supra* marginal 30.

39 *Jane C Ginsburg*, 'Berne-Forbidden Formalities and Mass Digitization' (2016) 96 Boston U. L. R. 745, 759–760 (citing to pp. 249–254 of the *travaux*, the Records of the 1908 Revision Conference).

40 *Dusollier* (n. 19), 987.

48 Insofar as the doctrine on the reservation of press rights can actually inform the reservation of TDM rights, it is still open. While some German interest groups had proposed to directly model the transposition of article 4 CDSMD on the older reservation of press rights,[41] others have argued that

49 "the drafting history of the Berne Convention indicates that art. 10bis(1) is a 'lex specialis,' a sui generis provision that [...] does not create a basis for generalization into a technique for instituting declaratory measures."[42]

50 As we will discuss later in section V., there are some questions regarding the reservation of TDM rights on which the doctrine regarding the reservation of press rights might, arguably, be brought to bear. On the other hand, the new reservation may provide unprecedented challenges, especially regarding its territorial reach. That is because the recently passed European AI Act requires all "providers of general purpose AI models" in the European Union – no matter how liberal the jurisdiction in which they trained their models[43] – to

51 "put in place a policy to respect Union copyright law in particular to identify and respect, including through state of the art technologies, the reservations of rights expressed pursuant to Article 4(3) of Directive (EU) 2019/790" – article 53(1)c AI Act (with recital 106)

52 Not only does this obligation enforce a Brussels effect on copyright law and revisit the principle of territoriality once more.[44] It also raises the question of what "state of the art technologies" are, and how rights reservations might be made intelligible to them.[45] This question will be the focus of the latter half of this paper (C.).

V. On Standards of Expressivity and Machine-Readability

53 The legal requirements for an effective reservation of TDM rights have been described as "an aspect of the commercial TDM exception or limitation that did not spark enough discussion in the EU so far".[46] In fact, there are two standards that article 4 CDSMD requires to be fulfilled cumulatively:

54 First, as cited previously, article 4(3) CDSMD requires rightsholders to "expressly" reserve TDM uses. This element seems to create some discomfort as authors tip-toe around a clear definition,[47] and lawmakers in member states such as Germany transposed article 4(3) CDSMD through "omission of the 'express' element", despite causing "linguistic divergences in its transposition".[48] So what should "expressly" mean, if one took the requirement seriously?

55 The term does not appear elsewhere in the Directive. Yet, a recital in another context uses the adjective "explicit",[49] which most language versions of the Directive equate with "express".[50] This suggests that an "express" reservation needs to be *expressis verbis*, i.e., "explicit" rather than implicit – which excludes some technological measures that we will encounter later (C.VII.). In addition, the Directive requires that "other uses should not be affected by the reservation" (recital 18 subpar. 2 CDSMD), meaning that it needs to be *use-specific*. A third requirement can be derived from the doctrine on the reservation of press rights under the Berne Convention introduced earlier (B.IV.). During its continual reformulation,[51] article 10bis was temporarily extended by a sentence saying:

56 "In the case of periodicals it shall be sufficient if such prohibition is indicated in general terms at the beginning of each number." – article 7(2)1 Berne Convention 1896–1908

57 This sentence was dropped from later versions of the Convention, suggesting that "express" should no longer include wholesale reservations in a central location. This is well-founded in the objective of having rightsholders decide in view of specific contents whether their use should be reserved

41 BDZV/VDZ/VDL, Legislative Amicus Brief of 31 Jan 2020 <t1p.de/ahzbb>, p. 10 („Diese Vorgabe kann durch eine Formulierung erreicht werden, die dem Rechtevorbehalt in § 49 UrhG [German transposition of article 5(3)c InfoSocD] nachgebildet ist.")

42 See *Ginsburg* (n. 39), 759 around fn. 58.

43 See the country survey by *Sean M.Fiil-Flynn et al.*, 'Legal reform to enhance global text and data mining research' (2022) 378 Science 951.

44 See already Madiega (European Parliamentary Research Service), 'EU copyright reform: Revisiting the principle of territoriality', Briefing of Sep 2015 <europarl.europa.eu/RegData/etudes/BRIE/2015/568348/EPRS_BRI(2015)568348_EN.pdf>.

45 Likewise skeptical, *Mezei* (n. 13), 469: "It is [...] far from being clear how the EU has imagined the respect of opt-out privileges via a 'policy'."

46 *Mezei* (n. 13), 465.

47 For instance, *Mezei* (n. 13), 465 defines "expressly" by saying that "rightholders shall openly and expressly claim ...", which is circular.

48 *Margoni/Kretschmer* (n. 21), 695.

49 Recital 69 CDSMD.

50 In the French version, both "express" and "explicit" get translated to « expressément », in the German version to „ausdrücklich", in the Italian version to « espressamente ».

51 See *supra* margin als 41-45.

or not.[52] Otherwise they could not reassess their stance vis-à-vis TDM reservations later, rendering themselves unable "to decide whether they want to include the new contents in their earlier reservations or not."[53] To sum up, the three dimensions of the "express" element preclude reservations that

58 "are complex, nested [or fully implied, HH] or cannot be accessed on the specific page of the content, as well as those that do not expressly refer to text and data mining".[54]

59 The second requirement of article 4(3) CDSMD is that reservations need to be made "in an appropriate manner, such as machine-readable means in the case of content made publicly available online."[55] For online content (which is most relevant for AI training), the "appropriate manner" requirement is slightly ambiguous: Due to its exemplification through "such as", machine-readability might be construed as one case of an *appropriate manner in the case of content available online*. If this reading was correct, then other (non-machine-readable) manners could be equally as appropriate. This is not, however, what the Directive intended. Its recital clarifies in most language versions[56] that

60 "[i]n the case of content that has been made publicly available online, it should *only* be considered appropriate to reserve those rights by the use of machine-readable means [...]" – recital 18 subpar. 2 CDSMD

61 This means that the provision is correctly construed by reading *machine-readable means in the case of content available online* as an example of the "appropriate manner". In our context, therefore, the second requirement is not appropriateness in general, but machine-readability. However, as with "express", the Directive neither defines "machine-readable" nor uses it in other contexts. Very few scholars have devoted significant attention specifically to the meaning of "machine-readable",[57] despite its being a cornerstone of article 4(3) CDSMD. It also requires the most guidance due to incorporating a strictly technological concept.

62 There is a wide range of potential interpretations of "machine-readable". It could be construed conservatively or liberally. The most conservative reading would only include *native machine code*, i.e., binary-encoded commands on the base layer of CPU language. The most liberal reading might include "any digitally provided information" that can "be 'read' into a computer's working memory".[58] The range of these potential interpretations has caused great uncertainty in the transposition of article 4(3) CDSMD.[59] While there is no doubt that "machine-readable means do not exclude human-readability of the reservation",[60] powerful interest groups such as the US Motion Picture Association have lobbied for the converse: They tried to convince legislators that "any reservation that a human could read is equally as machine-readable".[61] This would mean that "machine-readable" is really just synonymous with "readable", turning the "machine" limiter into inconsequential jargon. Opposing interest groups such as the Association of European Research Libraries have correctly highlighted the "theoretical" absurdity of such a boundless conception, stressing that

63 "[i]t is vitally important that it is clear this relates to widely used machine readable 'standards' [...] If this is not the case then anything is machine readable, and the wording is tantamount to requiring all terms and conditions on a website having to be read and interpreted by a human one by one."[62]

64 In this quote, "standards" cannot refer to mere linguistic conventions, despite what some authors suggested by proposing to exclude "lay-person phrasing in reservations" in favor of well-defined boilerplate text such as "Text und Data Mining

52 This is also the general understanding of the respective German provision, see *Hamann* (n. 1), 149, 154 (near the end of E.I. and E.II. respectively).

53 *Mezei* (n. 13), 468 and further: "rightholders might indeed change their mind and want to allow certain TDM activities for third parties."

54 *Hartmann/Jacobsen* (n. 29) sub II.3: „komplexe, verschachtelte oder nicht auf der konkreten Seite der Inhalte abrufbare Vorbehalte oder solche, die nicht ausdrücklich auf das Text und Data Mining abstellen".

55 I omitted this adverbial phrase earlier when citing article 4(3) CDSMD; it takes the place of the ellipsis at the end of section B.II.

56 See IBM Intellectual Property Law, Legislative Amicus Brief of 6 Sep 2019 <t1p.de/u5umi>, p. 3: "In the German translation of recital 18, this understanding is unfortunately not so clear".

57 Namely, *Hartmann/Jacobsen* (n. 29); *Lisa Löbling, Christian Handschigl, Kai Hofmann, Jan Schwedhelm*, 'Navigating the Legal Landscape: Technical Implementation of Copyright Reservations for Text and Data Mining in the Era of AI Language Models' (2023) 14 JIPITEC 499; 505–509; *Mezei* (n. 13).

58 *Hartmann/Jacobsen* (n. 29) sub II.2.a), II.2.c): „jede digital hinterlegte Information [...], denn solche Daten können in den Arbeitsspeicher eines Rechners ‚gelesen' werden."

59 See *Hamann* (n. 1), 128–133 (D.II.).

60 Mezei (n. 13), 466 after fn. 49.

61 MPA, Legislative Amicus Brief of 31 Jan 2020 <t1p.de/m1c3c>, p. 2.

62 LIBER, Legislative Amicus Brief of 31 Jan 2020 <t1p.de/hb30r>, p. 2 (no. 8).

vorbehalten".[63] Presenting this proposal *verbatim* to an international audience instantly highlights its most obvious flaw: Not quite every AI developer on the planet speaks German fluently. Even some German authors acknowledge this by advising to "reserve rights in English language (lingua franca) just in case".[64] Yet, as our introductory example shows,[65] spiders do not speak English either. The question which human language should be the "lingua franca" of TDM reservations is therefore moot. None should. Natural language, as will soon be illustrated (C.I.), is simply not amenable to sufficient standardisation. The only "machine-readable" languages can thus be artificial ones, created by well-defined technical standards.

65 This interpretation is backed by Directive (EU) 2019/1024 on Open Data and the Re-Use of Public Sector Information (PSI2D)[66] which defines "machine-readable format" as

> **66** "a file format structured so that software applications can easily identify, recognise and extract specific data, including individual statements of fact, and their internal structure" – article 2(13) PSI2D

67 While this definition, which originated in 2013,[67] directly applies only to "documents held by public sector bodies" (article 1 no. 1 PSI2D),[68] there are good reasons to use it in construing the machine-readability requirement of article 4(3) CDSMD as well.[69] After all, both instances of machine-readability serve the same purpose of automated processability. In that sense, the reservation of TDM rights is another instance of "Code is Law",[70] where a Code determines what *can* be expressed so that the Code definition becomes the authoritative interpretation of what *is* expressed.

68 However, instead of specifying a well-defined code interface, article 4(3) CDSMD "is lacking such a specification of the interface".[71] Despite the quasi-legal effect of the interface used, the legislator eschewed standard-setting and left "the number of different opt-out models" to "grow exponentially".[72] As syntax standards proliferate, we need to review them one by one to determine which ones qualify as "machine-readable" under article 4(3) CDSMD. This is the objective of the next chapter.

C. Human-to-Machine Communication of Copyright Reservations

69 Now that the legal requirements for an effective reservation of rights have been clarified, it is time to discuss the available standards. Scholars complain that "as of now, a specific technical standard is lacking",[73] and one renowned software developer's IP department emphasised the practical need for such a standard:

70 "It is important that technical hurdles in any transposition of Article 4(3) are kept to a minimum, because [...] any technical hurdle/limitation will quickly have ramifications on speed-to-market and progress of AI solutions. Any transposition must be kept broad and flexible enough to accommodate improvements in the advancement of the technology of defacto or standard practices."[74]

71 This quote highlights a pronounced ambiguity: On the one hand, industry needs a precisely defined standard to enhance legal certainty as a means of reducing hurdles and increasing speed-to-market. On the other, industry needs its improvements in standard practices, even *de facto* ones, to be accommodated by the law. This ambiguity, one might argue, was bound to paralyse the lawmaker and prohibit them from precisely specifying any standard of machine-readability in article 4(3) CDSMD.

72 Unsurprisingly, then, legal scholars have found "the substance and the functioning of rights reservation" to be nothing short of "a mystery".[75] A more sober

63 *Hartmann/Jacobsen* (n. 29) sub II.2.c). This translates to "text and data mining reserved".

64 *David Bomhard*, 'KI-Training mit fremden Daten – IP-Rechtliche Herausforderungen rund um § 44b UrhG' (2023) 14 DSRI-Tagungsband 255, 266: „sicherheitshalber immer auch in englischer Sprache (lingua franca)".

65 See *supra* after n. 10.

66 See *Griffiths/Synodinou/Xalabarder* (n. 20), 29 with reference to "other pieces of EU legislation".

67 Article 1(2) and recital 21 of the Directive 2013/37/EU of 26 Jun 2013 amending Directive 2003/98/EC.

68 Likewise, recital 1 of Directive 2013/37/EU (n. 67): "documents produced by public sector bodies of the Member States".

69 *Griffiths/Synodinou/Xalabarder* (n. 20), 29: "article 4 DSMD should be interpreted in combination with the PSI-II Directive".

70 *Lessig*, 'Code and Other Laws of Cyberspace' (1999), 6 (lessig.org/images/resources/1999-Code.pdf), with end note 7 (p. 241) citing, foremost, *Mitchell*, 'City of Bits: Space, Place, and the Infobahn' (1995), 111.

71 *Hartmann/Jacobsen* (n. 29) sub II.2.b): „an einer solchen Spezifikation der Schnittstelle fehlt es".

72 *Mezei* (n. 13), 465.

73 *de la Durantaye* (n. 20), 10 after fn. 58.

74 IBM (n. 56), p. 2.

75 *Mezei* (n. 13), 465; more cautiously, *Ducato/Strowel* (n. 36), 666: "questions remain as to what the reservations in a machine-

policy brief that reviewed some (not all) potential technologies concluded dryly:

> **73** "There are currently no generally recognized standards or protocols for the machine-readable expression of the reservation of rights provided for in Article 4 of the Directive."[76]

74 Despite (or because of?) this perception of failed standardisation, few scholars even try to systematically review the available protocols for reservations under article 4(3).[77] Some authors do refer to some technologies, but mostly without explaining their specific functioning. Conversely, technical experts propose protocols that cannot fulfil the legal requirements set out above.

75 The question remains, which technologies are machine-readable *in the sense of article 4(3) CDSMD*. Answering it requires an interdisciplinary perspective that integrates technological process knowledge and normative reasoning. In order to illustrate this process, our introductory example (supra A.) will illustrate most of the technologies discussed hereinafter. The paper thus comes full-circle by returning to our little spider's journey through the web: Has it violated copyright? Which of the reservations that it encountered but ignored, were actually valid under the CDSM Directive?

I. Terms and Conditions

76 The CDSMD recital clarifying that "only" machine-readable reservations should be appropriate for online content was cited partially earlier.[78] In place of the quote's closing ellipsis, the recital actually reads "including [...] terms and conditions of a website or a service." (recital 18 subpar. 2 CDSMD). Some authors read this to say that terms and conditions are one example given by the Directive of machine-readable means. If this reading was correct, it would follow that "AI trainers must take into account [...] terms and conditions of websites and online services"[79] because the "language in their terms of use" might "constitute an effective reservation".[80] Indeed, the online service in our introductory example did actually include such language in its T&Cs.[81]

77 As literally apt as this reading of "machine-readable means, including terms and conditions" might seem, it would upend the entire purpose of machine-readability that we discussed earlier (B.V.). Consider the variety of potential wordings that terms and conditions might take.[82] Even in our introductory example, the T&C's current language is very different (and located in a different provision) from the previous version of the same document just months earlier.[83] This explains why IT experts assume that identifying or parsing a reservation expressed in natural language would be "difficult to near impossible" without the use of "the most sophisticated technology".[84] From one experiment on TDM reservations across 100 websites, researchers have similarly concluded that "effective opt-out management would require advanced NLP methods".[85] Yet, advanced natural language processing (NLP) is itself a case of text and data mining (TDM). It may have to rely on a corpus of reproduced website contents, which could not be in turn justified under any copyright exception. In other words, one cannot simply use TDM to find out whether using TDM is permissible.

78 In addition, neither the location nor the file format of T&C documents are standardised in any way. Some websites include reservation language in the imprint,[86] and even the T&C document for the website being scraped in our introductory example (beck-online.beck.de) was found in another domain scope (rsw.beck.de) with an English version available only as a pdf file.[87] While many websites provide T&Cs in pdf format for best printability,

readable format are, and how they could be implemented".

76 *Keller/Warso*, 'Defining Best Practices for Opting Out of ML Training' (29 Sep 2023), OpenFuture Policy Brief #5 <openfuture.eu/wp-content/uploads/2023/09/Best-_practices_for_optout_ML_training.pdf>.

77 Without engaging technical specifications in detail, see *Löbling et al.* (n. 57), 505–509. After finishing the first draft of this paper, I learned of a draft version of *Mezei* (n. 13), who likewise notes that "research papers either omit or struggle with these problems" (465), then reviews technologies on an issue-by-issue basis rather than explaining or even discussing each of them.

78 *Supra* marginal 60.

79 *Senftleben* (n. 20), 1544.

80 *Vesala* (n. 20), 357 ("e.g. banning reverse engineering or similar methods, or the storing of available content"); likewise, *Mezei* (n. 13), 465: "There is a risk that expressed terms of end-user licence agreements can exclude the lawfulness of TDM".

81 See *supra* at n. 7, translated in n. 8.

82 Review of TDM terms on 21 platforms in *Ducato/Strowel* (n. 36), 669–673.

83 See no. 10.9 of the T&Cs of 9 Mar 2022, archived on 15 Jan 2024 at <web.archive.org/20240115214414/rsw.beck.de/docs/librariesprovider138/default-document-library/general_terms_and_conditions_beck_online_2022_03_09.pdf>.

84 IBM (n. 56), p. 2.

85 *Löbling et al.* (n. 57), 504.

86 See *supra* marginal 13. This may be a German *sonderweg* because the German legislator equated "metadata" (recital 18 subpar. 2 CDSMD) with "imprint", see *Hamann* (n. 1), 146–149 (E.I.).

87 See *supra* n. 9.

this format is notoriously ill-standardised, so that even advanced algorithms cannot reliably parse it. T&C documents were simply not made to be read by machines. Experts hence argue that if "a PDF, terms and conditions etc" were considered machine-readable, then "anything on a computer screen is".[88] This would revive the lobby position rejected earlier that "readable" and "machine-readable" are synonymous (marginal 62 at n. 61).

79 Given these challenges, the Directive's recital needs to be corrected by inserting the missing preposition "in": The correct construal of recital 18 has rightsholders "reserve those rights by the use of machine-readable means, including *in* terms and conditions". Consequently, AI developers may ignore any "reservations not expressed in code", which includes (but is not limited to) "when TDM restrictions are found in website terms and conditions in PDFs, images or as website text".[89]

80 Even if courts came to view this question differently and accepted at least some T&C documents written in natural language as "machine-readable", then the additional requirement of "express" reservation still limits its effect to the document within which it is found (i.e., the terms document itself). As discussed earlier for "wholesale reservations in a central location",[90] reservation statements cannot affect multiple contents because each of them needs to be reserved "expressly", i.e., content-specifically.

II. Robots Exclusion Protocol (robots.txt)

81 Apart from its terms and conditions, the website in our introductory example also reserved TDM rights in a file called robots.txt.[91] This file has aptly been called "the text file that runs the internet" because even five years ago, it was used on half a billion websites according to 2019 estimates by Google.[92] Each of these text files instantiates "an exclusion protocol that content providers can insert into the root directory to prevent crawling or indexing activities".[93] The protocol was proposed in 1994 by Dutch search engine pioneer *Martijn Koster* and became a *de facto* "established standard"[94] for repelling search engine spiders. Its formal canonization is rather recent, as the Internet Engineering Task Force (IETF) formalized this "Robots Exclusion Protocol" (REP) as an official standard in 2022.[95]

82 Given its widespread use and its machine-readability (except for comments in natural language, see example supra n. 5), the Robots Exclusion Protocol was quickly proposed – both by special interest groups[96] and academics[97] – as a suitable standard for reservations under article 4(3) CDSMD. Indeed, an ongoing empirical survey of 886 US-American and 273 other news portals from 31 countries shows that currently two-fifths of them (40.7 %) deny access in their robots.txt to the same spiders as the website in our introductory example (at marginal 6), while more than half of them (54.3 %) deny access to at least one of the spiders from the introductory example, or that of Google AI.[98]

83 It is important to note that by its very definition the Robots Exclusion Protocol is "not a form of access authorization" (rule 1 subpar. 4 REP), but a collection of "rules [...] that crawlers are requested to honor" (rule 1 subpar. 3 REP). It therefore does not really prevent spiders from entering a website,[99] but simply requests them to stay out. The REP is therefore best understood as a form of "Private Ordering Through Opt-Outs".[100] Some large crawlers openly defy the

88 LIBER (n. 62), p. 2 (no. 8).

89 *Griffiths/Synodinou/Xalabarder* (n. 20), 30; *Löbling et al.* (n. 57), 502.

90 See *supra* marginal 57.

91 See *supra* marginals 5 and 6.

92 *Pierce*, 'The text file that runs the internet', The Verge, 14 Feb 2024 <theverge.com/24067997/robots-txt-ai-text-file-web-crawlers-spiders>.

93 *Ducato/Strowel* (n. 36), 674; IBM (n. 56), 2: "a protocol/format that is used widely by web crawlers and web robots today".

94 *Hartmann/Jacobsen* (n. 29) sub II.3): „So ist ein Standard etabliert, Anweisungen an Suchmaschinen in einer spezifischen Datei abzulegen (‚robots.txt')."

95 *Koster/Illyes/Zeller/Sassman*, 'Standard RFC 9309: Robots Exclusion Protocol', as of Sep 2022, documented at <rfc-editor.org/rfc/rfc9309.html>.

96 As two of just many, see IBM (n. 56), 2, and LIBER (n. 62), 2 (no. 8).

97 *Ducato/Strowel* (n. 36), 674; *Dusollier* (n. 19), 987: "machine-readable means as robots.txt files"; *Tan/Lee* (n. 104), 1039: "owners may even adopt a Robots Exclusion Protocol"; *Senftleben* (n. 20), 1544: "AI trainers must take into account metadata, such as robots.txt files"; *Löbling et al.* (n. 57), 502: "setting up a robots.txt file can express an opt-out" (similarly ibid., 506); *Griffiths/Synodinou/Xalabarder* (n. 20), 25 after fn. 42: "machine-readable means, including [...] robot.txt type metadata"; *Mezei* (n. 13), 467: "inclusion of relevant computer-readable language in the robots.txt file".

98 Own analysis of data by *Welsh*, 'Who blocks OpenAI, Google AI and CC?', palewire, accessed on 2 Apr 2024 <palewi.re/docs/news-homepages/openai-gptbot-robotstxt.html>: 629 of 1.159 news publishers disallow either Google AI („Google Extended"), OpenAI („GPTBot", „ChatGPT-User") or Common Crawl („CCBot"). 472 disallow only the latter two, 421 disallow all three.

99 See *infra* at marginal 128.

100 *Matthew Sag*, 'Copyright and Copy-Reliant Technology' (2009) 103 Nw. U. L. Rev. 1607, 1666–1668.

Robots Exclusion Protocol,[101] and there are good reasons not to rely on it for communicating TDM reservations either:

84 First, a spider's name (so-called *product token*) cannot uniquely identify it because under the Robots Exclusion Protocol, "crawlers set their own name" (rule 2.2.1 REP). This is why our introductory example said that "our spider might have called itself...". Some spiders do not identify themselves at all,[102] and "many others attempt to operate in relative secrecy"[103] or to "maliciously bypass REPs".[104]

85 Second, the list of product tokens at <robotstxt.org/db.html> has not been updated since 2011, which means that even identifying today's AI spiders requires a lot of traffic analysis.[105] Major AI developers reacted to this issue promptly by officially announcing their crawlers' tokens[106] – probably not least in hopes of evading more effective regulation by supporting the dated Robots Exclusion Protocol.

86 Third, the Robots Exclusion Protocol cannot communicate reservations for large amounts of content. The protocol allows crawlers to adopt a "parsing limit to protect their systems" (rule 2.5 REP), whereby they need not process more than 512,000 characters of a given robots.txt file ("parsing limit must be at least 500 kibibytes"). If a website of just a few hundred content files sought to communicate TDM reservations for each of those files to each known crawler, it would quickly exceed the parsing limit and fail its purpose.[107] If, instead, the TDM reservation was couched in general terms (as in our introductory example[108]) it could no longer be content-specific and would fall short of the expressivity standard, as discussed previously.

87 Fourth, the Robots Exclusion Protocol defines only two potential declarations to begin with: "Allow" to designate contents that are free to crawl, and "Disallow" for others (rule 2.2.2 REP). Additional declarations could be made,[109] but they are not standardised. So, what does a "Disallow" declaration mean? The protocol does not precisely define its purpose other than stating that "it may be inconvenient for service owners if crawlers visit the entirety of their URI space." (rule 1 subpar. 3 REP) This harkens back to the early days of the Internet when search engine crawlers caused so much traffic that "all it took was a few robots overzealously downloading your pages for things to break and the phone bill to spike."[110] This purpose is no longer relevant, so a different rationale has taken its place:

88 "It's been a while since 'overloaded servers' were a real concern for most people. 'Nowadays, it's usually less about the resources that are used on the website and more about personal preferences,' says John Mueller, a search advocate at Google."[111]

89 Yet, since the Robots Exclusion Protocol was never meant to communicate sophisticated preferences and their subtle distinctions, its binary syntax ("geared toward search engine crawlers") does "not necessarily serve" other purposes.[112] In particular, it cannot communicate conditional permissions, as would be needed to reserve TDM content for automatable commercial licensing.[113] The REP cannot even distinguish between different crawling purposes, so that bots serving multiple purposes (e.g., search engine indexing *and* AI data collection) cannot be rejected for the latter reason without also engendering the former.[114] This is exactly what the Directive's "express" requirement should avoid.[115]

101 *Pierce* (n. 92): "The Internet Archive, for example, simply announced in 2017 that it was no longer abiding by the rules of robots.txt. [...] And that was that."

102 See *Wiese*, 'Robots.txt is not the answer', Search Engine Land, 18 Jul 2023 <searchengineland.com/robots-txt-new-meta-tag-llm-ai-429510>.

103 *Pierce* (n. 92), and further: "finding a sneaky crawler is needle-in-haystack stuff".

104 *David Tan, Thomas Lee Chee Seng*, 'Copying Right in Copyright Law - Fair Use, Computational Data Analysis and the Personal Data Protection Act' (2021) 33 Sing. Acad. Law J. 1032, 1070: "a key scenario is when web robots maliciously bypass REPs".

105 *Waldvogel*, 'How to block AI crawlers with robots.txt', netfuture.ch of 9 Jul / 31 Dec 2023 <netfuture.ch/2023/07/blocking-ai-crawlers-robots-txt-chatgpt>.

106 OpenAI christened its „GPTBot" on 8 Aug 2023 (platform.openai.com/docs/gptbot), Google introduced the product token "Google-Extended" on 28 Sep 2023 (developers.google.com/search/docs/crawling-indexing/overview-google-crawlers).

107 *Wiese* (n. 102).

108 See *supra* marginal 6: "Disallow: /", where the forward slash denotes all contents of the website.

109 According to rule 2.2.4 REP, "crawlers MAY interpret other records that are not part of the robots.txt protocol – for example, 'Sitemaps'".

110 *Pierce* (n. 92).

111 *Pierce* (n. 92).

112 *Graham* cited in *Pierce* (n. 92).

113 See *infra* marginal 114.

114 *de la Durantaye* (n. 20), 10 at fn. 60: "robots.txt files do not allow for differentiation: If you communicate that you do not wish your website to be scraped for training purposes, it will not appear in search engines either. De facto, then, your work will cease to exist online."; similarly, *Löbling et al.* (n. 57), 505 who thus propose a reform of the REP standard (507–509) but do not address any of the other aforementioned concerns.

115 See recital 18 subpar. 2 CDSMD, cited *supra* marginal 60.

III. Spawning Protocol (ai.txt)

90 Given these limitations of the Robots Exclusion Protocol, a newer standard has been proposed to "keep yourself searchable, while restricting AI training".[116] Or so runs the sales pitch of Minneapolis-based startup "Spawning" founded by musician *Holly Herndon*.[117] This startup set out on a mission to develop "data governance for generative AI", and more broadly to "build the consent layer for AI" by collaborating with major actors on both sides: AI developers such as Hugging Face and Stability AI as well as repertoire owners such as Shutterstock and ArtStation.[118]

91 One of the first Spawning products is a protocol presented on 30 May 2023 under the moniker ai.txt, which caught the attention of only a few legal scholars.[119] It strongly resembles the robots.txt discussed in the previous section (with which it shares a similar syntax placed as a text file in the root folder and voluntarily respected by crawlers), but a thorough comparison is hindered by a lack of public documentation.

92 From what Spawning's website reveals, its protocol seems to be an improved version of the REP in at least two dimensions of expressivity: Regarding use-specificity, TDM reservations in ai.txt are stored separately and apart from search index permissions in robots.txt. Regarding content-specificity, ai.txt is designed to be checked whenever a file is accessed through the proprietary "Spawning API" (a programming interface sold to AI developers), whereas robots.txt gets accessed only once upon entering a website through the landing page ("front door") and never laterally by direct hyperlink.[120] However, he extent to which Spawning has addressed other shortcomings of the REP (parsing limit, lack of conditional permissions, etc.) remains unclear.

IV. HTTP Response Header (tdm-reservation, X-Robots-Tag)

93 Another technology has rarely ever been discussed in relation to article 4(3) CDSMD,[121] namely Response Headers in the HyperText Transfer Protocol (HTTP). What this means is simply the machine-readable reply of a server to a file request sent by a user, as illustrated in our introductory example (marginal 4).

94 This reply starts with a status code (in our example, "200" for "OK") and delivers additional "meta" data (from Greek μετά for "after, behind; among, between"[122] in the sense of "appended" data that accompany, describe or categorize the datarequested). By virtue of this meta-communication, the Hypertext Transfer Protocol allows content-specific communication in relation to concrete files, which better fulfils the expressiveness requirement than any general reservation in a centrally located text file. As a large tech company's IP department explained,

> **95** "the most feasible method for checking reservation of rights for online content is by using common metadata. Using metadata would overcome the issue of readability as tools to parse metadata can be implemented fairly trivially and economically."[123]

96 In fact, even the Directive itself suggested "metadata" as a potential location for machine-readable reservations (recital 18 subpar. 2 CDSMD). This has been taken up by a community group of the World Wide Web Consortium (W3C), who recently proposed the Hypertext Transfer Protocol as one of three standards for implementing TDM reservations.[124] Unfortunately, their multi-pronged *TDM Reservation Protocol* ("TDM ReP") has received little attention in legal literature thus far.[125]

97 The core of this proposal is to insert into a server's response a meta declaration "tdm-reservation" with value 1 and a meta declaration "tdm-policy" containing the URL for a file containing contractual details (rule 6.2 TDM ReP) – as has been done in our introductory example.[126] In our example, the TDM policy file contained no contractual details, but merely the same proviso as the website's imprint:

116 Spawning ai.txt, accessed 7 Mar 2024 <spawning.ai/ai-txt> and <site.spawning.ai/spawning-ai-txt>.

117 See *Dredge*, 'Holly Herndon reveals plans for her AI-focused startup Spawning', music:)ally of 16 Nov 2023 <musically.com/2023/11/16/h>.

118 About Spawning, accessed 7 Mar 2024 <spawning.ai/about>.

119 See *Keller/Warso* (n. 76), 8–9; *Mezei* (n. 13), 467-468.

120 *Miller*, 'ai.txt: A new way for websites to set permissions for AI', Spawning Blog on 30 May 2023 <spawning.substack.com/p/aitxt-a-new-way-for-websites-to-set>.

121 Only *Mezei* (n. 13), 467 casually mentions "declaring a choice in an HTTP response".

122 See <etymonline.com/word/meta->.

123 IBM (n. 56), p. 2.

124 W3C TDMRep Final Community Group Report of 2 Feb 2024 (w3c.github.io/cg-reports/tdmrep/CG-FINAL-tdmrep-20240202).

125 See only *Keller/Warso* (n. 76), 7–8; *Löbling et al.* (n. 57), 507; *de la Durantaye* (n. 20), 10 in fn. 60; *Mezei* (n. 13), 467 at fn. 60.

126 See *supra* marginal 4.

98 "Text and Data Mining according to § 44b UrhG: The publisher reserves the right to reproduce for text and data mining according to § 44b UrhG."[127]

99 Since this "policy" is akin to T&Cs, it is equally as non-machine-readable.[128] If it were to become machine-readable, the policy file could not be written in HTTP syntax, because as a transfer protocol it is limited to short, transfer-related responses. Another language protocol would be required in addition, and we will later encounter examples (including another proposal by the W3C community group) of how such policies might be encoded machine-readably (infra C.VI.).

100 As an additional limitation, it is worth noting that unlike the Robots Exclusion Protocol, the TDM Reservation Protocol is not without alternatives. There have been at least two other proposals for reservation standards based on the Hypertext Transfer Protocol. Both repurpose the meta declaration "X-Robots-Tag", which (like robots.txt) had once been developed to control search engine indexing:

```
X-Robots-Tag: noai, noindex[129]
X-Robots-Tag: usage-rights: CC-BY, noindex[130]
```

102 While these proposals are unlikely to outcompete the TDM Reservation Protocol with its authoritative backing (W3C) and well-crafted, open documentation, the race has not been run yet and it is too early to tell which variant will be adopted more widely.

127 Quote from <rsw.beck.de/beck-online-service/tdm-vorbehalt>, accessed 7 Mar 2023. For the corresponding imprint language, see *supra* marginal 13.

128 Rule 5.2 TDM ReP: "A TDM Policy is considered human readable if its content-type is text/html. It is considered machine-readable if its content-type is either application/json or application/ld+json."; *Löbling et al.* (n. 57), 507: "if the information at this URL is solely available in HTML or text formats, it is not considered machine-readable. To achieve machine-readability, policies must be articulated using JSON or JSON-LD".

129 *Emanuel Maiberg*, 'An AI Scraping Tool Is Overwhelming Websites With Traffic', VICE, 25 Apr 2023 <vice.com/en/article/dy3vmx/a> on "Romain Beaumont, the creator of the image scraping tool img2dataset" who designed it "to scrape images from any site unless site owners add https headers like 'X-Robots-Tag: noai,' and 'X-Robots-Tag: noindex.'"

130 *Wiese* (n. 102), explaining this reservation as "the page should not be used for search results but can be used for commercial LLMs as long credit is given to the source", but without clarifying how a general prohibition against TDM should be communicated (or whether it be included in "noindex").

V. HyperText Markup Language (<meta>, data-notdm)

103 Another type of metadata appears in our introductory example at marginal 9. These are the "meta elements of an HTML-conformant website", which some legal scholars have considered a suitable medium for TDM reservations.[131]

104 HTML (HyperText Markup Language) is a so-called markup language, i.e., a human-readable text format that allows to encode both *semantic* content and *syntactic* information. Just like natural language structures text through syntax elements (such as these brackets, which separate parenthetical comments and illustrations from the main text), the Hypertext Markup Language spins structuring information off into so-called "tags" using less-than- and greater-than-signs to stand in for <angled brackets>. For example, in the text quoted earlier (marginal 13) both occurences of the
 tag would have been rendered by any browser as an on-screen line break.

105 Despite sharing the moniker "metadata" with hypertext transfer metadata, hypertext markup metadata are not "appended" to a file, but to its content instead. Using an analogy from the physical world, one could say that HTTP metadata are like the packing slip of a book, while HTML metadata are its imprint. The latter is placed within the book but nonetheless appended to its actual content. The analogy shows that metadata in the Hypertext Transfer Protocol and in the Hypertext Markup Language serve very different purposes, even though some information may be contained in both (like the book title or year of publication in our metaphor) while others only make sense in one of the two places (like the date of delivery in a packing slip and the names of illustrators in an imprint).

106 Returning to the introductory example, tagged metadata make up most of the "eighty lines [...] in machine language" mentioned in marginal 8. Hence, rightsholders might consider "using tags" as "a predefined format/syntax" for their TDM reservations.[132] Indeed, the TDM Reservation Protocol[133] refers to HTML tags of the class <meta ...> as its second prong for communicating TDM reservations (rule 6.3 TDM ReP). This would use the same attributes as in the HTTP Response Header, namely "tdm-reservation" and "tdm-policy" with the values of 1 and the policy URL, respectively.

131 *Hartmann/Jacobsen* (n. 29) sub II.3); *Löbling et al.* (n. 57), 506: "meta tags could serve as suitable machine-readable methods to accurately convey opt-outs for TDM".

132 IBM (n. 56), p. 2.

133 See *supra* marginal 96.

107 Since a hypertext markup file can contain multiple <meta ...> tags, this would even let rightsholders distinguish between different contents of the same file, enabling them to set highly granular permissions. On the other hand, it only works in HTML-conformant files; the sole other format covered by the TDM Reservation Protocol are e-books in .epub format (rule 6.4 TDM ReP).

108 The standard envisioned by the TDM Reservation Protocol gets jeopardized by a considerable proliferation of HTML-based standards. Including the TDM ReP, at least five different <meta> tags have been proposed since 2012 to reserve TDM rights:

```
109  <meta name="CCBot" content="nofollow">[134]
     <meta name="robots" content="noai, noimageai">[135]
     <meta name="usage-rights" content="CC-BY-SA" />[136]
     <meta name="generative-ai" content="notraining">[137]
     <meta name="tdm-reservation" content="1"> <meta
     name="tdm-policy" content="…">[138]
```

110 Even the website of a major legal publisher known to be highly rights-sensitive uses just two of these five declaration standards.[139] Not to speak of other proposals that rely not even on <meta> tags, but on newly minted HTML attributes such as "data-notdm".[140]

VI. JavaScript Object Notation (tdmrep.json, Reich's ai.txt, C2PA)

111 The third and final protocol utilized by the World Wide Web Consortium's community group was JavaScript Object Notation (JSON), a language specified since 1997 in two standards (RFC 8259 und ECMA-404). The website in our introductory example does not seem to use this language yet, which is unsurprising given JSON's powerful-yet-demanding scripting syntax.

112 According to rule 6.1 of the TDM Reservation Protocol, reservations can be declared by placing a text file with the filename *tdmrep.json* in the root directory, wherein information get encoded as pairs of attribute (e.g., „vcard:hasEmail") and value (e.g., "mailto:contact@provider.com"). These can be grouped and nested – as is common in many machine languages – through brackets and indentation. This enables rightsholders to even encode legal obligations by implementing, for example, the "Open Digital Rights Language" (ODRL).[141] One such sample declaration might read:[142]

```
113  "permission": [{
            "action": "tdm:min",
            "duty": [{
              "action": "compensate"
              }]
      }]
```

114 This code snippet defines a "permission", wherein the permissible "action" (of text and data mining) is coupled with a "duty", which itself is an "action" (of compensating). In other words, the code contains a contractual offer for a paid TDM license.[143] This syntax for what is essentially an automatable "smart contract" transcends any simplistic Allow/Disallow dichotomy and empowers users to create more complex obligations which actually serve the Directive's objective of market creation (see *supra* marginal 30 at the end). Insofar, this component of the TDM Reservation Protocol is truly visionary. At the same time, it is by far the most demanding (and, consequently, error-prone) coding language yet proposed in the TDM reservation context.

115 It is not unique either. In a "Guide for Preparing Website Content for Large Language Models" published online on 18 May 2023,[144] AI entrepreneur *Robert Reich* proposed another standard, meant to be "more akin to RSS feeds than robots.txt",[145] which is seemingly JSON based. In addition to lacking a public documentation, it shares another point in common with the Spawning protocol discussed earlier: It is meant to be published in a file called ai.txt. This

134 Common Crawl FAQ since 6 Dec 2012 <commoncrawl.org/faq>.

135 DeviantArt, 'UPDATE All Deviations Are Opted Out of AI Datasets', 11 Nov 2022 <deviantart.com/team/journal/UPDATE-All-Deviations-Are-Opted-Out-of-AI-Datasets-934500371>, using yet another "robots" attribute originally designed for search engines.

136 *Wiese* (n. 102) without clarifying how a prohibition against TDM should be communicated.

137 *Bustos*, 'Generative AI in web development. A new AI meta tag?', LinkedIn on 29 Jul 2023 <linkedin.com/pulse/generative-ai-web-development-new-meta-tag-eduardo-bustos>, proposed less in view of article 4(3) CDSMD, but in view of excluding AI *output* from future training in order to avoid "feedback loop[s] result[ing] in a degradation of the model".

138 Rule 6.3 TDM ReP, see marginal 106.

139 See *supra* marginal 9.

140 Notably, *Löbling et al.* (n. 57), 509.

141 See ODRL Information Model 2.2 (W3C Recommendation) of 15 Feb 2018 <w3.org/TR/odrl-model>.

142 From example 14 in rule 7.1.5.3 TDM ReP.

143 The snippet does not define the price (as an *essentiale negotii*) but it could be specified using the "payment" element and its attributes, see example 21 in the ODRL Information Model (n. 141).

144 User *menro*, ai.txt, accessed 7 Mar 2024 <github.com/menro/ai.txt>.

145 User *menro* (n. 144).

naming collision raises another complication that has yet to be addressed: How should crawlers determine which syntax to expect in a given reservation file, and subsequently to select the appropriate parsing scheme? Any less-than-perfect standardisation would thus depend on additional layers of higher order meta-rules, if not on mere trial and error – both of which undesirable from a standardisation perspective.

116 Lastly, JSON and related languages are also used within much more sophisticated software architectures. One that was casually mentioned in legal literature[146] is the C2PA framework by the "Coalition for Content Provenance and Authenticity".[147] Among its many purposes, it allows users to reserve TDM uses (rule 19.21 C2PA Specifications) through code such as the following:[148]

```
117 {
      "entries":
         "c2pa.ai_training" : {
                  "use" : "allowed"
         },
         "c2pa.ai_generative_training" : {
                  "use" : "notAllowed"
         },
         "c2pa.data_mining" : {
                  "use" : "constrained",
                  "constraint_info" : "may only be mined on
    days whose names end in 'y'"
         }
    }
```

118 This example illustrates three of the four possible entries defined by rule 19.21 of this protocol, each taking one of the three states of "use", where a "constrained" use allows all sorts of complex conditions (as illustrated in the example). What distinguishes this declaration from the JSON examples discussed earlier, is that it is not meant to be encoded in a simple text file that anyone could open using any text editor. Instead, the Coalition for Content Provenance and Authenticity designed a complex framework where the text of this declaration gets wrapped into a cryptographically signed "claim" which is then embedded, along with other claims, as a "manifest" into the header data of a binary file. Never mind the technical details of this process. Its consequences are threefold:

119 For one, the use of cryptography (rule 14 C2PA Specifications) means that such reservations cannot simply be created or read by humans. Rather, the "claim generator" specifically needs to be "non-human (hardware or software)" as per rule 2.1.3 C2PA Specifications. While from an engineering perspective this cryptographical element increases trust, it reduces legal transparency – and raises the question whether "machine-readable" reservations under article 4(3) CDSMD need not *also* be human-readable. At the very least, non-human-readability poses a major practical obstacle to expressing, revising, and communicating TDM reservations.

120 A second consequence of this architecture is that its output can be embedded into binary file formats (specifically, images and pdf files, see rule 3.4 C2PA Specifications) that are not amenable to some of the previously discussed protocols.[149]

121 Conversely, however, this means that the same reservation can no longer be embedded into the simplest types of content (such as text files on a server), including most that rely on plain text (such as websites). Given that our introductory example focussed on just this kind of textual data, the Content Provenance and Authenticity framework is unhelpful in reserving TDM rights for it. What these considerations ultimately suggest is that a general standard for reserving rights across different file formats is unlikely ever to transpire.

VII. Technical Protection Measures (Paywalls, CAPTCHA, Poisoning)

122 As a last way to deter crawlers (and one we observed in our introductory example, marginal 15), rightsholders could simply conceal their contents behind a login screen ("paywall") or Turing test ("CAPTCHA"), which essentially makes them invisible to naïve web-scraping algorithms. Thus far, it is still an "open issue" how the reservation of TDM rights "might correlate with the existing rules on technical protection measures (TPM) and rights management information (RMI) under the InfoSoc Directive."[150] Essentially there are two very different ways in which TPMs may become relevant in the context of TDM reservations:

123 Firstly, the Directive allows rightholders "to apply measures to ensure that their reservations [...] are respected" (recital 18 subpar 2 CDSMD). This implies that a non-self-enforcing reservation may get protected through "effective technological measures" as defined in article 6(3) InfoSocD. In such cases, the European Directives require

124 "appropriate measures to ensure that rightholders make available [...] means of benefiting from that

146 *Löbling et al.* (n. 57), 507; *Keller/Warso* (n. 76), p. 9.

147 Technical Specifications v1.3 as of April 2023 available at <c2pa.org/specifications/specifications/1.3>.

148 Example from rule 19.12.1 C2PA Specifications (n. 147).

149 For instance, HTML/epub tags, see *supra* marginal 107.

150 *Mezei* (n. 13), 465.

exception or limitation [...] where that beneficiary has legal access to the protected work or subject-matter concerned." – article 7(2)2 CDSMD conjoined with article 6(4) subpar. 1 InfoSocD

125 This means that even "effective" technological measures cannot safely preclude TDM on reserved contents, because AI developers and other users could "request that such technological measure [...] be disapplied towards them."[151]

126 Secondly, in addition to merely "ensuring respect" for declared reservations, technological precautions may themselves be interpreted as *de facto* means of reserving rights. In the context of website framing, the European Court of Justice has argued that

127 "in order to ensure legal certainty and the smooth functioning of the internet, the copyright holder cannot be allowed to limit his or her consent by means other than effective technological measures, within the meaning of Article 6(1) and (3) of Directive 2001/29."[152]

128 If this applied not just to framing, but also "by analogy" to TDM reservations,[153] all previously discussed communication protocols would appear unsuitable, as "any software agent can simply ignore" them.[154] For instance, the Robots Exclusion Protocol (C.II.) cannot "qualify as a technical barrier because any software agent can simply ignore the 'Disallow' command without actively forcing any digital fence."[155] The fact that no reservation language constitutes any "access control or protection process" within the meaning of article 6(3)2 InfoSocD might explain why some authors seem to limit "machine-readable means" to "systems used to *prevent* the algorithm from mining the contents of a source",[156] such as paywalls or CAPTCHAs.

129 However, mere factual hurdles cannot constitute even an implicit declaration in the legal sense, let alone an "express" declaration as required by article 4(3) CDSMD. The doctrinal framework developed earlier (supra B.) and the explicit wording of the pertinent Directives do not support such a restrictive interpretation. Specifically, the AI Act's obligation for AI developers to ensure "respect" for "reservations of rights"[157] does not make sense if reservations needed to be self-enforcing anyway. Hence the legislator clearly implies that reservations *cannot* be "effective" as per article 6(3)2 InfoSocD.

By the same logic, other "anti-TDM practices" (i.e., "options to limit the TDM activities of GenAI developers")[158] cannot constitute a reservation of rights either. A notable example would be "poisoning" strategies that have made most progress for image files: Researchers at the University of Chicago introduced a software called *Glaze* to carry out "Prompt-Specific Poisoning Attacks on Text-to-Image Generative Models"[159] by modifying pictures in a manner invisible to humans, but adversarial to AI algorithms who subsequently misclassify dogs as cats, handbags as toasters, or STOP signs as birds.[160] While the safety implications of the last example may exert *de facto* pressure on AI developers to scrutinize their data sources and exclude unlicensed materials, it is hard to imagine how this might work for text. A more promising approach in this respect was proposed by Spawning who in addition to their ai.txt protocol (see supra C.III.) also offer a program called *Kudurru*, which is meant to automatically identify server requests by AI spiders and respond to them with useless pseudo-content.[161] This might be feasible for text, but would still "be far from being right[s] reservations per the CDSM Directive".[162]

D. Summary and Outlook

130 In lieu of a conclusion, the last section of the paper will summarize the previous discussions in tabulated form (I.), discuss potential legal and technological reactions to the current proliferation of proposed standards (II.), and suggest an avenue towards effective standardisation through the newly established AI Office (III.).

151 *Rosati* (n. 19), 90–91.

152 Case C392/19 (*VG Bild-Kunst v. Stiftung Preußischer Kulturbesitz*), Judgement of 9 Mar 2021 (ECLI:EU:C:2021:181), marginal 46.

153 As has been argued, most prominently, by *Rosati* (n. 19), 90.

154 See *supra* at marginal 83.

155 *Ducato/Strowel* (n. 36), 674 (stating too cautiously that "[s]ome authors have argued that").

156 *Romain Meys*, 'Data Mining Under the Directive on Copyright and Related Rights in the Digital Single Market: Are European Database Protection Rules Still Threatening the Development of Artificial Intelligence?' (2020) 69 GRUR Int. 457, 466 fn. 157 (italicized here), and further: "In the absence of such systems, it should be assumed that the source can be freely mined."

157 See *supra* marginal 51.

158 *Mezei* (n. 13), 467.

159 Thus is the title of *Shan et al.*, arXiv Working Paper v1 of 20 Oct 2023, v2 of 16 Feb 2024 <arxiv.org/abs/2310.13828v2>.

160 See figure 7 on p. 8 of the pdf-Version of *Shan et al.* (n. 159).

161 *Knibbs*, 'A New Tool Helps Artists Thwart AI—With a Middle Finger', WIRED of 12 Oct 2023 <wired.com/story/kudurru-ai-scraping-block-poisoning-spawning>.

162 *Mezei* (n. 13), 467.

I. Summary of Proposed Reservation Standards

131 In order to summarize the discussions in the previous section, the following table lists, for each subsection, the language involved, the number of proposed standards in that language (which were reviewed hereinbefore), the language's three main limitations, and whether it is suitable to fulfil the requirements of expressivity ("xp?") and machine-readability ("mr?") under article 4(3) CDSMD.

¶	Language	variants	main limitations	xp?	mr?
C.I.	natural language (e.g., English)	∞	■ sufficiently standardized expression unfeasible ■ no default location and file format for T&Cs, etc. ■ placement in central location is not content-specific	√	X
C.II.	Robots Exclusion Protocol (REP)	1	■ syntax does not allow for use-specific reservations ■ placement in central location is not content-specific ■ parsing limit precludes content-specific reservations	X	√
C.III.	Spawning Protocol	1	unclear due to lack of documentation; resembles REP	?	√
C.IV.	Hypertext Transfer Protocol (HTTP)	3	■ no widespread adoption of recent proposals yet ■ competing variants may hamper standardisation ■ syntax unsuitable for license contracts → JSON?	√	√
C.V.	HyperText Markup Language (HTML)	6	■ strictly limited to HTML-conformant text files ■ competing variants strongly hamper standardisation ■ syntax unsuitable for license contracts → JSON?	√	√
C.VI.	JavaScript Object Notation (JSON)	3	■ demanding syntax hampers widespread adoption ■ placement in central location is not content-specific ■ use of cryptography may upend human-readability	√	√
C.VII.	none (merely TPM)	4	mere technical protection has no expressive content	X	X

II. "Standards are great. Everyone should have one!"

132 Looking back on the standards that have been proposed and occasionally discussed in legal writing, one is reminded of a decades-old engineering quip:

> "The nice thing about standards is that you have so many to choose from"[163]

133 Technologists and lawyers will approach this situation differently:

Technologically speaking, so long as hopes for standardization or "best practices or codes of conduct" remain vague,[164] there will inevitably be cases where multiple expressions in different languages contradict. To resolve such contradictions, rules are needed to establish a meta-hierarchy of standards. For instance, the TDM Reservation Protocol contains a rule on "processing priority" for the communication protocols recommended by the standard (rule 6.5 TDM ReP). One would need similar interpretive meta-rules when other standards collide.[165]

163 *Tanenbaum*, 'Computer Networks' (1981), 168.

164 *Mezei* (n. 13), 468.

165 For one particular context, see *supra* marginal 115.

134 Legally speaking, while some standards can be ruled out as insufficiently machine-readable under article 4(3) CDSMD (supra I.–III., VII.), the remaining protocols (IV.–VI.) exhibit as much variation as any file format on the Internet. This is unsurprising given the legislator's intent of market-creation. For instance, one standard discussed herein (C.III.) was proposed by a commercial startup as merely a conduit to selling its actual proprietary product (namely, its "Spawning API"). Unsurprisingly then, market incentives lean towards fragmentation rather than standardisation.

III. The Standard of the Future, in the Near Future?

135 The current fragmentation is ample encouragement to continuously collect candidate standards,[166] but we need not stop there. Again, there are at least two perspectives one might take in reaction to the foreseeable difficulties in establishing a standard.

136 Skeptics may point out that "the author will not necessarily benefit directly" from standardized TDM reservations anyway; rather "it will likely be the big rightsholders that will license the uses".[167] Indeed, the large majority of small creators can barely keep an eye on the developing landscape of reservation standards, let alone properly implement the requisite standard(s). Only resourceful repertoire owners have the capacity needed to understand and implement each of the available standards – some of which (like the REP) may seem "trivial",[168] others (like JSON) so demanding that not even large commercial publishers (like the one in our introductory example) have begun using them. This may be for the better because it is still far from clear whether repertoire owners are authorized to even declare reservations on behalf of content creators.[169]

137 Futurists may respond that creators might reassume control as soon as standardization issues get resolved "in an abstract, quasi legislative way"[170] by the European AI Office established under article 64 AI Act in January 2024.[171] Under article 56(1)–(2) and recital 116 AI Act, this Office should "encourage and facilitate the drawing up of codes of practice" that "cover at least the obligations provided for in Articles 53 and 55". This includes the obligation under article 53(1)c AI Act to respect reservations of TDM rights. Hence, the tasks of legally defining machine-readability and of specifying a (hopefully user-friendly) protocol through which rights should be reserved both fall within the AI Office's authority. This is especially evident in light of its responsibility under article 56(8)2 AI Act to "assist in the assessment of available standards".[172]

138 As always though, whether standard-setting ultimately helps to solve, or even to tackle, the most relevant practical problems remains yet to be seen.[173]

166 See GitHub user *healsdata*, Repository AI Training Opt Out, accessed 7 Mar 2024 <github.com/healsdata/ai-training-opt-out>.

167 *Geiger* (n. 15), 78.

168 *Sag* (n. 100), 1667: "The monetary cost of using the Robots Exclusion Protocol is zero and the information costs are not significantly higher. Adding a robots.txt file to a website is trivial".

169 See (in German) *Hamann* (n. 1), 137–140 (D.V.). In addition, insofar as the reservation of TDM rights is seen as protecting moral rights (see *supra* marginal 30), signing it over may not be straightforward.

170 *Peukert* (n. 22), 504: "meta-regulation of the AI Act could help to resolve these open issues much faster than the conventional copyright system".

171 See Commission Decision C (2024) 390 of 24.1.2024 establishing the European Artificial Intelligence Office, available at <ec.europa.eu/newsroom/dae/redirection/document/101625>.

172 Once any standard gets laid down in a code practice, article 53(4) AI Act would allow model providers "to demonstrate compliance" by relying on this code of practice "until a harmonised standard is published".

173 Skeptically *Senftleben* (n. 20), 1546: "[e]ven if standardized rights reservation protocols – capable of expressing remuneration wishes and modalities – become available, it is unclear whether copyright holders and collecting societies will ever manage to create efficient, pan-European rights clearance solutions that offer reliable and well-functioning payment interfaces with the technical safeguards"; similar challenges will plague more optimistic proposals of a "New Limitation-Based Remuneration Right" for AI developers, such as *Geiger* (n. 15), 78–81.

The Data Act & Policy Options for a Sectoral Regulation to Protect Competition in the Automotive Aftermarket

by **Daniel Gill** *

Abstract: The European Data Act seeks to end the exclusive control of device manufacturers over IoT data in order to open secondary markets for innovative data-driven services. One of the sectors where the Data Act may have disruptive potential is the automotive aftermarket. Here, vehicle manufacturers and third-party service providers have debated access to "vehicle data, functions and resources" for nearly a decade. Despite the acknowledgement of the European Commission that the vehicle manufacturers' data governance concept may be anticompetitive, this issue is still unregulated. The Data Act could potentially offer a solution to this problem, however due to a series of general shortcomings and sector-specific application issues, it fails to open the automotive aftermarket for innovative third-party services. Aware of this, the European Commission published an initiative for a sectoral regulation on access to vehicle data, functions and resources. While the Data Act and sectoral regulation in principle pursue similar objectives, they have different approaches. This raises the question how the lex-specialis should be designed in order to protect competition in the automotive aftermarket in the light of an enacted Data Act. Finally, this article provides policy recommendations for such a sectoral access regulation.

Keywords: data act, sector regulation, connected cars, data access, data sharing

Recommended citation: Daniel Gill, The Data Act & Policy Options for a Sectoral Regulation to Protect Competition in the Automotive Aftermarket, 15 (2024) JIPITEC 122 para 1.

A. Introduction

1 The Data Act (DA) introduces new data access and sharing rights for users of IoT devices and an obligation for the data holder to conclude a contract with the user about the utilization of the IoT data.[1] Through these means, the Data Act aims to solve the problem that manufacturers – by the technical design of the IoT device – gain exclusive control over the generated data, which often leads to insufficient data access for users and third parties, resulting in numerous problems for competition and innovation in data-driven secondary markets. This article analyzes the effects of the Data Act on competition and innovation in the automotive aftermarket, which is particularly relevant due to a controversial policy debate that currently exist between car manufacturers and third-party services regarding

* Daniel Gill: Research Assistant, Marburg Centre for Institutional Economics, School of Business & Economics, Philipps-University Marburg, daniel.gill@wiwi.uni-marburg.de. The author declare that he has no affiliation with or involvement in any organization or entity with any financial interest in the subject matter or materials discussed in this article.

1 Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonized rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act).

access to vehicle data and technical interoperability of the vehicle. This discussion is directly linked to the well-known problem of the protection of competition in the automotive aftermarket through mandatory access to essential repair and maintenance information and interoperability with the on-board diagnostic interface, within the sectoral type approval regulation.[2] While this regime has been found to successfully protect competition in the automotive aftermarket,[3] past reforms, despite the acknowledgement of arising competition problems by the Commission (in 2018), have failed to adapt the regime to the digitalization of the vehicle.[4] In 2022, the Commission made a first step into the direction of regulating this issue by publishing a call for evidence for an impact assessment for the initiative "access to vehicle data, functions, and resources".[5] Initially, Commission adoption was planned for the 2nd quarter of 2023, however nothing has happened so far. Currently (as of July 2024) Commission insiders expect that delay to continue.

2 The connected car example offers the opportunity to analyze both, the direct effects of the Data Act and the need for additional sectoral regulation, as well as the policy options for the sectoral regulation in the light of the Data Act. To what extent can the Data Act solve the problem of access to vehicle data, functions, and resources? Are additional sectoral rules necessary? And where might there be conflicts? First, this requires an analysis of the problems of the currently applied data governance model of connected cars and a brief overview of the policy discussion in this sector (section B). In a second step, it will be analyzed why the Data Act is no solution and why an additional sectoral regulation is still needed (section C). This is followed by a critical analysis of the sectoral initiative and policy recommendations for a sectoral regulation (section D). The conclusion summarizes the main results and points to alternative, more far-reaching regulatory approaches (section E).

B. The Policy Discussion on Access to Vehicle Data, Functions and Resources

3 The car manufacturers have repeatedly tried to foreclose independent competition (in the relatively profitable) automotive aftermarket by refusing access to essential information. Ultimately, this behavior led to the introduction (in the Motor Vehicle Type Approval Regulation) of the obligation of vehicle manufacturers to provide unrestricted, standardized and non-discriminatory access to repair and maintenance information (against reasonable and proportionate fees) as well as to ensure interoperability with the on-board diagnostic interface for all third parties operating in the aftermarket. Moreover, it provides a list of affected information and lays down the technical requirements for this access.[6] This sectoral technological regulation can be seen as one of the first FRAND (Fair, Reasonable And Non-Discriminatory)-like data access and interoperability solutions. An evaluation by the EU Commission in 2014 confirmed that overall, this system has successfully preserved competition in the aftermarket, albeit issues around vehicle connectivity are emerging.[7] Fueled by this new technology, these issues developed into a controversial policy discussion on access to vehicle data, functions and resources between vehicle manufacturers and third parties in 2016. Starting point of this debate is the so-called "Extended Vehicle", a technical architecture – standardized and applied by all vehicle manufacturers – that establishes a closed (non-interoperable) system that channels every communication with the vehicle

2 Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC.

3 Ricardo-AEA, Study on the operation of the system of access to vehicle repair and maintenance information – Final Report, 2014, available at: <https://op.europa.eu/en/publication-detail/-/publication/c2c172a5-3f49-4644-b5bb-c508d7532e4a> last accessed 02.07.2024, 133-134.

4 European Commission, Communication On the road to automated mobility: An EU strategy for mobility of the future, COM(2018) 283 final. European Parliament, Resolution of 13 March 2018 on a European strategy on Cooperative Intelligent Transport Systems, OJEU C162/2; European Parliament, Resolution of 15 January 2019 on Autonomous driving in European transport, OJEUC411/2.

5 European Commission, Call for evidence for an impact assessment for the initiative "Access to vehicle data, functions and resources", Ref. Ares(2022)2302201. There is no clear definition of the terms "functions" and resources" and they are oftentimes used interchangeable in the literature. Here, access to vehicle functions refers to the possibility of remotely activating vehicle functions such as unlocking doors (e.g. for shared mobility services) or diagnostic functions (e.g. for roadside services), but also more safety/security critical functions such as braking or steering. Access to vehicle resources on the other hand refers to the opportunity to communicate with the vehicle user (e.g. by displaying information on the dashboard).

6 Regulation (EC) No 715/2007 of the European Parliament and of the Council of 20 June 2007 on type approval of motor vehicles with respect to emissions from light passenger and commercial vehicles (Euro 5 and Euro 6) and on access to vehicle repair and maintenance information, OJEU L 171/1.

7 See Ricardo-AEA (n 3).

through the proprietary backend server of the respective manufacturer.[8] This implies the exclusive control of car manufacturers over the vehicle data, the technical (write) access to the car, and the means to directly communicate with the vehicle user (through the vehicle dashboard). Therefore, if a third party needs access to the vehicle or its data in order to develop, offer, or perform a service, direct access to (via the vehicle user, e.g., through apps) is not possible, but has to be organized through the Extended Vehicle based on individually negotiated contracts between manufacturer and third party.[9] This exclusive control is exacerbated by the fact that the majority of vehicle data, functions and resources in question are unique, non-substitutable, and inimitable, i.e., wherever a third party wants to perform a specific service for a particular vehicle, specific vehicle data, functions and resources are necessary. This setting provides car manufacturers with control over the aftermarket (and all other data-driven secondary markets), and therefore a gatekeeper position that allows them to make market entry of third parties conditional on contractual agreements. Thereby, the manufacturers have – in addition to strong incentives –sufficient means to leverage this position into secondary markets and to foreclose competition. This situation is susceptible to all sorts of anticompetitive strategies, which range from discrimination regarding the prices and conditions of access, to a full access refusal. Both may lead to the exclusion of third parties from the aftermarket. For the "locked-in" users of the connected cars this implies that they can only choose between service providers that have been allowed by the car manufacturer. Access via the on-board diagnostic system as mandated by the Type Approval Regulation offers no comparable access opportunities (both, regarding quantity and quality of access) for third parties. Consequently, competition, innovation and consumer choice are restricted, i.e., the automotive aftermarket fails to deliver efficient market results.[10]

4 This problem is not limited to the automotive aftermarket, but affects potentially all secondary markets that could benefit from technical access to vehicle and its data, and may lead to significant welfare losses due to inefficient levels of competition and innovation. Therefore, this limited access is a problem for the whole ecosystem of connected cars and the mobility system in general. Ultimately, this debate is about how open or closed cars should be as a key element of the bigger (mobility) system?[11]

5 In the policy debate on the Extended Vehicle, there are two important additional arguments. First, strong competition on the primary market will force car manufacturers to choose a more open and interoperable approach, and second, no alternative system could be as safe and secure. Regarding the first argument, the application of the economic theory of aftermarkets suggests that there is no competition between the vehicle systems (bundles of cars and the services available in the respective ecosystems) of the different manufacturers.[12] With respect to the second point, alternative systems have been developed that are less anticompetitive, and can also be made safe and secure.[13]

6 These alternative technical architectures cannot be discussed in detail here; however, they play an important role for the question of how to move forward with the sectoral regulation and are thus outlined in the following. The superior technical architecture according to the important study on "Access to In-Vehicle Data and Resources" is the "on-board application platform", an open interoperable telematics platform – and thus a totally different technological solution – which would enable car users to install third party applications directly in the vehicle – comparable to a smartphone – and decide directly about the access to vehicle data and

8 For a seminal study about this conflict see: Mc Carthy et al., Access to In-Vehicle Data and Resources – Final Report, 2017, available at: <https://transport.ec.europa.eu/system/files/2017-08/2017-05-access-to-in-vehicle-data-and-resources.pdf> last accessed 02.07.2024. For the basic ExVe concept see: ACEA, Position Paper – Access to in-vehicle data, 2021, available at: <https://www.acea.auto/publication/position-paper-access-to-in-vehicle-data/> last accessed 02.07.2024.

9 In this regard, "direct" access for third parties means access to vehicle data, functions and resources authorized by the user, but without the need to negotiate with the vehicle manufacturer. In practice, the user would authorize a third party service e.g., by concluding a service contract, or by giving its consent to an application.

10 For similar conclusions see: Kerber, Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data, JIPITEC 9, 2018, 310-330; Kerber/Gill, Access to Data in Connected Cars and the Recent Reform of the Motor Vehicle Type Approval Regulation, JIPITEC 10, 2019, 201-213; and Martens/Mueller-Langer, Access to digital car data and competition in aftersales services, Digital Economy Working Paper 2018-06, JRC Technical Reports, 2018, 7-10.

11 Determann/Perens, Open Cars, Berkeley Technology Law Journal, Vol. 32(2), 2018, 915-988.

12 This is also because of a limited ability of customers to consider the value of these services at the point of purchase, and a limited ability of customers to switch to other vehicle brands once the car has been purchased. See: Hawker, Automotive aftermarkets: A case study in systems competition, The Antitrust Bulletin Vol. 56(1) 2011, 57-79.

13 See: McCarthy et al. (n 8) 77; Bartsch, et al., On-Board Telematics Platform Security, 2020, available at: <https://www.tuvit.de/en/news/press-releases/press-release-detail/article/tuevit-specifies-cybersecurity-architecture-for-on-board-telematics-platform-otp/> last accessed 02.07.2024.

technical interoperability. A compromise solution is the "shared server", a data trustee solution which would put all vehicle data under the governance of an independent (neutral) entity, that can give non-discriminatory access to all stakeholders (including car manufacturers), the data economy (e.g. via data markets), and public authorities.[14]

7 Against this background, third parties (since 2016) demand a reform of the Type Approval Regulation. A reform in 2018 essentially failed to update the regulatory system to the new technology of connected cars and thus ignored the problem of access to vehicle data, functions and resources.[15] The impact assessment for the sectoral regulation that has been executed in 2022 has not been published until today, and therefore this market failure remains unsolved. The Data Act, although of horizontal scope, provides the first applicable rules that directly impact this long-standing policy debate and could be seen as a potential solution.

C. The Data Act – A Solution for the Problem of Access to the Vehicle and its Data?

8 The Data Act aims to tackle competition and innovation problems in secondary markets (similar to the case at hand) by breaking open existing data silos to facilitate data sharing and data utilization in the EU.[16] From a competition policy perspective, the key problem that the Data Act wants to solve is that manufacturers of IoT devices can obtain– through the technical design of the device,– exclusive de facto control over the generated data, with the consequence that users are unable to access and share the data they (co-)generated. As a result, third parties have only limited access to essential data, which restricts their ability to develop innovative services that can compete with those services offered by the device manufacturer.[17] Or, as Podszun and Offergeld put it: "In the data economy it is easy to block access by technical or legal means; if you cannot access the data of a smart device or system, you are quickly out of the game."[18]

I. Overview of the Data Act`s Rules on Data Sharing and Related Discussions

9 The basic approach of the Data Act to facilitate data sharing relies on the user who gets allocated the inherent value of the data and is basically free in its use and monetization.[19] To empower the user to fulfill this role, the Data Act obliges manufacturers to design the IoT product in a way that the data is easily, and where relevant and technically feasible, also directly accessible to the user by default (Art. 3(1) DA).[20] If this direct (on-device) data access is not possible, the user can demand that the data be made available (Art. 4(1) DA).[21] In addition, the Data Act provides a direct way for the user to share data with third parties, either upon request by a user or by a party acting on its behalf (Art. 5(1) DA).[22] In theory, this enables different options for the user to share data with third parties: (1) by making data available to a third party directly through the device,[23] (2) by downloading data from the manufacturer and making it available to a third party,[24] as well as (3) by requesting the manufacturer to share the data

14 For detailed descriptions of these technological alternatives and the finding that the On-Board Application Platform may be superior to the Extended Vehicle when it comes to its effects on competition and innovation in the automotive aftermarket, see: Mc Carthy et al. (n. 8).

15 Regulation (EU) 2018/858 (n 2). For an analysis of the reform of the TAR in 2018 see: Kerber/Gill (n 10).

16 Bomhard/Schmidt-Kessel, EU-Datengesetz ante portas, MMR 2024, 69, (69).

17 Regulation (EU) 2023/2854 (n 1) Rec. 20; Kerber, Data Act and Competition: An Ambivalent Relationship, Concurrences 1/2023, 31.

18 Podszun/Offergeld, The EU Data Act and the Access to Secondary Markets, available at: <http://dx.doi.org/10.2139/ssrn.4256882>, 6.

19 Hennemann/Steinrötter, Der Data Act, Neue Instrumente, alte Friktionen, strukturelle Weichenstellungen, NJW, 2024, 1; Wiebe, Der Data Act – Innovation oder Illusion? GRUR 2023, 1569 (1572).

20 Easy, secure, free of charge access for the user to the data in a comprehensive, structured, commonly used and machine-readable format, and if relevant and technically feasible directly through the device.

21 In this case, the data have to be accessible to the user without undue delay, of the same quality as is available to the data holder, easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format and, where relevant and technically feasible, continuously and in real-time.

22 Under the same conditions as Art. 4(1), see (n 20).

23 Which is dependent on the manufacturers decisions whether this direct access is "technically feasible", whether accessible means that the user can actually receive a copy of the data or "in-situ" access, and whether this copy can be transferred to the third party.

24 While this "circumvention" possibility exists in theory, it is questionable how practical it is, since the user has to have the technical infrastructure in place to receive data from the manufacturer and to share it with third parties, probably continuous and in real-time. For consumers, this may cause prohibitively high transaction costs.

with a third party.[25] This way, the Data Act aims to stimulate innovation on secondary markets (esp. aftermarkets) while simultaneously trying to "avoid undermining the investment incentives for the type of product from which the data are obtained".[26] To achieve a balance between these seemingly conflicting objectives, the Data Act accepts the de facto control of the manufacturers over the data and thus relies upon a data governance model that is only limited through the initial contract with the user and the new user rights of Arts. 4 and 5 DA.[27]

10 The Data Act has been subject to discussions right from the first proposal, and it is still an open question whether it can fulfill its objectives, i.e., unfold innovative effects on data-driven secondary markets.[28] In the center of this discussion is the user-centric approach of the Data Act which, especially. in B2C scenarios, may not to be able to facilitate purpose-oriented data sharing.[29] In the following, the most important general arguments are summarized. First, it is surprising that a user-centric approach has been chosen for the Data Act instead of parallel usage rights, given that IoT data is largely perceived as co-generated data to which no exclusive legal position should be created in order to facilitate independent data use.[30] Second, the de facto control of the user (consumer) is much weaker than the Data Act suggests, because the contract of Art. 4(13) DA suffers from the same issues as consent under data protection law: the user faces many informational and behavioral problems regarding the handling of data;[31] no consumer protection rules are provided by the Data Act; the manufacturer can tie the sale of the device to the data use contracts, etc. As a result, users often will have to accept contracts in which they grant the manufacturer broad and long-term competences regarding the utilization of the data ("total buy-out contracts", "take-it-or-leave-it" situation).[32] Third, the data access and sharing rights suffer from a number of problems that make them inefficient. In general, there are too many restrictions and legal uncertainties for users and third parties;[33] difficult disputes may arise about the "reasonable compensation" or the protection of trade secrets, and the scope of data may be too narrow to enable innovative services. Regarding the last point, an additional problem is that the Data Act allows for "in-situ" access, i.e., instead of a data transfer, data access and processing can take place within the server of the manufacturer, which may often not meet the requirements of third parties.[34] Moreover, hardly any criteria are provided on data usability, i.e., the technical state of the data, which may also run counter to the objective of facilitating innovative services.[35]

11 Another important general discussion is about the relation of the Data Act and the General Data Protection Regulation (GDPR). This relationship is important for this article since the majority of

25 Subject to a negotiated "licensing contract" between manufacturer and third party with FRAND conditions and a reasonable compensation for the manufacturer (Regulation (EU) 2023/2854 (n 1) Arts. 8 & 9.).

26 Regulation (EU) 2023/2854 (n 1) Rec. 32.

27 Kerber, Governance of IoT Data: Why the EU Data Act Will not Fulfill Its Objectives, GRUR International 2023 Vol. 72(2), 120-135, (132); Kerber, EU Data Act: Will new user access and sharing rights on IoT data help competition and innovation?, Journal of Antitrust Enforcement 2024, 1-7, (3); Specht-Riemenschneider, Der Entwurf des Data Act – Eine Analyse der vorgesehenen Datenzugangsansprüche im Verhältnis B2B, B2C und B2G, MMR 9 2022, 809-826, (817).

28 See among others: Drexl, et al., Position statement of the Max Planck Institute for Innovation and Competition on the Commission's Data Act Proposal of 23 February 2022, at: <https://doi.org/10.2139/ssrn.4136484>; Specht-Riemenschneider (n 27); Podszun/Offergeld (n 18); Krämer, Improving the Economic Effectiveness of the B2B and B2C Data Sharing Obligations in the Proposed Data Act, CERRE Report (2022); Martens, Pro- and Anticompetitive Provisions in the Proposed European Union Data Act, Bruegel Working paper 01/2023; Metzger/Schweitzer, Shaping Markets: A Critical Evaluation of the Draft Data Act, ZEuP 2023, 42; Wiebe (n 19); Kerber (n 27 2023 & 2024); Hennemann/Steinrötter (n 19); Antoine, Datenzugangsrechte im finalen Data Act – Fortschritt, Rückschritt, neue Fragen? Schlüssel zur Förderung datengetriebener Geschäftsmodelle? CR 2024, 1-8; Eckardt/Kerber, 'Property Rights Theory, Bundles of Rights on IoT Data, and the EU Data Act', European Journal of Law & Economics 2024, Vol. 57, 113–143, <https://doi.org/10.1007/s10657-023-09791-8>.

29 The purpose in this case is to ensure competition and innovation in the automotive aftermarket. For the general discussion of a more purpose-based approach within the Data Act see Drexl et al. (n 28).

30 Drexl et al. (n 28) 19; Leistner/Antoine, IPR and the use of open data and data sharing initiatives by public and private actors, Study requested by the JURI committee, 2022, available at: <https://www.europarl.europa.eu/RegData/etudes/STUD/2022/732266/IPOL_STU(2022)732266_EN.pdf>, 81.

31 For an overview about such informational and behavioral problems see e.g.: Sibony/Micklitz/Esposito, Research Methodes in Consumer Law, 2018; Zamir/Teichmann, Behavioural Law and Economics, 2018.

32 Kerber (n 27, 2024) 4; Hennemann/Steinrötter (n 19) 7; Antoine (n 28) 6; Specht-Riemenschneider (n 27) suggests a ban in tie-ins, better cancelation possibilities and a limited contract duration.

33 Kerber (n 27, 2023) 125-128; Krämer (n 33); Podszun and Offergeld (n 18) 28.

34 Specht-Riemenschneider (n 27) 816; Podszun/Offergeld (n 18) 31-31.

35 Kim/Kwok, Data Usability as a Parameter of Rights and Obligations under the EU Data Act, Max Planck Institute for Innovation and Competition Research Paper No. 24-04.

vehicle data is considered personal data.[36] Basically, data sharing and data protection are in conflict. The question is in how far the GDPR limits data access and sharing under the Data Act. On the one hand, the data access and sharing rights also cover personal data (Art. 1(2), Rec. 35 DA); on the other hand, the Data Act is without prejudice to the GDPR (Rec. 7 DA). Therefore, both regulations apply in parallel when personal data is affected. For example, the information obligations of Arts. 13 & 14 GDPR complement the transparency obligations from Art. 3(2) DA. Also, the data portability right of Art. 20 GDPR applies parallel to the access and sharing rights of Arts. 4 and 5 DA. However, problems arise from this parallel application when it comes to the legal basis of the data processing. As Wiebe et al. (2023) explain, none of the existing legal bases (Art. 6(1) GDPR) appropriately serves as a general justification for lawful data processing in the case of the connected car and possible data access and sharing requests under the Data Act. Therefore, they conclude that the vehicle data should be anonymized as early as possible.[37] But if the data is anonymized, i.e., non-personal, the manufacturer can only use the data based on a contract with the user, and the user has the exclusive right to determine who can access, use and share the data for what purpose (Arts. 4(13) & 4(14) DA). As a result, the manufacturer faces interesting tradeoffs regarding the question whether or not to anonymize the data.[38] The following case specific analysis assumes that all vehicle data initially is personal data, esp. in typical repair and maintenance situations, where a specific user is receiving a specific service for a specific car based on individual-level data, however, in other situations, such as improvement of components, or traffic management it is assumed that the aggregated-level data that is relevant here, is anonymous data.

36 Commission Nationale Informatique & Libertés, 'Compliance Package – Connected Vehicles and Personal Data', 2017, available at: <https://www.cnil.fr/sites/default/files/atoms/files/cnil_pack_vehicules_connectes_gb.pdf> last accessed 02.07.2024, 5; Störing, What EU legislation says about car data – Legal Memorandum on connected vehicles and data, 2017, available at: <https://www.fiaregion1.com/wp-content/uploads/2017/06/20170516-Legal-Memorandum-on-Personal-Datain- Connected-Vehicles-www.pdf> last accessed 02.07.2024, 2; Metzger, Digitale Mobilität – Verträge über Nutzerdaten, GRUR 2019, 129-136, (131).

37 Wiebe et al., Studie zur Notwendigkeit und Ausrichtung von spezifischen Datenzugangsregelungen im Bereich des vernetzten Fahrzeugs in der Automobilwirtschaft, 2023, 77-78, available at: <https://www.bundesnetzagentur.de/DE/Fachthemen/Digitalisierung/Daten/Datenoekonomie/schlussbericht.html> last accessed 02.07.2024.

38 Bomhard/Schmidt-Kessel (n 16) describe this as "escape into data protection law".

II. Limitations of the Data Act as Solution for Access to the Vehicle and its Data

12 The mobility sector and the need for new rules "to ensure that existing vehicle type-approval legislation is fit for the digital age" were explicitly addressed in the explanatory memorandum of the Data Act proposal.[39] Consequently, the different roles defined by the Data Act fit quite well to the different stakeholder groups in this discussion: the car manufacturer suits the "data holder" definition of Art. 2(13) DA. The "user" according to Art. 2(12) DA can be the vehicle owner or driver, which can be a natural or legal person, [40] which seems to exclude passengers and bystanders although they are often captured by the data generation process.[41] However, the term "user" is also subject to several open questions, e.g., what happens when the device is sold, or when usage authorization (e.g. car sharing) ends.[42] "Data recipient" pursuant to Art. 2(14) DA would be third parties who either get data made available by the manufacturers directly under a legal obligation, or by request of the user.[43] The main question is whether the new instruments introduced by the Data Act are able to solve the data access problem in the automotive aftermarket. To answer this question, the following sections analyze: (1) limitations regarding the scope of data, (2) limitations regarding the data sharing mechanism, and (3) limitations regarding the utilization of data through data holders, users and third parties.

1. Limitations Regarding the Scope of Data

13 The Data Act "grants users the right to access and make available to a third party any product or related service data, irrespective of its nature as personal data, of the distinction between actively provided or passively observed data, and irrespective of the legal basis of processing."[44] Articles 4(1) and

39 European Commission, Proposal on harmonized rules on fair access to and use of data (Data Act) COM/2022/68 final, 6.

40 In this paper the term "users" is used for natural persons, i.e. consumers. In case the user explicitly is a legal person, the term "business user" is used.

41 For a narrower definition see: Drexl et al. (n 28) para. 59f.

42 Also general about the relations of the different stakeholders see: Schmitdt-Kessel, Heraus- und Weitergabe von IoT-Gerätedaten, MMR 2024, 77.

43 Similiar for the example of connected cars: Etzkorn, (Vertragliche) Datenzugangsansprüche nach dem Data Act, RDi 2024, 116 (118).

44 Rec. 35 DA. Art. 1(2) provides that the DA covers personal and non-personal data, and specifies that Chapter 2 applies

5(1) DA concretize this seemingly broad scope of data as the "readily available data, as well as the metadata that is necessary to interpret and use that data", without disproportionate effort, going beyond a simple operation.[45] Recital 15 DA clarifies that this includes data "which are not substantially modified, meaning data in raw form [...] as well as data having been pre-processed for the purpose of making it understandable and usable prior to further processing and analysis".[46] In contrast, information derived from this data as the outcome of additional investments is excluded. This formulation implies significant limitations to the scope of data, making it unsuitable for the purpose of maintaining competition in the automotive aftermarket.

14 First, the limitation to 'readily available data' that the manufacturer can obtain 'without disproportionate effort', or 'which the OEM designed to be retrievable' means that car manufacturers are not obliged to make vehicle data accessible that is not stored (volatile data)[47] or not retrievable without additional investments. As a consequence, the car manufacturers are free to decide which vehicle data to generate and cannot be expected to invest in the generation of additional data besides that which they use themselves. However, for competition in the aftermarket, especially for the creation of innovative services, it can be necessary to access certain categories of (volatile) data that are not stored in this form, because it provides specific insights (e.g., performance data of specific parts, that is only stored in case of a fault). Moreover, if the data generation is limited to data that the car manufacturers needs to generate in order to provide their own services, the potential of innovation (from market entrants) is also limited relative to the situation where all data is generated and made accessible that could be generated technically.

15 Second, the exclusion of derived and inferred data, together with the limitation to readily available data, ignores the problem that most of the data needed to provide aftermarket services has already been processed to a certain extent. This is also directly related to the question of the impact of intellectual property rights and trade secrets on the scope of data, since the majority of the generated data is directly processed through proprietary software (e.g., predictive maintenance algorithm or diagnostic tools). This aggregated and derived/inferred data is often more important for secondary markets, but only the manufacturers are able to apply value-generating data processing. Predictive maintenance, for example needs access to raw as well as aggregated data.[48] The approach of the Data Act to include pre-processed data, as well as the data necessary to make use of this data, is a right step towards a more purpose-based scope of data.[49] However, whether this is enough to ensure competition and innovation in the automotive aftermarket and other secondary markets is still unclear.

2. Limitations Regarding the Basic Data Sharing Mechanism of the Data Act

16 The Data Act acknowledges that users of IoT devices are often not able to obtain the data necessary to make use of secondary services.[50] To solve this problem, new data access and sharing rights are introduced, which complement the right to data portability of Art. 20 GDPR.[51] While Art. 20 GDPR has been found to have severe problems regarding its

to data concerning the performance, use and environment of connected products and related services.

45 Art. 2(17) DA. Further definitions: Product data: "data, generated by the use of a connected product, that the manufacturer designed to be retrievable, via an electronic communications service, a physical connection or on-device access, by a user, data holder or a third party, including, where relevant, the manufacturer" (Art. 2(15) DA). Related service data: "data representing the digitization of user actions or events related to the connected product, recorded intentionally by the user or as a by-product of the user's action, which is generated during the provision of a related service by the provider" (Art. 2(16) DA).

46 Rec. 15 further explains that "the term 'pre-processed data' should not be interpreted in such a manner as to impose an obligation on the data holder to make substantial investments in cleaning and transforming the data. Such data should include the relevant metadata, including basic context and timestamp to make the data usable, combined with other data (e.g. sorted and classified with other data points relating to it) or re-formatted into a commonly-used format."

47 Volatile data is raw data that is directly processed within the vehicle for a specific purpose and deleted immediately afterwards. This data is also often not transferred outside the vehicle due to bandwidth limitations and the costs of transferring and storing huge amounts of data.

48 Wiebe et al. (n 37) 62; Gill, The Data Act Proposal and the Problem of Access to In-Vehicle Data and Resources, available at SSRN: <http://dx.doi.org/10.2139/ssrn.4115443>, 11.

49 Data having been pre-processed for the purpose of making it understandable and useable prior to further processing and analysis, including data collected from a single sensor or a connected group of sensors, for the purpose of making the collected data comprehensible for wider use-cases. (Rec. 15 DA). In fact, the Data Act recognizes that these data are "potentially valuable to the user and support innovation and the development of digital and other services protecting the environment, health and the circular economy, including though facilitating the maintenance and repair of the products in question." (Rec. 15).

50 Regulation (EU) 2023/2854 (n 1) Rec. 20.

51 Regulation (EU) 2023/2854 (n 1) Rec. 35.

applicability,[52] the Data Act seems to have learned from this discussion by, on the one hand, abstaining from the limitations of Art. 20 GDPR,[53] and on the other hand, exceeding it by including non-personal data and metadata, and by mandating continuous and real-time data availability (where feasible). However, while it is debatable whether this mechanism can be effective in general, there are specific issues as to its ability to maintain competition in the automotive aftermarket, since (1) vehicle users may not claim their rights, and (2) the Data Act even protects the exclusive control of car manufacturers over the vehicle data.

17 Option one for the users would be to directly access the data on the device and make it available to third parties (Art. 3(1) DA). This seems unlikely for several reasons: the car manufacturer may decide to declare that this kind of access is technically not feasible (e.g., due to safety and security considerations), the data access may only take place in-situ, i.e., without the user receiving an actual copy of the data, and even if the user would receive such a copy, the interface would need to be designed in a way that allows the user to easily transfer the data to the third party (which the manufacturer is neither obliged to, nor incentivized by competition). Option two, namely to request data from the manufacturer, and to make it available to the third party (Art. 4(1) DA), would require the user to have the infrastructures available to download from the manufacturer and to upload to the third party potentially high volumes of real-time and continuous vehicle data, which seems unrealistic. The option remains to request that the manufacturer shares the data with a third-party (Art. 5(1) DA). It seems unlikely that the user will actively claim this right when there are transaction costs for making vehicle data available to third parties. This holds especially where the car users cannot directly identify whether and how much they benefit from the (additional) data sharing with the third party, and where the service in question is already offered (as default option) by the vehicle manufacturer. Take for example the situation when a car user has to decide between the manufacturer's official repair service and a third-party repair service. If it is cumbersome for the user to authorize the third party to access and use the data (e.g., because of a lack of information and experience), the price of the third-party service (including the compensation) plus the perceived transaction costs of providing access to vehicle data, has to be lower than the price of the manufacturer's service. The price for the third-party service could even increase if the data contains trade secrets, since, in this case, additional agreements are necessary to preserve the confidentiality of the data.[54]

18 These transaction costs depend strongly on the manufacturers' design of the interface with the vehicle user and how difficult it is for the user to request the data sharing, i.e., to authorize access by a third party. The Data Act seems to be aware of the implications of the design choice towards the transaction costs of the users and consequently obliges data holders (1) to design products and services in a way that the data is easily accessible and sharable for the user as well as usable (data interoperability) for users and third parties,[55] and (2) to provide the user with far-reaching information on the data that can be generated, whether it can be generated continuously and in real-time, where it is stored, how it can be retrieved, whether the data contains trade secrets etc.[56] However, despite these provisions, the car user may still be overburdened, especially. when facing multiple or repetitive situations of decisions regarding data sharing with a third party (e.g., privacy or consent fatigue).[57] One option against this problem could be to empower users to authorize a specialized third party (e.g., a data trustee)[58] to access, manage, and share the

52 See: Krämer/Senellart/de Streel, Making Data Portability More Effective for the Digital Economy, 2020, available at: <https://cerre.eu/publications/report-making-data-portability-more-effective-digital-economy/> last accessed 02.07.2024. For a detailed analysis of the practicability of Art. 20 GDPR for providing access to vehicle data for third parties in the automotive industry see: Gill/Metzger, Data Access through Data Portability - Economic and Legal Analysis of the Applicability of Art. 20 GDPR to the Data Access Problem in the Ecosystem of Connected Cars, European Data Protection Law Review, 8(2) 2022, 221 – 237.

53 E.g. regarding the nature of the data as personal or non-personal data, whether actively or passively observed, with respect to the legal basis of its processing, and whether or not it is technically feasible to port the data.

54 Gill (n 48) 13.

55 Art. 3(1) obliges the manufacturers to make the data "by default, easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format, and where relevant and technically feasible, directly accessible to the user." In addition, Art. 4(4) obliges the manufacturers to not make access to the data through the user "unduly difficult". Moreover, Rec. 27 demands that users should be given the necessary technical interface to manage permissions.

56 Regulation (EU) 2023/2854 (n 1) Art. 3(2).

57 See: Choi et al., The role of privacy fatigue in online privacy behavior, Computers in Human Behavior, Vol. 81, 2018, 42-51.

58 For approaches of data trustees in the area of mobility, see: Specht-Riemenschneider/Kerber, Designing Data Trustees – A Purpose-Based Approach, 2022, available at: <https://www.kas.de/de/analysen-und-argumente/detail/-/content/datentreuhaender-gesellschaftlich-nuetzlich-rechtlich-groessere-anforderungen-erforderlich> last accessed 02.07.2024); or, with a study about the concept of a "Mobilitätsdatenwächter", Reiter et al., Gutachten

data on behalf, and in the best interest of the user in order to further reduce transaction costs. This way, third parties could aggregate data from many vehicle users (and across brands) and provide all stakeholders with higher quality data sets regarding scale and scope. Article 5(1) DA explicitly includes this option.[59]

19 A more fundamental problem with respect to the basic data sharing mechanism is that the Data Act protects the de facto exclusive control of the manufacturer over the vehicle data. It does not provide third parties with a direct right to access the data and requires a negotiated agreement between data holder and third party which can lead to considerable problems and costs. The Data Act provides leeway for themanufacturers to make the data accessible either within the vehicle, or through their servers (Rec. 22), or to organize data availability for third parties in the form of "in-situ" data access (Rec. 8), which means that the third parties would not get a copy of the data, but would bring their algorithms to the manufacturers servers in order to derive insights.[60] At the same time, the Data Act is silent on the user's ability to directly transfer data for free to third parties in return for benefits without the approval of the data holder. According to Martens (2023) the Data Act does not want to open this possibility because it would undermine the data holder's ability to charge a price.[61] Although the user initiates the data sharing, the specific conditions of the data sharing agreement are subject to negotiations between data holder and third party based on the principles of contractual freedom.[62] Kerber (2022) states that this can lead to considerable problems (e.g., around the modalities of "FRAND" terms, or the reasonable compensation) and raise costs and delays that make the mechanism unattractive. Moreover, this contractual freedom may be problematic where there are imbalances in the negotiation power between data holder and third party, which may potentially lead to contractual terms that limit effective competition and innovation in the independent aftermarket. The Data Act provides a complex thicket of obligations regarding these contracts. The next section compares these limitations regarding the opportunities of data holders, users and third parties to make use of the data.

3. Unequal Opportunities Regarding the Utilization of the Vehicle Data

20 The Data Act regulates the contractual relationship between data holder, user and third party with the objective to prevent the exploitation of contractual imbalances.[63] It bases on the principle of contractual freedom to negotiate the conditions for making data available and provides asymmetric limitations to this freedom for data holders and third parties.[64] These unequal opportunities may distort competition and innovation in the automotive aftermarket. For the car manufacturers, the only restrictions, besides the general rules on unfair contractual terms of Art. 13 DA, seem to arise with respect to the pre-contractual information obligations of Art. 3(2) DA, the prohibition to derive insights about the commercial situation of the user of Art. 4(13) DA, and the prohibition of "dark patterns" in Rec. 38 DA (not reflected in the Articles). In contrast, for third parties, the Data Act provides a range of direct limitations. Art. 6(1) DA obliges the erasure of the data when no longer necessary for the agreed purpose (unless contractually agreed with the user), which may deprive third parties of the possibility to aggregate and store this data for any future (currently unknown) purposes. Art. 6(2)c DA prohibits data sharing with other third parties (unless contractually agreed with the user), which prevents better supply of vehicle data e.g., on data marketplaces and thus adds to the preservation of the gatekeeper positions. Art. 6(2)d DA prohibits third parties (and users, but not manufacturers) to share data with gatekeepers (designated pursuant to Art. 3 DMA), which is particularly critical due to the role of Google and Apple regarding automotive operating systems. Art. 6(2)e DA prohibits third parties to use the data to develop a product that competes with the manufacturer`s product, or to share the data with a third party with that intent, which "reduces the scope of legitimate data-driven innovations to not-too-close substitute products"[65] and raises legal risks for innovators.[66] Moreover,

– Einführung eines „Mobilitätsdatenwächters" für eine verbrauchergerechte Datennutzung – Notwendigkeit, Modell, gesetzliche Grundlagen, 2022, available at: <https://www.vzbv.de/sites/default/files/2022-11/22-11-15_Gutachten_Mobilit%C3%A4tsdatenw%C3%A4chter_BRC_2022-15-11_Clean_Finalversion.pdf> last accessed 02.07.2024.

59 See also Regulation (EU) 2023/2854 (n 1) Recs.: 26, 30, 33.

60 See critically Kerber (n 27) 124; Drexl et al. (n 28) 29. For a more positive understanding of "in-situ" access see: Martens et al., Towards Efficient Information Sharing in Network Markets, 2021, available at: <https://ssrn.com/abstract=3954932> last accessed 02.07.2024.

61 Martens (n 28) 11.

62 Regulation (EU) 2023/2854 (n 1) Rec. 43: "On the basis of the principle of contractual freedom, parties should remain free to negotiate the precise conditions for making data available in their contracts within the framework for the general access rules for making data available."

63 Regulation (EU) 2023/2854 (n 1) Rec. 5.

64 Regulation (EU) 2023/2854 (n 1) Rec. 43.

65 Martens (n 28) 14.

66 Graef/Husovec, Seven Things to Improve in the Data

the Data Act provides data holders (and users) with possibilities to (contractually) restrict the accessibility and sharing of the data, if security requirements (Art. 4(2) DA) or the confidentiality of trade secrets (Arts. 4(8) and 5(11) DA) would be undermined. These provisions may be abused by the car manufacturer in order to prevent data sharing based on safety and security consideration, which is particularly relevant for connected cars. There are no similar limitations for the manufacturers.[67]

4. No Technical Access to the Vehicle (Functions and Resource)

21 Most importantly, the Data Act does not regulate the interoperability of IoT devices with third party services, or in this case, access of third parties to the vehicle functions and resources. However, this access is critical for many innovative services for several reasons. First, similar to the existing (but technologically obsolete) on-board diagnostic interface, aftermarket services may need (remote) access to specific vehicle functions and resources in order to trigger certain events and, test functionality. Second, for some aftermarket services it may be necessary to install an application on-board the vehicle to directly access, aggregate and process relevant information, or activate certain functions and resources. If this is not possible, their services may be limited in functionality and quality. Third, direct access to the vehicle also implies opportunities to communicate with the driver (and/or passengers), without being dependent on mails or calls. If this ability is held exclusively by the vehicle manufacturers, they have an additional competitive advantage in offering services, i.e., they will be able to steer the consumers into their services (manipulation). The existing access to vehicle functions and resources through the on-board diagnostic interface does not provide sufficient access, since it is limited in scope and functionality and reflects only a minor part of the access opportunities of the manufacturers.[68]

III. Suitability of the Data Act to solve the Problem of Access to the Vehicle and its Data

22 Does the Data Act eliminate the exclusive de facto control of the car manufacturers over the vehicle data? No, but it may even strengthen it! Indeed, accessibility by design and the rights of users to access and share the data with third parties may have a positive effect on competition and innovation in the automotive aftermarket. However, this is based on the problematic assumptions that individual vehicle users are able to negotiate with the manufacturers about the terms and conditions and even dictate the purposes of the data processing,[69] and that the users will actively make use of their data sharing right. Both seem unrealistic given the potentially high transaction costs, uncertain benefits, and the ability of the manufacturers to offer these contracts on a "take-it-or-leave-it" basis. In fact, it can be argued that the users do not have meaningful control about their vehicle's data, which can be interpreted as another market failure due to informational and behavioral problems.[70] Moreover, the scope of data may not be fit for the purpose of maintaining effective competition. Most importantly however, interoperability of the IoT device with third party services is not regulated at all.

23 Despite its good intentions, the Data Act may in fact confirm the existing exclusive de facto control of the car manufacturers over the vehicle data

Act, 2022, 2 at: <https://ssrn.com/abstract=4051793> last accessed 26.06.24.

67 Another question is, in how far Art. 4(13) DA de facto limits the data utilization opportunities of the car manufacturers (for non-personal data). According to the literature, the manufacturer can make the sale of the vehicle conditional on the users' agreement on potentially far-reaching and long-term data usage because the user faces the same informational and behavioral problems that are well-known regarding the consent to the processing of personal data and the Data Act is nearly entirely silent on this initial contract and includes no specific rules for the protection of consumers. Therefore, it is widely expected that the manufacturers can offer "total-buy-out" contracts on a "take-it-or-leave-it" basis, which would allocate all rights to use, share and monetize the data to the manufacturers for the entire life-time of the vehicle (see: Kerber (n 27) 132; Wiebe et al. (n 37) 67; Specht-Riemenschneider (n 27) 817; Colangelo, European Proposal for a Data Act – A first Assessment, 2022, 17, available at: <https://cerre.eu/wp-content/uploads/2022/07/200722_CERRE_Assessment-Paper_DataAct.pdf> last accessed 02.07.2024).

68 See also Kerber/Gill, Revision of the Vehicle Type-Approval Regulation: Analysis and Recommendations, 2022, available at SSRN: <http://dx.doi.org/10.2139/ssrn.4174028>, 5.

69 Which may be true in specific B2B situations in which the business user is in the better negotiation position, but cannot hold for B2B situations where the business user depends on data access, or any B2C situation.

70 See: Kerber (n 27) 132. In the discussion about the Data Act there are a number of suggestions that would strengthen the position of the consumers, see: BEUC, Commission must take urgent action to protect consumers' data in the automotive sector, 2022, available at: <https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-009_action_to_protect_consumers_data_in_the_automotive_sector.pdf> last accessed 02.07.2024.

because it acknowledges, legitimizes, and protects this position.[71] First, the largely unrestricted initial contract between manufacturers and vehicle users, in relation to the highly restricted data utilization opportunities of third parties, grants the manufacturers a competitive advantage. Second, the Data Act neither provides direct access rights for third parties, nor is it self-evident that vehicle users are de facto able to directly transfer data to third parties for free in return for benefits without the approval of the data holder. Instead, the Data Act relies to a large extent on contractual freedom for negotiations between car manufacturers and third parties, potentially leading to many problems e.g., around the interpretation of FRAND conditions or the calculation of compensations. A sectoral regulation as announced multiple times in the Data Act,[72] and as called for by third parties, would have the opportunity to be much more targeted towards the purpose of competition in the automotive aftermarket.

D. Critical Analysis of the Policy Options for a Sectoral Regulation

24 Shortly after the Data Act proposal the European Commission published a call for evidence for an impact assessment for the initiative "access to vehicle data, functions and resources".[73] This initiative, if translated into a regulation and enacted, would reform the existing Type Approval Regulation for motor vehicles (with its rules on access to repair and maintenance information),,[74] through an (additional) access regime about access to vehicle data and technical access to the vehicle (interoperability) for the automotive aftermarket and other stakeholders within the broader mobility system. This raises the question how to align the sectoral Type Approval Regulation with the horizontal principles of the Data Act and what additional rules are necessary.[75]

25 The objectives of this initiative are to promote innovation in the automotive and mobility sector, to ensure higher quality, more choice and lower prices of vehicle-related and mobility services for consumers, and to safeguard cybersecurity, safety, personal data protection, intellectual property, as well as the necessary investment incentives for data-driven vehicle-related services.[76] This is consistent with the Data Act. However, also like the Data Act, this initiative would not eliminate the gatekeeper positions of the vehicle manufacturers but would only limit the negative effects of their exclusive control position. Moreover, different to the Data Act, the initiative does not mention (a) the empowerment of users for more meaningful control over their vehicle and the data, and (b) the unlocking of vehicle data for innovation beyond the mobility sector (e.g. data markets).[77]

26 In the policy initiative, the European Commission compares a baseline scenario (Data Act enacted, no sectoral regulation) with three policy options that represent a step-by-step deeper regulation for technical access to the vehicle and its data. Option 1 would complement the data access rights of the Data Act with equal access rights to functions and resources, and would ensure transparency about the available vehicle data, functions and resources. Option 2 would complement this by a minimum list of vehicle data, functions and resources that have to be available, including communication with the driver and access to the on-board diagnostic port. Option 3 would additionally specify how this access would occur and be controlled. All options would address the option-specific interplay between access rights and cybersecurity rules. In the following, these policy options are assessed regarding (1) access to data, (2) access to functions and resources, and (3) additional governance rules.

I. Regulated Access to Vehicle Data

27 The scope of data covered by the initiative is not clearly described and thus subject to different interpretations. First, it may rely on Art. 4 & 5 DA to make vehicle data accessible to third parties. In this case, the scope of data covered would be subject to the same legal uncertainty than the one under the Data Act (see C.I.1). Second, the principle of equal, non-discriminatory access to functions and resources of option one could also refer to data. This would imply that the manufacturer has to make available to third parties all the data that is made available to the manufacturers' services, which is a reasonable approach in theory, but could have anticompetitive consequences in practice, since an increasing number of services are provided directly by the manufacturer (e.g. software updates), and a non-discriminatory scope of data vis-à-vis authorized services could be too narrow (especially. for innovation). Third, the minimum list of vehicle data, functions and resources of policy option two could go beyond the scope of data covered by the Data Act in order to enable certain innovation activities and services, depending on the regulator's decision

71 See for a similar conclusion about the Data Act in general: Eckardt/Kerber (n 28) 22.

72 Regulation (EU) 2023/2854 (n 1) Recs 14, 25, 27.

73 European Commission (n 5).

74 Regulation (EU) 2018/858 (n 2).

75 Regulation (EU) 2023/2854 (n 1) Rec. 6.

76 European Commission (n 5) 2.

77 Kerber/Gill (n 68) 6.

on which data to include. In this interpretation, the degree of openness of the automotive sector would depend on the regulator and not anymore on the strategic decisions of the manufacturers. Overall, it is not clear if the initiative chooses a functional approach similar to the Type Approval Regulation. From a competition and innovation perspective, such an approach should be chosen since it would include all data in all forms that are necessary for the provision of the aftermarket service.[78] To reduce the uncertainty as to the interpretation of the scope of data, a sectoral regulation would have the opportunity to make much more specific definitions. It could provide e.g., a more practical delimitation of personal and non-personal data as well as of raw, pre-processed and derived/inferred data, develop guidelines to clarify which data may constitute a trade secret, or is critical to the safety and security of the vehicle, mandate a minimum of data to be accessible (independent of brand and model), and facilitate the standardization of metadata (particularly important for the many multi-brand service providers, and public sector services).

28 A conflict exists regarding the basic data sharing mechanism. The Data Act is based upon a user-centric approach where data sharing is always initiated by the user, while the Type Approval Regulation provides direct access rights for third parties. Which approach should the initiative take? It would fit into the logic of the Data Act if the Type Approval Regulation would also provide vehicle users with data access and sharing rights. From the perspective of user empowerment (Data Act objective) this would make sense. However, from the perspective of innovation and competition such a solution is unlikely to lead to sufficient quantities of data being shared and would thus be unlikely to facilitate independent innovation and competition.[79]

29 Different to the Data Act, the initiative does not seem to set restrictions regarding the possibilities of manufacturers and third parties of how to use the data, i.e., the Data Act provides the default rules. However, it would be an opportunity for the sectoral regulation to clarify some aspects that the Data Act does not sufficiently consider. Amongst others, the initial contract between manufacturer and user could be specified. This may include e.g. a limitation to the duration of this contract, minimum standards as to the granularity of the users' choice, the prohibition of "total buy-out" contracts, a clarification of which data may not be shared due to security or confidentiality requirements, rules for situations in which either the user or the data holder change, and means to discontinue data sharing without losing functionality of the car.

78 Wiebe et al. (n 37) 81; Drexl et al. (n 28) para. 25.

79 See also Kerber (n 27) 125 ff.

30 A final important aspect regarding access to vehicle data that needs to be clarified sectorally, is the relationship between the automotive industry and gatekeepers (pursuant to Art. 3 DMA), in particular Google and Apple with their automotive operating systems. The prohibition of Art. 6(2)d Data Act for users and third parties to share data with these companies may lead to significant problems regarding the interoperability of vehicles with these application platforms, and may result in less choice for users, but also to less data availability for third parties.[80] This is because the gatekeepers could, depending on the depth of their integration into the vehicle system, have incentives to allow third parties to access vehicle data through their operating systems, or at least have incentives to also collect and trade the generated vehicle data.

II. Regulated Access to the Vehicle (Functions and Resources)

31 Since the Data Act already addresses the general issue of access to (vehicle) data, the main focus of the initiative is on the specific problem of access to vehicle functions and resources. Policy option 1 proposes to complement the data access right of the Data Act with equal and non-discriminatory access rights to and transparency about the accessible functions and resources.[81] This would fit to the logic of the Data Act. Again, it is questionable whether a user-centric approach can achieve competition and innovation objectives.[82] However, the manufacturers would still be free to decide which functions and resources they make available, which implies leeway for them to decide for which services they open up their systems and for which not.[83] Additional problems would occur where third parties want to develop novel services that require access to functions and/or resources that the manufacturers are not using themselves. These innovations could be blocked because they would not be covered by the principle of equal, non-discriminatory access.[84] The minimum lists of policy option 2 could solve this problem since now the regulator would decide which

80 Martens (n 28) 13 ff.

81 For most third parties this option seems to be the absolute minimum and thus rather a starting point towards more comprehensive regulations. Since it is unlikely that the data sharing mechanism of the Data Act can solve the data access problems, merely adding functions and resources to this mechanism would be no solution.

82 Wiebe et al. (n 37) 91.

83 Determann/Perens (n 11) even argue that vehicle users should be free to decide which operating system they want to use independent of the vehicle brand.

84 Kerber/Gill (n 68) 7.

functions and resources need to be accessible from every vehicle (if the regulator includes the necessary functions and resources). Such a minimum list would be in line with the existing Type Approval Regulation, which provides such a list in its annex. An open question is whether equal and non-discriminatory access to functions and resources can be understood as FRAND approach, i.e., whether this access would be granted also on fair and reasonable terms. If not, manufacturers could easily set fees and terms that discourage third parties from seeking access.[85]

III. Additional Governance Rules for Access to the Vehicle and its Data

32 In the sectoral regulation additional governance rules need to be defined that alleviate the specific legal uncertainties, economic risks and technical issues. While the Data Act provides such rules, the initiative on access to vehicle data, functions and resources remains rather vague on this topic and only indicates a need for additional rules regarding: (1) fair competition, (2) standardization, as well as (3) cybersecurity, safety, intellectual property rights and data protection.

1. Fair Competition in the Automotive Aftermarket

33 The sectoral regulation has the opportunity to maintain fair competition in the automotive aftermarket. While competition plays only a minor role in the Data Act, the existing Type Approval Regulation has a clear focus on preserving competition in the automotive aftermarket.[86] Two additional important points have to be mentioned here for the leveling of the playing field: the compensation to be paid for the access and the dual role of the vehicle manufacturers.

34 If the sectoral regulation would follow the tradition of the Type Approval Regulation, it would oblige the manufacturers to enable access on a time-based or transaction-based model, and charge reasonable and proportionate fees that do not discourage third party access.[87] The Data Act foresees reasonable and non-discriminatory compensation for access by third parties, to promote the generation and making available of data.[88] Similar to the Type Approval Regulation, this compensation may vary depending on the volume of data and the duration of the arrangement. However, the Data Act allows for a margin (except regarding SMEs),[89] which depends, among others, on the size of the manufacturers' investments into the data collection and the question whether the data is co-generated.[90] As Monti et al. (2022) show, the calculation of the reasonable compensation under the Data Act is very complex and depends on a broad range of criteria that can be individual to the specific data access request.[91] One option to avoid this complex calculation with all its legal uncertainty, would be to oblige the manufacturers to provide access free of charge. This would also solve the inconsistency problem of the Data Act around the dual data-pricing regime.[92] If e.g., a vehicle user wants to share vehicle data with a third party in order to receive a service, the user can access the data free of charge, but may de facto not be able to directly share the data with the third party, nor can the third party access the data free of charge on behalf of the user. As a result, the third party will need to pay the manufacturer for the data access, which will increase the price of the service. Therefore, the user will indirectly pay for the data access.

35 An additional fundamental problem is the conflict of interests that car manufacturers face due to their dual role as service providers and enforcers of the necessary rules for safety, security, privacy etc. This refers to all kinds of certification and accreditation processes that third parties have to undergo. Since it is questionable whether the manufacturer can do this in a fair and neutral manner, third parties demand a "separation of duties", requiring these processes to be performed by a neutral entity.[93] An exemplary issue that could be solved this way is business monitoring. By monitoring exactly who accesses which data, functions and resources, in

85 Kerber/Gill (n 68) 8.

86 See e.g. Regulation (EU) 2018/858 (n 2) Rec. 52. This is done by adopting a purpose-based approach, which includes also independent operators other than repairers (e.g. manufacturers of spare parts and diagnostic tools, data aggregators and publishers) and covers – besides Repair and maintenance information – also a broad range of other essential inputs (e.g. diagnostic equipment, tools, applicable software, training material).

87 Regulation (EU) 2018/858 (n 2) Art. 63.

88 Regulation (EU) 2023/2854 (n 1) Rec. 46.

89 Regulation (EU) 2023/2854 (n 1) Art. 9(1).

90 Regulation (EU) 2023/2854 (n 1) Rec. 47.

91 Monti et al., Study for developing criteria for assessing "reasonable compensation" in the case of statutory data access right – Study for the European Commission Directorate-General Justice and Consumers – Final report, 2022, available at: <https://data.europa.eu/doi/10.2838/19186> last accessed 02.07.2024.

92 Martens (n 28) 10.

93 AFCAR, Creating a level playing field for vehicle data access: Secure On-board Telematics Platform Approach, 2021, available at: <https://www.afcar.eu/access-to-in-vehicle-data-and-resources> last accessed 02.07.2024.) 31. See also Wiebe et al. (n 37) 71 who suggests a trustee solution for a separation of duties.

which intervals etc., the car manufacturers may derive insights into innovation projects, customer relations etc., which may provide them with an additional competitive advantage.[94]

2. Standardization of Access to Vehicle Data, Functions and Resources

36 The Type Approval Regulation obliges standardized access to vehicle repair and maintenance information presented in an easily accessible manner that can be processed with reasonable effort.[95] The data itself has to be in a standardized (or, if not feasible, appropriate) format and also third parties other than repairers shall be empowered to process the data "with commonly available information technology tools and software".[96] Furthermore, the Type Approval Regulation mandates the development of a standardized format for the exchange of data that reflects the needs of manufacturers and third parties alike.[97] In comparison, the Data Act does not require standardization beyond the obligation to make data "easily" accessible.[98] This is reasonable since many different standards for data and interfaces have already been established in different sectors and thus standardization should be done sectorally to avoid straightjacket effects. Therefore, it should be part of the sectoral regulation to find a suitable level of standardization in the automotive industry. In particular for the objective to promote innovation in the mobility sector in general, a certain (high) level of standardization and interoperability is crucial.[99]

37 Standardization is also particularly important for the automotive aftermarket since third parties usually offer multi-brand services (or produce multi-brand parts and tools). Different data formats and qualities, different metadata, different descriptions of functions and resources, different interfaces etc. increases the costs of third parties, drive up prices and may make independent services unattractive. Accordingly, the proposed transparency requirement and the (standardized) minimum lists of accessible vehicle data, functions and resources would be particularly important since they provide third parties with (legal) certainty about what they can at least expect to be accessible.[100] Further need for standardization exists e.g., regarding sector-specific technical and organizational standards for the sufficient anonymization of personal data,[101] technical standards concerning the protection of trade secrets, the development of standard contract terms, or regarding cybersecurity and product safety.[102]

3. Cybersecurity, Trade Secrets & Data Protection

38 Cybersecurity and safety risks have always been among the most important arguments by the manufacturers to justify their exclusive control. While clearly every additional access point creates additional risks, this problem seems to be solvable through appropriate technical and organizational solutions (e.g. certification and accreditation systems).[103] The Data Act mandates secure access for users (Arts. 3(1) & 4(1) DA) and third parties (Art. 5(1) DA), it enables users and data holders to contractually restrict data access or sharing if it could undermine security requirements (Art. 4(2) DA), and prohibits third parties to use data in a manner that adversely impacts the security of the IoT device (Art. 6(2)f DA). Still, according to the regulatory initiative, the Data Act does not adequately consider the possible tradeoffs between access rights and cybersecurity requirements.[104] Additional sectoral rules should ensure the safety and security if access to vehicle data, functions and resources.[105]

39 Closely connected to cybersecurity is the topic of trade secrets that may be part of the data that

94 This problem also relates to the recent discussion that platforms (e.g. Amazon) can potentially use the data on transactions between users and third parties on their platforms to develop better (potentially anticompetitive) strategies. In the connected car discussion this issue exists since 2016 (Mc Carthy et al. (n 8)) and thus years before it has gotten an issue in the Digital Markets Act, and in some provisions of the Data Act.

95 Regulation (EU) 2018/858 (n 2) Art. 61(1).

96 Regulation (EU) 2018/858 (n 2) Art. 61(2).

97 Regulation (EU) 2018/858 (n 2) Rec. 54.

98 The Data Act acknowledges the absence of standards for semantic and technical interoperability as a barrier to data sharing (Rec. 2) but does only refer to standards regarding data processing services and data space.

99 Kerber/Gill (n 68) 10. For such an initiative see: European Commission, A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility, COM(2016) 0766 final; Beyrouty et al., C-ITS Support Study, 2018, available at: <https://op.europa.eu/en/publication-detail/-/publication/426495e6-81c1-11e9-9f05-01aa75ed71a1> last accessed 02.07.2024.

100 Kerber/Gill (n 68) 9.

101 Leistner/Antoine, Attention, here comes the EU Data Act! A critical in-depth analysis of the Commission's 2022 Proposal, JIPITEC 13 2022, 339 (341).

102 Similiar: Wiebe et al. (n 37) 93.

103 Bartsch, et al. (n 13).

104 European Commission (n 5) 3.

105 This could be approach similar to the SERMI certification on access to safety/security-critical repair and maintenance information. See: <https://www.vehiclesermi.eu/>.

has to be made accessible. Granting access to such data risks the secrecy of the trade secret, and thus trade secret protection. While trade secrets are not at all mentioned in the policy initiative, the Data Act clarifies that trade secret protection does not generally shield data holders from data sharing obligations, and provides rules that aims towards preserving the confidentiality of the trade secret.[106] Although this approach has been welcomed by some scholars,[107] there is still legal uncertainty about the protection of trade secrets, which can lead to difficult disputes that can impede the effectiveness of the whole data sharing mechanism.[108] Against this background, a sectoral regulation should aim to reduce this legal uncertainty. This could include the provision of clear and neutral guidelines for manufacturers on how to determine which access risks the secrecy of trade secrets, and the definition of which technical protection measures are necessary and sufficient to protect these trade secrets.

40 A final problem is the issue of protection of personal data. With the Data Act, the correct delimitation of personal data becomes even more decisive.[109] Since the sectoral regulation cannot avoid dealing with personal data,[110] it has to justify the lawfulness of the processing with any of the legal bases defined in Art. 6(1) GDPR. A straightforward solution would be to define the sharing of vehicle data for third parties as processing necessary for compliance with a legal obligation (Art. 6(1)c GDPR).[111] However, consent would still be necessary for sensitive data.[112] This means that some form of consent management may be needed anyways. This may be less of a problem where a user, who is a data subject, requests access/sharing of data that only relates to him/her. However, if the user is a business and the data relates to employees or customers (company fleets, car sharing etc.), or where the user is a data subject, but also other data subjects use the vehicle (e.g., in a family situation), more sophisticated technical solutions are necessary to unequivocally identify the data subject and assign the right data to it. In practice this could be achieved through user accounts, where the vehicle user has to log in prior to every journey. This is mandated by Rec. 21 DA, which states that, where several persons or entities are users, every user should be enabled to have access to his/her specific data. The sectoral regulation may adopt similar provisions and could add to user empowerment by demanding standardized interfaces (login-screens) and to fair competition by ensuring non-discriminatory conditions regarding consent. Another problem in this regard is that there could be situations in which the data holder cannot serve data access or sharing requests without violating the GDPR (e.g., where consent cannot be obtained from every affected data subject).[113] Since Art. 1(5) DA provides priority to the GDPR, a denial of access would likely be justified. This argument could be strategically used by car manufacturers to deny data sharing with third parties. An alternative way to deal with these issues would be consequent and state-of the art anonymization of the data prior to the sharing. The sectoral regulation could pick this way and provide sector-specific guidelines on the necessary technical and organizational means, which would be important, esp. since the Data Act does not provide such information.

106 Regulation (EU) 2023/2854 (n 1) Arts. 4(6) & 5(9). This is complemented by rules which allow the data holder to withhold/suspend the data sharing in specific cases (Arts. 4(7) & 5(10) DA) or, even refuse the data sharing upfront in exceptional circumstances, e.g. where the data holder is highly likely to suffer serious economic damages from the disclosure of the trade secret (Arts. 4(8) & 5(10) DA).

107 Leistner/Antoine (n 101) 341; Metzger/Schweitzer (n 28) 26; also, in favor of this approach and with a view to connected cars, but before the Data Act proposal: van den Boom, Vehicle data controls – Balancing interests under the trade secrets directive, 2022, available at: <https://ssrn.com/abstract=3991561> last accessed 02.07.2024.

108 Leistner/Antoine (n 101) 341ff.; Wiebe et al. (n 37) 86.

109 Drexl, Legal challenges of the changing role of personal and non-personal data in the data economy. In: De Franceschi, Schulze (eds.), Digital Revolution: Data Protection, Smart Products, Blockchain Technology and Bitcoins Challenges for Law in Practice, München, Beck, 2019, 19-41.

110 In many cases (such as providing data for traffic management) the data might be anonymized before it is shared, however, esp. in situations where a specific user (data subject) requests a specific aftermarket service, such as repair and maintenance, the service provider can and needs to identify this user.

111 For such an approach with regard to the DA see: Leistner/Antoine (n 101) 341.

112 For the definition of "sensitive data" see Rec. 51 GDPR. In the case of connected cars, every data that reveals information about mobility patterns of individual persons (e.g. to which churches, political events, or other cultural activities the data subject drives) may be defined as sensitive.

113 Bomhard/Merkle, The Draft of the Data Act, Law Digital RDi, 2022, 168, (172).

Table 1: Overview about policy recommendations for a sectoral regulation

1. Scope of access to vehicle data	• Ensure a purpose-based scope of data by including all the data (and only those) that are necessary for third parties to independently and effectively and compete in the aftermarket o independent of the level of processing of the data o independent of whether it is personal data or not o independent of trade-secrets o independent of safety/security considerations • Provide a minimum list of data to be made available to achieve further objectives in the mobility ecosystem in general
2. Scope of access to vehicle functions and resources	• Basically, similar approach as for vehicle data (scope has to fit the purpose of enabling independent and effective innovation and competition)
3. Sharing mechanism for access to vehicle data, functions and resources	• Enable users to effectively share data with third parties, e.g. by making "in-situ" access the exception • Enable users to install third party applications that then can have directly access to vehicle data, functions and resources
4. Additional governance rules	• Compensation: o either establish a FRAND based compensation regime o or empower the user to authorize third parties to access vehicle data, functions and resources free of charge • Establish specific sectoral rules to: o ensure the safety and security of access o ensure the protection of privacy o ensure the protection of trade-secrets • Facilitate the standardization of: o data formats, data quality, semantics, metadata o interfaces (for users and third parties) o safety/security requirements (authorization, accreditation) o anonymization and means to provide consent • Regulate the contract between user and manufacturer, e.g.: o duration and breadth of contract (prevent total buy-out) o possibility for user to discontinue data sharing without losing functionality of the device • Regulate the relation between gatekeepers (DMA) and automotive stakeholders with a view to competition and innovation in the mobility system

E. Conclusion

41 The Data Act is the preliminary apex of EU data regulation and a milestone of innovative law, which is not based on a classical market failure logic but constitutes a market-shaping approach.[114] Its clarification that it is no longer the de facto data holder, but the user (private or business) of the IoT device who should have control over the use and sharing of the generated data represents a fundamental readjustment of the monetization opportunities in the data economy.[115] However, in general – and especially in B2C situations – the Data Act does not challenge the gatekeeper-like position of manufacturers vis-à-vis users and third parties. Through technological design and contractual arrangements, the manufacturers may be able to keep de facto control over the data and therefore significant improvements for competition and innovation in data-driven secondary markets are hardly imaginable. The same holds for the problem of access to the vehicle and its data. The Data Act may weaken the exclusive control of vehicle manufacturers over the vehicle data but does not challenge the de facto control of the vehicle manufacturers. While the data access and sharing rights may slightly improve the data availability for vehicle users and third parties, it cannot be expected that this systematically enables third parties to effectively compete. This is mainly because the Data Act does not regulate the sector-specific issues around access to vehicle functions and resources, but also due to a series of limitations, imbalances, and legal uncertainties around access to vehicle data. Moreover, the Data Act does not provide a level playing field between car manufacturers and third parties regarding the utilization opportunities of the data. As a consequence, additional sectoral rules are necessary to ensure competition and innovation in the automotive aftermarket.

42 The European Commission has acknowledged some of these limitations and published an initiative for a sectoral regulation. This paper has analyzed the different policy options of this initiative in conjunction with the rules of the Data Act and the traditional approach of the existing regulation on access to repair and maintenance information. The analysis in chapter 4 shows that, while the objectives of the sectoral regulation are consistent with the Data Act, the basic data sharing mechanism in the sectoral regulation may rely much less on the car user. Clearly, the user would still be in the position to authorize access to the vehicle and its data for certain services, but the actual process of sharing this access may be much more direct (in line with the Type Approval Regulation), i.e., would be initiated

114 Metzger/Schweitzer (n 28) 49.

115 Hennemann/Steinrötter (n 19) 8.

by third parties and rely much less on the strategic decisions of the vehicle manufacturer. However, since the initiative is very vague on this point, other scenarios are also imaginable, e.g., that any future sectoral regulation will be aligned with the Data Act principles, by including a user-centric data sharing mechanism. In this case, this paper argues that no facilitation of competition and innovation can be expected. This shows one of the core conflicts between the objectives of the sectoral regulation and the Data Act: User empowerment – an important target in itself – may not automatically lead to improved data sharing for better competition and innovation.

43 It seems the regulator has two ways to deal with this fundamental conflict. Both ways can only be outlined here: The first option would be to stay within the current line of thinking, i.e., to accept the exclusive initial control of the car manufacturers and to improve this regulated access system in a way that enables third parties to independently and effectively compete. This would require a strong sectoral regulation with FRAND access conditions and far-reaching standardization (e.g., of user interfaces) and sectoral specifications of the Data Act (e.g., safety & security, IPRs and data protection) that should aim to create a more level playing field regarding competition between car manufacturers and third parties. The second, and much more radical, option would be to not accept the exclusive initial control of the car manufacturers and thus to avoid (a priori) many of the problems that the Data Act and the initiative want to solve. There are again two options: Either (1) mandating the introduction of a shared server through which car manufacturers and third parties can access vehicle data, functions and resources on FRAND terms, which is managed and operated by a neutral organization. Or (2) mandating the implementation of an On-Board Application Platform, through which third party applications have the same direct access as the manufacturers. Both of these alternative solutions also require extensive regulation, and therefore a sectoral regulation needs to be introduced anyways.

Data Usability as a Parameter of Rights and Obligations under the EU Data Act

by **Daria Kim and Man Wai Kwok** *

Abstract: As an instrument for advancing the data economy, the EU Data Act aims to enhance the accessibility of data generated through the use of connected products and related services, thereby unlocking the potential of data for the benefit of society. This article focuses on data usability as an equally crucial factor in harnessing value from data, an aspect that gained recognition only in the later stages of the legislative process. In particular, we examine the technical state of data, which is both a technical factor for realising the value of data and a legal parameter delineating the scope of data access and usage rights, along with the respective obligations introduced by the Data Act.

Our analysis finds that data usability is not thoroughly considered in the Data Act and is only minimally addressed within the framework of its data-sharing regime. We identify several concepts bearing on the technical state of data – including the notions of 'pre-processed data', 'readily available data', 'simple operation', 'insignificant investment', and 'disproportionate effort' – that remain unclear, leading to uncertainties regarding the scope of data-sharing obligations. Attaining the policy goals will to a significant extent hinge on the interpretation and application of these criteria. While acknowledging that the final version of the Data Act represents an improvement over the initial proposal in terms of addressing data usability, we contend that the imposition of restrictive criteria on the scope of 'readily available data' and 'pre-processed' data is not justified, whether viewed from the perspective of technical necessity, legal certainty, or a balance of interests.

Keywords: data access and usage rights; data-driven economy; EU Data Act; data usability; readily available data

Recommended citation: Daria Kim and Man Wai Kwok, Data Usability as a Parameter of Rights and Obligations under the EU Data Act, 15 (2024) JIPITEC 139 para 1.

A. Introduction

1 The vision of a thriving data economy and the question of which measures can fulfil it have been debated extensively in the European Union (EU) in recent years. Several legislative initiatives at the EU level have been underway, pursuing the overarching objective of unlocking the value of digital data for society, particularly by facilitating access to data as a multi-purpose input for innovation and a determinant of competition.[1] The regulatory thinking has undergone a notable shift, transitioning from the idea of conferring a data producer's right in relation to sensor-generated data[2] towards an

* Daria Kim (M.A., LL.M., Dr. iur.) is Senior Research Fellow at the Max Planck Institute for Innovation and Competition (Munich).

Man Wai Kwok is a holder of MSc in Engineer (Data Science) and BSc.

1 European Commission, 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 (19.2.2020).

2 European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Building a European Data

appreciation of the need to establish a legal basis for claiming access to data and its further utilisation.

2 The Data Act of 13 December 2023[3] presents an unparalleled statute worldwide that has introduced cross-sectoral access and usage rights as regards data generated by connected products[4] or related services.[5] Thereby, the EU legislature aspires to promote the data economy by enabling the broad utilisation of such data,[6] recognised as 'a core component of the digital economy, and an essential resource to secure the green and digital transitions'.[7] Data subject to new data-sharing obligations should serve as input for aftermarket services and downstream use cases that may extend beyond the products or services through which that data was initially collected.[8]

3 By introducing data access and usage rights, the legislature intends to mitigate contractual imbalances and legal uncertainty identified as 'problem drivers' leading to the suboptimal realisation of the value of data.[9] However, equally important is the technical state of the data in which it has to be made available for subsequent use. Such a state should allow for subsequent meaningful processing and analysis of the shared data. This aspect seems to have been overlooked in the initial proposal by the European Commission (hereinafter, the Commission).[10] Only once does the Commission mention usability in its ex-ante impact assessment accompanying the proposal for a data act when stating that it 'aims to make more data in the EU usable to support sustainable growth and innovation by [...] removing barriers for access to data'.[11] In other words, the Commission associated data usability with opening up access to data and focused on overcoming the restrictive effects of the de facto exclusive control by device manufacturers and service providers over product and service data.[12] Unsurprisingly, the initial proposal did not say much about the technical state of data subject to the obligations to make data available, except for limiting such state to 'the form and format in which [data] are generated by the product'[13] and excluding 'derivative data'[14] and 'information derived or inferred' from data.[15] Though not explicitly stated, one would understand it as referring to 'raw' data,[16] which, as keenly pointed out by critics, would fall short of fulfilling the policy objectives.[17]

Economy' COM(2017) 9 final (10.1.2017) 13; European Commission, Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, SWD(2017) 2 final (10.1.2017) 33-34.

3 Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) OJ L, 2023/2854 (22.12.2023).

4 Defined as 'an item that obtains, generates or collects data concerning its use or environment and that is able to communicate product data via an electronic communications service, physical connection or on-device access, and whose primary function is not the storing, processing or transmission of data on behalf of any party other than the user' (art 2(5) Data Act).

5 Defined as 'a digital service, other than an electronic communications service, including software, which is connected with the product at the time of the purchase, rent or lease in such a way that its absence would prevent the connected product from performing one or more of its functions, or which is subsequently connected to the product by the manufacturer or a third party to add to, update or adapt the functions of the connected product' (art 2(6) Data Act).

6 recs 2, 4, 5, 6, 15, 16 and 21 Data Act.

7 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 (23.2.2022) 1.

8 rec 6 Data Act: 'the data recorded by connected products or related services are an important input for aftermarket, ancillary and other services'; rec 15 Data Act: 'data [covered by the Data Act] includes data collected from a single sensor or a connected group of sensors for the purpose of making the collected data comprehensible for wider use-cases'; 'such data [...] support innovation and the development of digital and other services to protect the environment, health and the circular economy, including through facilitating the maintenance and repair of the connected products in question'.

9 Commission Staff Working Document, Impact Assessment Report Accompanying the document 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) SWD(2022) 34 final (23.2.2022) 9, 15. See also rec 2 Data Act.

10 Apart from addressing data semantic interoperability in the context of switching data processing service providers.

11 SWD(2022) 34 final (23.2.2022) 133.

12 rec 20 Data Act.

13 COM(2022) 68 final, rec 17: 'Such data should include data in the form and format in which they are generated by the product, but not pertain to data resulting from any software process that calculates derivative data from such data as such software process may be subject to intellectual property rights.'

14 ibid.

15 ibid rec 14.

16 References to 'raw' data are made in the context of the impact of the Data Act on the database protection sui generis. SWD(2022) 34 final 132, 138.

17 Drexl J and others, 'Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on harmonised rules on fair access to and use of data (Data Act)' < https://pure.mpg.de/rest/items/item_3388757_4/component/file_3395639/content > para 333 ff; Podszun R, *Der EU Data Act und der Zugang zu Sekundärmärkten am Beispiel des Handwerks* (Nomos 2023) 41

4 Something must have prompted the Council of the EU to introduce within its negotiation mandate[18] a technically dense Recital 14(a) that specifies the technical state of data covered by the Data Act, along with the notion of 'metadata that is necessary to interpret and use [data]' as part of the data holders' obligations.[19] These proposals made their way into the final version of the Data Act, while the reference to data 'in the form and format' that is generated by a product was omitted. Ostensibly, the EU legislature must have recognised that the latter would not suffice for unlocking the value of data through its use.

5 In the following, we take a close look at data usability, which is both a legal parameter delineating the scope of rights and obligations introduced by the Data Act and a technical precondition for harnessing the value of data, as aspired by the legislature. By doing so, we aim to make an original contribution to the existing analysis of the Data Act.[20] The analysis is structured as follows: Part II explains the key aspects of data usability that are relevant for understanding the technical state of data falling within the ambit of the Data Act. Part III examines the notions of 'pre-processed data', 'readily available data', 'inferred or derived data', 'metadata' and the related qualitative criteria – 'significant investment', 'simple operations', 'disproportionate effort' – that are applied to determine the scope of data covered by the Data Act. It identifies interpretative difficulties presented by these notions and criteria, introducing uncertainty in delineating the scope of new data-sharing obligations. In Part IV, we consider how the Data Act treats the technical state of data in view of the policy objectives, and contemplate an alternative approach where 'readily available data' and 'pre-processed data' would not be restricted by the criteria of 'a simple operation', 'disproportionate effort', and 'significant investment'. In conclusion, we submit that, while the final version of the Data Act represents an improvement over the initial proposal in terms of data usability, the imposition of the limiting criteria on the scope of 'readily available data' and 'pre-processed' data is not justified, whether viewed from the perspective of technical necessity, legal certainty, or a balance of interests.

B. Why does the technical state of data matter?

6 The value of data can be realised only when its technical state allows for processing in a particular use case. This section explains the concept of data usability within the context of data generated through the use of connected products and related services, which is a focus of the Data Act.

I. Data usability as a purpose-oriented concept

7 Neither a commonly agreed-upon definition of the usability of sensor-generated data nor a universal taxonomy of data processing exists.[21] In essence, the usability of sensor-generated data is a characteristic of the technical state of data, indicating its suitability relative to the intended purpose, whether it be sharing, record-keeping, display, status tracking,

ff; Kerber W, 'Governance of IoT Data: Why the EU Data Act Will Not Fulfill Its Objectives' (2023) 72 GRUR International 120, 126 ff.

18 Council of the European Union, 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). Mandate for negotiations with the European Parliament (17 March 2023) 2022/0047(COD) <https://data.consilium.europa.eu/doc/document/ST-7413-2023-INIT/en/pdf>.

19 ibid arts 3(1), 4(1), and 5(1).

20 Eckardt M and Kerber W, 'Property Rights Theory, Bundles of Rights on IoT Data, and the EU Data Act' (2024) European Journal of Law and Economics, https://doi.org/10.1007/s10657-023-09791-8; Kerber W, 'EU Data Act: Will New User Access and Sharing Rights on IoT Data Help Competition and Innovation?' (2024) Journal of Antitrust Enforcement, 10.1093/jaenfo/jnae011; Chiarella ML and Borgese M, 'Data Act: New Rules about Fair Access to and Use of Data' (2024) 10 Athens JL 47; Stuhldreier MA, 'Fostering Innovation by Utilising Big Data: The Data Act and the Risk of Quasi-Exclusivity Reinforcing Data Lockups' in Nadia Naim (ed), *Developments in Intellectual Property Strategy* (Springer 2024); Colangelo G and Borgogno O, 'Shaping Interoperability for the Internet of Things: The Case for Ecosystem-Tailored Standardisation' (2024) 15 European Journal of Risk Regulation 137; Hennemann M and others, *Data Act: An Introduction* (1. Auflage, Nomos 2024); Picht PG, 'Caught in the Acts: Framing Mandatory Data Access Transactions under the Data Act, Further EU Digital Regulation Acts, and Competition Law' (2023) 14 Journal of European Competition Law & Practice 67; Leistner M and Antoine L, 'IP Law and Policy for the Data Economy in the EU' (2023) 17 Economics 1; Schweitzer H, Metzger A, 'Data Access under the Draft Data Act, Competition Law and the DMA: Opening the data treasures for competition and innovation? (2023) GRUR Int. 337; Metzger A, Schweitzer H, 'Shaping Markets: A critical evaluation of the draft Data Act' (2023) 1 ZEuP 42; Paal F, 'Access to Data in the Data Act Proposal' (2023) ZfDR 249; Kerber (n 17); Podszun (n 17); Drexl J and others (n 17).

21 Different qualities of data have been discussed as the components of data usability in technical, managerial, and economic literature. See eg Chen B, 'What is Data Usability? Definition, Examples, and Best Practices' (*Metaplane*, 29 May 2023) <https://www.metaplane.dev/blog/data-usability-definition-examples>.

machine learning, business analytics and decision-making, or other applications. Data usability is enhanced as a dataset[22] is processed within the data value chain, progressing from raw sensor data to a state more closely aligned with the pursued objective. Given that data usability is defined and assessed relative to the purpose of data processing, it is not a fixed characteristic that can be universally defined.[23]

8 The purpose of each data processing step within the data value chain is to improve data usability qualitatively and/or quantitatively. The results of each processing phase can be assessed in terms of qualitative and quantitative benchmarks, such as 'accuracy' and 'precision'. Table 1 (annex) presents a non-exhaustive list of major types of processing[24] sensor-generated data: value calibration, data value de-noising, missing data value imputation, data selection, and data extraction.[25] It also illustrates the respective contributions of these steps to data usability with respect to the assumed objectives.

II. Data pre-processing

9 Calibration[26] and de-noising are foundational data processing steps that are crucial for data interpretability and usability. Usually performed early in the data value cycle, these steps are generic in nature compared to purpose-specific data transformations and enhance the results of the follow-on steps. These generic steps can be considered as data pre-processing and are briefly explained below, given their relevance to the scope of the Data Act.[27]

1. Calibration and data accuracy

10 As sensors interact with the physical environment, they generate electrical signals, which are digitised into raw data. For example, a temperature sensor generates signals that are converted into raw data, not direct temperature values. However, the link between this raw data and understandable units like degrees Celsius can be unclear. To determine this relationship, a formula[28] is required to convert the raw sensor data into a form with an interpretable unit of measurement. This formula can be obtained through a process called calibration, a procedure of comparing the raw sensor data with that of a calibration standard[29]. This process typically involves placing the sensor in a controlled environment with stable temperatures at selected levels, measuring the actual temperature values with the standard, and recording the raw sensor data to establish a relationship and derive a calibration formula.

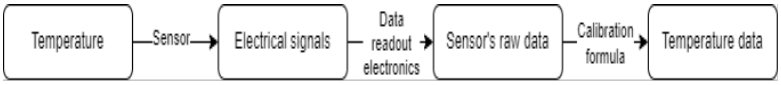

Figure 1: A schematic view of the conversion process from physical temperature to temperature data

11 The outcome of the conversion is characterised in terms of the accuracy of data, a quantitative measure of the difference between raw data values and their true values. Accuracy serves as a quantitative measure of data usability – improved accuracy denotes higher usability. Such a difference is known as a systematic error and, therefore, a lower accuracy value indicates better accuracy.[30] Several

22 A dataset can include data from different sources, as well as metadata.

23 For example, if A's goal is to sell raw temperature sensor data to B, who needs it for data analytics aimed at product improvement, the usability of such data would be higher for A than for B.

24 These steps can be, but do not have to be, performed consecutively. While calibration and de-noising are almost a must-have for sensor data, other steps are optional and some steps might need to be iterated.

25 Some may categorise de-noising, missing value imputation, and selection into data cleaning/cleansing as they detect and correct or remove corrupt or inaccurate data values. On the other hand, extraction and other techniques, including discretisation and normalisation, can be referred to as 'data transformation'.

26 Yeong DJ et al,. 'Sensor and Sensor Fusion Technology in Autonomous Vehicles: A Review' (2021) 21(6) Sensors 2140, https://doi.org/10.3390/s21062140.

27 Below at C.I. While technical literature uses the term 'data pre-processing', there is no fixed catalogue of operations falling within this category. In this paper, we apply the term 'data processing' as encompassing any data processing activity required to achieve the goal and refer to certain generic operations – typically necessary to enable purpose-specific use of data, such as calibration and de-noising – as 'pre-processing'. As discussed in part III, the Data Act is not explicit on the types of data processing considered as 'pre-processing'.

28 The formula can consist of one or more equations, taking raw sensor data as input and providing an output with an interpretable unit of measurement (e.g., degrees Celsius). This formula may also be visually represented in a graph, featuring a curve that illustrates the correspondence between the raw sensor data value and the standard's data value.

29 Fraden J, *Handbook of Modern Sensors: Physics, Designs, and Applications* (5th edn, Springer 2016) 24-26.

30 In this context, accuracy is, counterintuitively, defined as a measure of error rather than a positive feature. It is typically expressed either as an absolute term (e.g. ±5 for temperature data) or equivalently as a percentage of the sensor's full scale (e.g. ±5% if the full scale is 100). Fraden

factors can influence the accuracy of calibrated data, including the accuracy of the calibration standard, the accuracy of the calibration formula, and the sensor's sensitivity to environmental changes, such as temperature variations. While there is no universal standard for the minimum acceptable accuracy, it is determined relative to a specific objective. For instance, if calibrated data is utilised only to indicate outdoor temperatures, worse accuracy might be more tolerable compared to situations where the data is employed to monitor temperature-sensitive plants in a laboratory environment.

2. De-noising and data precision

12 Noise, also known as random or stochastic error, is a type of error distinct from the systematic error as the above-described measure of accuracy. Noise is unavoidable[31] and uncorrelated with the physical phenomenon being measured. Since a sensor first produces electrical signals, any environmental factor that interferes with the sensor or the supporting electronics can induce noise in the signal[32], and consequently, in the sensor's digitised raw readings.[33] Given that noise is uncorrelated with the physical phenomenon, it cannot be calibrated away, and thus, it remains in the calibrated data.

13 The level of noise is measured in terms of precision.[34] Without noise, the data value should stay constant if the physical phenomenon being measured is also unchanged. However, noise causes the data value to fluctuate around that constant level. Precision measures the amount of fluctuation in the sensor data (either raw or calibrated, given that noise passes freely without reduction due to the conversion of raw data to calibrated data). Thus, the more fluctuation, the lower the precision.

14 Calibration and de-noising are the foundational steps within the sensor data processing chain. Figure 2 illustrates a typical data processing workflow using temperature sensor data as an example that can be extrapolated to other types of sensor-generated data, considering their measurement specifics.

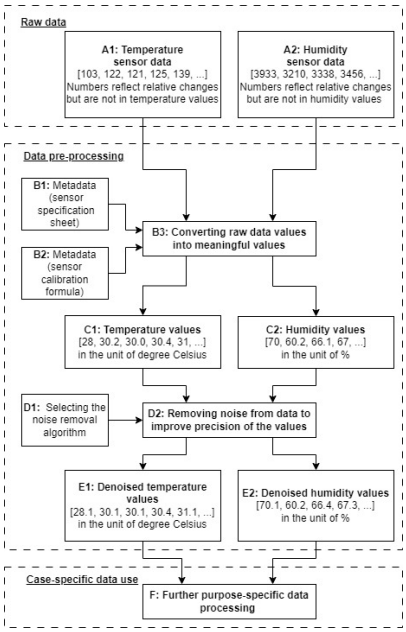

Figure 2 Data processing workflow exemplified by temperature and humidity sensor data[35]

III. An optimal technical state of acquired data

15 Given that data is frequently acquired elsewhere, the question arises about the optimal state in which data should be obtained to allow for its meaningful processing in a given use case. The answer depends on technical and practical considerations within a specific context. Essentially, the choice is between obtaining raw data or data that has undergone generic processing steps (that is, calibration and de-noising in the case of sensor-generated data). In principle, raw data can be usable if accompanied by sufficient metadata. Raw or generically processed data possesses greater potential for fulfilling various purposes and producing diverse outcomes. In some cases, sharing data in a pre-processed form can be both commercially and technically suitable for both the data holder and the data user. While obtaining purpose-specific processed data can be an option when purposes align, even minor differences may lead the data recipient to prefer conducting pre-processing themselves. Thus, there should not be a bias that the more data is processed, the greater its usability. In reality, the data user knows its own needs best and would be better off with data that allows for the most flexibility and diversifiable results.

(n 29) 39-42.

31 ibid 243-244.

32 ibid 237-238.

33 Some sources of noise include electromagnetic interference from a power converter that is connected to the circuit board hosting the sensors, and random vibrational movements of electrons (the carriers of the sensor's signal) which are proportional to temperature and thus called the 'thermal noise'. Apart from factors related to the electronics, natural noise can be introduced, for instance, by turbulent flow around a pressure sensor during air pressure measurement, or by ambient noise from pedestrians and cars when measuring sound levels by using an audio receiver.

34 Sometimes a related but distinct term 'reproducibility' is used as a measure of noise in the sensory context.

35 In this scheme, Bs and Ds are processing steps, while As, Cs and Es are the data states.

16 In summary, this part underscores that data usability is a characteristic of data defined and assessed in relation to a specific purpose. Two foundational pre-processing steps of sensor-generated data explained above – calibration and de-noising – have specific benchmarks and measures associated with data usability, namely accuracy and precision. These attributes denote continuous qualities that can vary in degree, while the acceptable level can be determined in relation to the intended purpose of data usage.

C. How does the Data Act account for data usability?

17 The key insight from the preceding section is that mere data accessibility does not ensure the realisation of its value in a given use case. Equally important is the technical state of the data, enabling its further processing. In the following, we analyse how the Data Act factors in this aspect.

I. 'Pre-processed data'

1. Definition

18 Recital 15 clarifies that the scope of the Data Act covers both:

19 data 'which are not substantially modified, meaning data in *raw* form, also known as source or primary data which refer to data points that are automatically generated without any further form of processing', and

20 'data which have been *pre-processed* for the purpose of making them *understandable* and *useable* prior to subsequent processing and analysis' (emphasis added).

21 The latter category 'includes data collected from a single sensor or a connected group of sensors for the purpose of making the collected data *comprehensible for wider use-cases* by determining a physical quantity or quality or the change in a physical quantity, such as temperature, pressure, flow rate, audio, pH value, liquid level, position, acceleration or speed' (emphasis added). For those not tech-savvy, this might require an explanation. Recall that the Data Act defines data as a 'digital representation of acts, facts or information'.[36] In the case of sensor-generated data, such representations result from the conversion[37] of an analogue signal to a digital signal[38] taking place within a converter that can be located in a device or on a server. Raw sensor data – data resulting from the conversion of an analogue signal to digital – is indeed not comprehensible or usable because such data does not represent the physical values/quantities. For that, data should be calibrated,[39] which corresponds to the wording of Recital 15: 'determining a physical quantity or quality or the change in a physical quantity'. If we look at Figure 2 and try to locate the type of data pre-processing described therein, it would be step B1 – converting raw values to meaningful values.

22 If calibration of data values only exemplifies data pre-processing, as signalled by the wording 'includes', what other technical operations on data can count as 'pre-processing'? Such operations would, in effect, delineate the scope of the rights and obligations under the Data Act as far as the technical state of data is concerned. As explained in Part II, data processing entails a sequence of operations that progressively enhance data usability, bringing it closer to the technical state aligned with the intended purpose. Where exactly did the legislature intend to delimit the scope of the Data Act when introducing the notion of 'pre-processed' data? The concretisation of making data 'comprehensible for wider use-cases' in Recital 15 presupposes data-processing steps *generic* in nature, as opposed to purpose-specific data processing. Besides calibration, this could potentially include de-noising.

2. Insubstantial investment

23 While Recital 15 does not provide other examples of pre-processing operations that improve data usability or comprehensibility, it does place a constraint on data pre-processing: such pre-processing 'should not be interpreted in such a manner as to impose an obligation on the data holder to make substantial investments in cleaning and transforming the data'. Thus, theoretically, it may also include data transformation beyond calibration, such as 'cleaning' (step D2 in Figure 2),[40] as long as

36 '...and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording' (art 2(1) Data Act).

37 While the Data Act does not define the terms 'generate', 'obtain', and 'collect' (data), all these activities should be interpreted – in line with the definition under art 2(1) Data Act – as acts of transforming real acts and facts into their digital representation, such as by converting an analogue signal into a digital signal in the case of sensor-generated data.

38 See Figure 1 and the accompanying explanation.

39 For explanation, see above at B.II.1.

40 As mentioned earlier, data cleaning/cleansing can be understood to encompass processes that detect, correct,

this would not entail 'substantial investment'.

24 If these criteria were to be applied to delineate the scope of the data holder's obligation to make data available, certain aspects require clarification. First, the characteristics of the technical state of data (usable/understandable) and the data holder's investment in data processing (substantial) denote continuous qualities that vary by degree, which prompts the question of the applicable threshold. Second, such criteria are relative – what constitutes comprehensible or usable data, or substantial investment, depends on a perspective or a point of reference. For data usability, the point of reference is the purpose of data processing. By which standard is the substantiality of investment to be determined, and by whom? Furthermore, how do these criteria correlate? Since it cannot be generally presumed that making data understandable and usable always requires an insubstantial investment, how should tension be resolved if making the data usable, as deemed by the data user, requires an investment deemed substantial by the data holder? The greater the misalignment between the criteria of data usability and the insubstantiality of investment, the greater the legal uncertainty regarding the scope of obligations for making data available, and the greater the potential for disputes between the data holder and the product/service user.

25 To explore this potential, let us first consider the practical aspect: How significant are the expenses associated with data pre-processing? The most straightforward case is providing product or service data in a 'commonly used format'[41] which would typically entail trivial costs.[42] Concerning calibration, the tendency is also rather towards an insubstantial cost. Sensor and device manufacturers routinely verify their product's sensors for performance, including for quality assurance.[43] Therefore, it is assumed that data holders should be able to provide calibrated data without substantial additional – i.e. discounting necessary equipment expenses – costs. However, it is worth noting that the cost of calibration can vary depending on calibration quality, which in turn impacts data accuracy and usability. For instance, data accuracy may suffer if calibration is done by a layperson in a poorly controlled environment and with a subpar calibration standard. In contrast, device or sensor manufacturers would usually be in a position to achieve superior results due to better standards, equipment, and a better-controlled environment at their disposal.

26 The question may further arise about the expenditures that are relevant for evaluating the substantiality of investment. Would the costs incurred by a device- or sensor manufacturer to purchase calibration equipment count? For instance, inertial sensors like an accelerometer or a gyroscope can be calibrated with or without precision equipment. While calibration can be performed in both cases, the cost for precision equipment is undoubtedly higher, resulting in better accuracy. Furthermore, some cases might require sensor re-calibration to ensure accuracy throughout the product's lifetime.[44]

27 In the case of de-noising, a device's circuit board could be designed to reduce the level of noise from within the circuit. However, additional de-noising software can deal with noise from unpredictable sources. The factors impacting the cost of de-noising include the choice of the de-noising methods, as well as the complexity and number of de-noising algorithms. The quality and its acceptable level may vary depending on the purpose, influencing the cost of de-noising.[45] Thus, if a device or sensor

or remove corrupt or inaccurate data values, such as de-noising, imputation of missing values, and selection. See above at B.II.2.

41 Which formats are 'commonly used' can vary depending on the context and purpose, and it can be interpreted within the relevant industries or technical communities. The guidance on this term, which is also employed in the General Data Protection Regulation, may provide further insights. See Article 29 Data Protection Working Party, 'Guidelines on the Right to Data Portability, 16/EN WP 242' <https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf> 13 (clarifying that 'the GDPR does not impose specific recommendations on the format of the personal data to be provided' and emphasising the purpose-bound approach to interpretation).

42 The term 'format' in this context refers to structures such as Excel (xlsx, xls), CSV, SQL, Parquet, JSON, and XML, each of which has own standard, at a minimum, indicating how the data should be stored and read.

43 Sensors are usually sold with product specification sheets detailing calibration results.

44 While it is impractical to re-calibrate typical personal-use products such as refrigerators, watches, and phones, in the case of industrial equipment – especially where accuracy is crucial for safety and/or where the product's sensors may shift significantly over time – re-calibration is necessary.

45 Different de-noising methods are described in literature. See eg Buades A, Coll B and Morel JM, 'A Review of Image Denoising Algorithms, with a New One' (2005) 4(2) Multiscale Modeling & Simulation 490, https://doi.org/10.1137/040616024; Banos O and others, 'On the Use of Sensor Fusion to Reduce the Impact of Rotational and Additive Noise in Human Activity Recognition' (2012) 12(6) Sensors 8039, https://doi.org/10.3390/s120608039; Du J, Gerdtman C and Lindén M, 'Signal Quality Improvement Algorithms for MEMS Gyroscope-based Human Motion Analysis Systems: A systematic review' (2018) 18(4) Sensors 1123, https://doi.org/10.3390/s18041123.

manufacturer de-noises data for their purposes, the quality level may or may not align with the data user's needs.

28 Accordingly, while it would be desirable for 'pre-processed' data to include calibrated and de-noised data, the limitation that pre-processing can only involve 'insubstantial investment' might be suboptimal from a data usability perspective. Alternatively, if the device manufacturer provides raw sensor data along with the relevant metadata[46] – information necessary for leveraging techniques such as sensor fusion for de-noising – such data can, in principle, be converted into calibrated and de-noised data. Nevertheless, it would be advantageous for data users if the device manufacturer, with a better understanding of the device and access to a larger sensor network for sensor fusion, could provide de-noised data.

29 In summary, it is not entirely clear how the criteria of insubstantial investment and usable/understandable data introduced by Recital 15 align and should be cumulatively applied to delineate the scope of the Data Act. The minimal prerequisites for data usability – calibration and de-noising – already suggest that the notion of pre-processed data may involve a trade-off between data usability and the compliance with the yet-to-be-clarified requirement of 'insubstantial investment'.

30 The question arises as to whether the statement in Recital 15, stipulating that both raw and pre-processed data 'fall within the scope of this Regulation', implies that the latter necessarily falls within the scope of the obligations to make data available, as considered next.

II. 'Readily available data'

1. The definition

31 While the term 'pre-processed data' appears only in Recital 15 Data Act, the data holder's obligations to make data available under Articles 4 and 5 refer to 'readily available data'.[47] The latter is defined as 'product data and related service data that a data holder lawfully obtains or can lawfully obtain from the connected product or related service, without disproportionate effort going beyond a simple operation'.[48] On the surface, this definition does not specify the technical state of such data – whether 'readily available data' is confined to raw data or can/must encompass pre-processed data. This question directly bears on the scope of the data holder's obligations. An indication that the fulfilment of this obligation can involve data processing is found in Recital 47, which explains that the cost of making data available includes technical costs, comprising 'the costs for processing, necessary to make data available, including costs associated with the formatting of data'.

2. Can data be processed before it is obtained from a product or service?

32 To understand the technical state in which data should be made available, let us consider what 'obtaining' data by the data holder refers to, bearing in mind that only 'simple operations' would count. The act of 'obtaining' data technically refers to the transmission of data from a device to the data holder's server. For related services, the data resides on either the service provider's server or the server operating the service. In which state does a data holder typically obtain data *from* a connected product or related service? And can any type of data (pre-)processing take place within the device at all before data is obtained from a product through transmission to a server? The decision-making of relevant entities in this regard can be influenced by different technical and practical considerations. As explained earlier, the conversion from an analogue to a digital signal typically takes place within the device. Subsequent data processing on a server allows the data holder to make changes to the data processing chain at any time.[49] Processing within a product offers benefits of offline use, cost savings on server computation, and pre-aggregation of data to reduce network traffic fees. However, if the product allows operation offline, then all steps relevant to the product's offline functionality have to occur within the product.[50]

46 On this option, see below at C.4.

47 art 4 Data Act. This notion was first introduced in the Council's version (n 18). Notably, in the Council's negotiation mandate, 'readily available data' was also in Article 3(1), which lays down an obligation to design products or provide services in a way to make product data and related service, in the wording of the final version, data 'directly accessible to the user'.

48 art 2(17) Data Act.

49 For instance, if the product manufacturer/service provider intends to implement a new function or improve an existing function of a product/service.

50 For example, the data processing chain of a sports watch may span over three computational entities – the watch, a mobile phone connected to the watch via Bluetooth, and a remote server connected to the mobile phone via the Internet. Since the watch is designed to work in standalone mode, it processes sensor data to support all its functions, such as calculating and displaying the heartbeat rate. The

33 Thus, in principle, data that can be obtained from a connected product or a related service is not confined to raw data but can extend to data that has undergone any transformations performed in-device or on a server.

34 To define which data falls within the meaning of 'readily available data', two cumulative criteria need to be further considered: the obtaining of such data should (i) be lawful, and (ii) should not involve 'disproportionate effort going beyond a simple operation'. Let us address each in turn.

3. In which technical state is product and service data 'lawfully obtained'?

35 Of relevance to this inquiry is whether the conditions of lawfully obtaining connected product or related service data explicitly or implicitly suggest any particular technical state of data or impose any restrictions thereon.

36 The sources of 'lawful obtaining' of data are exemplified in Recital 20: 'such as by means of the connected product design, the data holder's contract with the user for the provision of related services, and its technical means of data access'. Thus, both technical/factual means (via product design)[51] and a contractual basis for obtaining data would fulfil the condition of data being lawfully obtained, given that 'such as' indicates non-cumulativeness of conditions. Before the Data Act, the initial allocation of rights in sensor-generated data had not been statutorily prescribed, at least not at the EU level, leading to the frequent confusion between de facto exclusive control over data by device manufacturers and legal ownership of data.[52] In this context, Article 3 Data Act can be viewed as the first attempt at the EU level to statutorily allocate access and usage rights to users of connected products or related services. Furthermore, the Data Act appears to strengthen[53] the user's position by mandating that 'a data holder shall only use any readily available data that is non-personal data on the basis of a contract with the user'.[54] However, this limitation would not apply to data processing occurring *within* the product or service, i.e. before data is obtained *from* a product or service, which is the reference point of the definition of 'readily available data'.

4. Which operations should be deemed as 'disproportionate' and 'going beyond simple'?

37 The qualifiers 'disproportionate' and 'simple' serving as the delineators for 'readily available data' – consequently, the obligation to make data available – necessitate clarification. Given their relative character, questions inevitably arise concerning the threshold for simplicity and the point of reference for proportionality. For instance, if conversion from an analogue to a digital signal already constitutes a simple operation, should it be sufficient for the data holder to deny a claim for making available data in any (pre-)processed form? As discussed in Part II, every subsequent data-processing operation can vary in terms of both technical complexity and costs involved. Where is the line meant to be drawn? One could suggest that the rule of thumb would apply in a given situation, in light of its circumstances. However, this may jeopardise the objectivity of assessment and legal certainty. Furthermore, questions arise as to whether the criteria of 'disproportionate effort' and 'a simple operation' pertain solely to the act of obtaining data *from* the product or service, or if they are also applicable to data processing operations occurring *within* the product or service. Either way,

mobile phone, equipped with the watch's application, may process heartbeat rate data to display a performance review with historical data as one of the application's offline functions. However, certain functions, such as exercise recommendations, may require an internet connection to the remote server for aggregating and processing the watch user's and other users' historical data. Such 'division of labour' in the data processing chain is determined by product design – whether a function should work online and/or offline – and variations in computational and data storage capabilities among these three entities.

51 Notably, rec 20 explicitly states that a manufacturer's control over the generation of and access to data through the product technical design does not confer legal rights to such data in a manufacturer. In the wording of rec 20: 'In many sectors, manufacturers are able to determine, through their control of the technical design of the connected products or related services, what data are generated and how they can be accessed, despite having no legal right to those data.' Thus, while obtaining data by way of a product's technical design is deemed to be lawful, it does not translate into legal rights over such data.

52 Drexl J and others, 'Data Ownership and Access to Data – Position Statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the Current European Debate', <https://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/positionspaper-data-eng-2016_08_16-def.pdf>; Kim D, 'No One's Ownership as the Status Quo and a Possible Way Forward: A Note on the Public Consultation on Building a European Data Economy' (2018) 13 Journal of Intellectual Property Law & Practice 154.

53 But see Kerber (n 17) (assuming that the users would 'agree in this initial contract that the manufacturers or data holders get all rights to use and commercialize this non-personal data for the entire lifetime of the IoT device').

54 art 4(13) Data Act.

what would be the consequences if the data holder considers the efforts or operations involved as going beyond 'simple' and 'proportionate'? Could this potentially serve as a backdoor to deny access to data, given that there is no obligation for products or services to be designed in such a way that 'readily available data' only involves 'simple operations' and 'proportionate efforts'?

38 The notions of 'disproportionate effort' and 'simple operations' within the definition of 'readily available data' may invoke 'significant investment' as a delineating criterion of 'pre-processed' data falling within the scope of the Data Act, according to Recital 15. While there is no explicit linkage between Articles 4(1) and 5(1) and Recital 15 Data Act, an interpretation in light of the explanations in the Recital suggests that the data holder's obligations to make data available can encompass data in a calibrated or further (pre-)processed form, to the extent that such processing does not involve 'substantial investment', supposedly aligned with the notions of 'beyond a simple operation' and 'disproportionate effort'. As noted above, the relative nature of these qualifiers introduces some indeterminacy in interpreting the scope of data-sharing obligations.

39 To summarise, on the surface, data-sharing obligations under the Data Act do not explicitly require data holders to make available data in any 'pre-processed' form. The conversion from an analogue to a digital signal alone – i.e. the provision of raw data – can be argued to suffice for complying with the definition of 'readily available data'. The relevance of the reference to 'pre-processed' data laid down in Recital 15 for the obligations of data holders under Articles 4 and 5 remains open to interpretation.

III. 'Inferred and derived' data and information

40 The notion of 'readily available data' is contrasted with information and data 'inferred' or 'derived' from connected product or related service data, which 'should not be considered to fall within the scope' of the Data Act.[55] Notably, the rationale behind this delineation is based on the involvement of 'additional' investment and 'proprietary' algorithms and software. As articulated in Recital 15, inferred or derived information/data constitute 'the outcome of additional investments into assigning values or insights from the data, in particular by means of proprietary, complex algorithms, including those that are a part of proprietary software'. Situations to which Recital 15 refers would typically involve data analytics, usually performed on aggregated data, including through sensor fusion.[56] By 'assigning values', it hints at the use of data as input for developing machine learning (ML) models, while 'insights' may refer to predictions generated by ML models that enable the functionality of ML-based systems and applications.

41 References to 'additional investment' in data analytics, 'proprietary' algorithms, and 'proprietary' software indicate an intention to safeguard the economic interests of the data holders. This rationale aligns with the conventional logic of intellectual property (IP), where restricting third-party access to and usage of the 'fruits' borne by investment is assumed to incentivise innovation, which in this context may translate into innovation in the field of data analytics and ML. While this cannot be read as conferring any exclusive rights in derived/inferred data, it is notable that they are treated as 'untouchable' by default due to the very reason of being derived through (potentially) 'proprietary' algorithms and software – the mere fact that inferred/derived data can result from 'proprietary'[57] algorithms and software is deemed sufficient to limit restrict access to such information/data.

42 Furthermore, inferred or derived 'data could include, in particular, information derived through sensor fusion, which infers or derives data from multiple sensors, collected in the connected product, using proprietary, complex algorithms and which could be subject to intellectual property rights'.[58] The clause 'which could be subject to intellectual property rights' logically refers to 'data' or 'information', even though it grammatically correlates with 'sensor fusion' (which, as such, cannot be 'subject to' IP rights). One may wonder what kind of data or information resulting from sensor fusion could be protectable by IP rights. A plausible candidate might be an ML model as part of a patentable invention, but a model is not 'information'. Trade secrets do not come into question because they are not considered IP 'rights'.[59] While the linkage to IP is not articulated,

55 rec 15 Data Act.

56 For an explanation, see Table Annex.

57 The source of this proprietary status of algorithms is not quite clear, given that, as such, they cannot be protected by copyright or patents. Recital 15 also uses more cautious wording stating that 'algorithms' can be 'part of proprietary software'.

58 rec 15 Data Act.

59 rec 16 of Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, OJ L 157, 15.6.2016, p. 1–18. See also Proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful

the legislature seems to have presumed - bluntly and pre-emptively - its limiting effect on access to data.

43 In summary, dichotomies between substantial and insubstantial, simple and complex are applied to delineate the scope of the Data Act: raw data is defined as data that is 'not substantially modified', simple operations are a criterion of 'readily available data', '(in)substantial investment' is a criterion of 'pre-processed data', and derived/inferred data or information is that which results from 'complex' algorithms and additional (i.e. beyond insubstantial) investment. The challenge is that these criteria exist along a continuum with some range of legal uncertainty in between where it can be unclear whether a process might be rather simple or complex, or whether the associated investment or effort might be more or less substantial. If the motivation behind excluding substantial investment from the scope of the data-sharing obligation stems from protecting economic interests, a relevant reference point would be the definition of investment under the Database Directive, which includes 'the deployment of financial resources and/or the expending of time, effort and energy'.[60] The question may still arise regarding the investment that should be deemed relevant in this context, such as whether the expenditure associated with developing a data-processing algorithm would fall within this category.

IV. Metadata

44 Another latecomer to the Data Act, motivated by data usability considerations, was the notion of 'metadata' as part of access and usage rights and respective obligations, first introduced by the Council of the EU.[61] Defined as 'a structured description of the contents or the use of data facilitating the discovery or use of that data',[62] metadata should include inter alia 'basic context and timestamp, to make the data usable, combined with other data'.[63]

45 Notably, in the case of the obligation to make product data and related service data directly accessible to the user by design, metadata is supposed to be *included* in the connected product or related service data.[64] In contrast, in the case of the obligations to make data available to the user or third parties, metadata should be provided *in addition* to the 'readily available data'.[65] For metadata to be literally and technically 'included' in the connected product or related service data to be made directly accessible by product or service design, such metadata first needs to be placed within the same file[66] as product or related service data, located either in a product,[67] or on a remote server.

46 Metadata is an umbrella term – an exhaustive categorisation of information and data falling within this notion in all possible use scenarios is unfeasible. The Data Act adopts a purpose-based approach to determining the relevant metadata subject to data-sharing obligations when it emphasises that the 'relevant' metadata is data 'necessary' for interpreting and utilising the connected product or related service data for further purposes.[68]

47 The question may arise whether the Data Act imposes any constraints on the scope of metadata subject to the data holder's obligation to make such data either

acquisition, use and disclosure COM(2013) 813 final (28.11.2013) 3 (noting that trade secrets are 'not protected as a classical [intellectual property right]'). See also art 49(e) and (f) Data Act, distinguishing between the impact on intellectual property rights and on trade secrets as part of an evaluation of the Data Act.

60 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, 27.3.1996, p. 20–28, rec 40.

61 Namely, rec 14a and 56; art 3, 4, 5, 14, 17, and 19 of the version of the Council of the EU (n 18). The Commission's proposal referred only to metadata generated by the customer's use of a service which should be portable according to the provisions on switching between data processing services.

62 art 2(2) Data Act.

63 rec 15 Data Act.

64 art 3(1) ('Connected products shall be designed and manufactured, and related services shall be designed and provided, in such a manner that product data and related service data, including the relevant metadata necessary to interpret and use those data, are, by default, easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format, and, where relevant and technically feasible, directly accessible to the user.').

65 Both arts 4(1) and 5(1) Data Act state that 'the data holder shall make available readily available data, *as well as* the relevant metadata' (emphasis added).

66 Timestamps – an example of metadata mentioned in Recital 15 – are usually placed side-by-side with sensor values in one data file. The decision of whether to store metadata in the same file as the data depends on technical and practical factors. Opting for separate files for data and metadata allows for avoiding redundant metadata duplication, enhancing memory efficiency, and maintaining metadata consistency and currency.

67 It might not be even feasible to make all relevant metadata 'directly accessible' from on-device data storage or from a remote server at any point in time, already for the reason that the product manufacturer or service provider may not know all purposes for which users might need metadata for the subsequent data uses to fulfil the obligation under art 3(1) Data Act. See also below (n 78).

68 rec 15 and 20; art 3(1), 4(1), 5(1) Data Act.

directly accessible[69] or readily available.[70] While the provisions referring to metadata do not contain any direct, specific indication regarding the scope of metadata,[71] one could suggest that the legislature might not have deemed such limitations as necessary because it had already included safeguards for trade secrets, potentially embedded within metadata, to protect the interests of trade secret holders, who may or may not be data holders. Indeed, the protection of trade secrets is factored into the data access and usage rights.[72] While data-sharing obligations extend to trade secrets, they presuppose only inter partes disclosure,[73] subject to contractual and technical measures agreed upon with the trade secret holder.[74] This concerns sharing product and service data, along with metadata, with product/service users, as well as third parties.[75] Furthermore, a trade secret holder can, under some conditions, withhold, suspend, or refuse to share trade secrets.[76] It is worth noting that the mandatory sharing of trade secrets – even when subject to safeguarding measures to protect confidentiality – does constitute a limitation on the trade secret holder's rights, in the sense that it restricts their discretion in deciding with whom to share trade secrets and whether to share them at all.[77]

48 Furthermore, the question arises: What if the data holder simply does not have metadata – or does not have *all*[78] of 'the relevant metadata necessary to interpret and use those data'?[79] This issue is seemingly not regulated under the Data Act. Considering that data usability is a relative concept, the metadata at the disposal of the data holder might make product or service data more usable but not ideal from the prospective data user's perspective. Should a dispute between the data holder and the user arise in this regard, the user can contest the fulfilment of the obligations before a dispute settlement body or 'seek an effective remedy' before a Member State's court or tribunal.[80]

V. An interim conclusion

49 The overall approach taken by the Data Act regarding data usability can be characterised as establishing minimum conditions for data utilisation. From a technical perspective, even if only raw sensor-generated data is made available, the inclusion of all 'relevant' metadata should enable its utilisation. The practicality, feasibility, and efficiency of this approach would depend on the specifics of the scenario and the technical and economic capabilities of the data user. From a legal perspective, the technical state of shareable data – hence, the scope of data-sharing obligations – are challenging to delineate due to the ambiguous legal criteria examined in this part. This ambiguity introduces the potential for disputes if such limiting criteria are interpreted in a way jeopardising data utilisation. Considering that the latter is the very purpose of the Data Act, data usability may and should carry significant weight in the legal assessment in contested cases.

69 art 3(1) Data Act.

70 arts 4(1) and 5(1) Data Act.

71 Apart from an exemplifying reference to the data's 'basic context and timestamp' (rec 15). From a technical perspective, contextual information should encompass the sensor's location, which is particularly useful in cases where multiple sensors detect the same physical phenomenon, as well as the sensor's specifications, typically including details such as calibration accuracy, sensor precision, etc.

72 rec 31; arts 4(6)-(8) and 5(9)-(11) Data Act.

73 rec 31 Data Act: 'While this Regulation requires data holders to disclose certain data to users, or third parties of a user's choice, even when such data qualify for protection as trade secrets, it should be interpreted in such a manner as to preserve the protection afforded to trade secrets under Directive (EU) 2016/943.'

74 arts 4(6) and 5(9) Data Act. In particular, such agreed measures directed at the preservation of the 'confidentiality of data considered to be trade secrets' include 'model contractual terms, confidentiality agreements, strict access protocols, technical standards and the application of codes of conduct' (rec 31 Data Act).

75 arts 4(6)-(8); 5(9)-(11); 6(2)(c), (g); 8(6); Data Act.

76 arts 4(6)-(8) and 5(9)-(11) Data Act.

77 This follows from the trade secret holder's (voluntary) consent being the condition for the lawful acquisition, use, and disclosure of trade secrets (art 4 of Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, OJ L 157, 15.6.2016, p. 1–18).

78 In practice, manufacturers may not have at their disposal all the metadata relevant to the needs of the prospective data users, as the assessment of the relevance of certain metadata can differ between a data recipient and a manufacturer. For instance, if a manufacturer utilises a temperature sensor solely to generate an on-off signal, indicating whether the temperature exceeds a specific threshold, the manufacturer may not have the metadata, e.g. concerning the sensor's accuracy and calibration outside the temperature range of interest. However, this incomplete information may become an issue of missing metadata if a data recipient decides to use the sensor data for recording temperatures beyond the manufacturer's range of interest.

79 recs 15 and 20; arts 3(1), 4(1), and 5(1) Data Act.

80 art 10(13) Data Act.

D. Normative considerations

50 The Data Act serves as a regulatory instrument aiming to 'maximise the value of data in the economy and society'.[81] In light of its instrumental nature, the validity of the Data Act hinges on how well it aligns with the intended objectives. Furthermore, its legitimacy is contingent upon its adherence to the balance of interests as a fundamental principle of policymaking.

I. Uncertainty within the 'means-ends' relationship

51 According to the intervention logic outlined by the Commission in its ex-ante impact assessment, the Data Act should maximise the value of data, particularly by increasing the availability of data for innovation.[82] In this logic, the new access and use rights, along with the corresponding obligations to make data available, specifically target 'legal uncertainty for consumers and businesses concerning data access and use' and 'abuse of contractual imbalances with regard to data access' in the B2B and B2C context.[83]

52 As discussed, data usability was not envisaged in the initial proposal but was addressed at a relatively late stage in the legislative process. While several provisions of the Data Act bear on data usability, the overall impression is that it lacks thorough consideration. In an attempt to remedy the shortcomings of the original proposal, a number of concepts were introduced – 'source or primary' data, 'data in raw form [...] which are not substantially modified' distinguished from 'pre-processed data' which does not involve 'substantial investment' in processing, contrasted with 'readily available data' delineated by 'a simple operation' and 'disproportionate effort', yet distinct from 'derived' or 'inferred' data or information defined by 'additional investment' and the complexity of an algorithm. This terminology appears convoluted, lacks coherence and clarity, and undermines legal certainty in defining the scope of data falling within the obligation to make data available. Furthermore, comparing the notion of 'readily available data' under Articles 4(1) and 5(1) with making data 'directly accessible' under Article 3(1) Data Act, the criteria of simplicity of operations or proportionality of effort, applicable to the former type, might lead to discrimination between the scope and technical states of data 'directly accessible' vs. made 'readily available' to users.

53 Given the relative nature of the legal concepts involving relative qualifiers 'substantial', 'simple', and 'disproportionate', a certain middle ground appears inevitable, which introduces uncertainty. While courts may eventually need to establish a threshold and develop a corresponding test, having guidance clarifying the criteria regarding the technical state of data subject to the obligation of making data available could have streamlined data access. The absence of a specific[84] or general[85] mandate vested by the Data Act in the European Commission or the European Data Innovation Board suggests that the legislature had not anticipated uncertainty regarding the technical aspects of data usability. The European Commission could proactively address this issue by developing guidance clarifying these criteria and what exactly they imply for the technical state of data subject to the obligation of making data available. To the extent that ambiguity surrounding the applicable threshold can be leveraged to interpret data-sharing obligations narrowly, compromise data usability, or give rise to disagreements over the technical state of data between the data holder and the user or third-party data recipients, these qualitative criteria may jeopardise the benefits anticipated from the Data Act.

II. An alternative approach?

54 The Data Act has already faced criticism for the overall design of its data-sharing mechanism, being deemed cumbersome in practice, lacking a sound economic justification, and suboptimal for fostering the data economy.[86] Even though this framework is not going to be changed in the near future, we would like to contemplate an alternative approach: What if the qualitative criteria of 'a simple operation' and 'disproportionate effort' were eliminated from the definition of 'readily available data' – along with eliminating substantial investment as a criterion of 'pre-processed data' – in view of their potential to diminish the scope and technical state of data, and, consequently, data utility? In other words, what if data were subject to the data-sharing obligations in the same technical state and scope as it is obtained from a product or service, including pre-processing that takes place within that product or

81 SWD(2022) 34 final 26-28.

82 ibid.

83 ibid.

84 Such as the development and adoption of interoperability standards in the context of common European data spaces and data processing services.

85 Akin to Article 47 of the Digital Market Act (laying the basis for the Commission to 'adopt guidelines on any of the aspects of this Regulation in order to facilitate its effective implementation and enforcement').

86 (n 17).

service to ensure its functionality?[87] Assuming all other parameters of the data-sharing regime stay the same, how would eliminating such constraints impact the equilibrium of interests, relative to the baseline established by the Data Act?

55 From the data usability perspective, removing the qualitative constraints on shareable data would be beneficial. In principle, even if 'readily available data' turns out to be data in its raw form,[88] it would allow the data user to extract value through purpose-specific processing if supplemented with the relevant metadata. As noted earlier, raw or generically processed data holds the highest potential for generating diverse outcomes and serving various use cases. In the case of sensor-generated data, it would be advantageous in terms of data usability if in-device processing of connected product data included calibration and de-noising, as the resulting level of accuracy and precision is typically sufficient to ensure product functionality. Provided that the relevant metadata is made available, raw or generically processed data can serve both primary purposes (i.e., ensuring product functionality, including product maintenance and repair) and secondary purposes, where data serves as input in new product or service development, often involving data aggregation.

56 From a legal perspective, omitting the criteria of 'simple operation' and 'disproportionate effort' from the definition of the 'readily available data' would reduce legal uncertainty concerning the determination of an elusive threshold of simplicity and proportionality, especially considering that the point of reference (proportionate to what?) is unclear.

57 From a balance-of-interests perspective, removing constraints on 'readily available data' – to the extent this could enhance data usability – would benefit prospective data users, both product/service users and third parties of their choice. For users, this would not entail additional costs, given that data should be made available to them free of charge to them (while the corresponding cost would be calculated within the market price of the product or service). For third-party recipients, this is a matter of compensation which they have to pay for data anyway.[89] Given that data can be made available to third-party data recipients under fair, reasonable, and non-discriminatory (FRAND) terms and conditions,[90] these terms can reflect the difference in the technical state of the data, i.e., either reduced to 'simple operations' or involving processing beyond this level. Hence, they can be adjusted to reflect the cost of data processing.[91] In this view, it is unclear why shareable data should be constrained by the 'simplicity' of operations, 'proportionality' of efforts, or 'substantiality' of investment.

58 For data holders, the current constraints within the definition of 'readily available data' might appear as a safeguard for their economic incentives and, hence, one would conjecture negative consequences ensuing if they were removed. Limitations on the scope and the technical state of shareable data[92] under the Data Act might be read as a precaution to prevent data-sharing obligations from becoming 'too burdensome' for data holders. Some could view this as the legislature's attempt to strike a fair balance between enabling broader access to and meaningful utilisation of data across a broad spectrum of use cases while avoiding imposing onerous requirements on parties under data-sharing obligations. However, such a restrictive approach to data sharing, tiptoeing around the data holders, might also be viewed as overly favouring their interests, without a sound justification.[93]

59 In principle, the requirement to share data in the technical state as it is obtained from a product or service would not interfere with the economic calculus underlying the current data-sharing obligations under the Data Act, particularly by imposing additional costs on data holder. By requiring data to be made directly accessible by the

87 While the technical state of data is determined by the product or service design, there is still some room for variability. For instance, the product can be designed to transmit data states A, B, C, D, and E. By default, the 'related service' may only necessitate states A and B, resulting in only A and B being transmitted. However, C can also be transmitted to the user if necessary.

88 As argued earlier, the conversion of an analogue to a digital signal can already be argued to satisfy the definitional criteria of 'readily available data' under art 2(17) Data Act.

89 art 8 Data Act.

90 This is not to idealise the FRAND system, the shortcomings of which have been discussed elsewhere. See eg Drexl J and others (n 17) para 99 ff; Picht PG, 'Caught in the Acts: Framing Mandatory Data Access Transactions under the Data Act, Further EU Digital Regulation Acts, and Competition Law' (2023) 14 Journal of European Competition Law & Practice 67, 26 ff; Kerber (n 17) 126. To clarify, here we are only comparing the option of removing the restrictions on the accessible and shareable data versus the existing baseline adopted in the Data Act, without challenging the latter.

91 art 9 Data Act.

92 This manifests in excluding the following categories of data from the scope of the Data Act: cleansed or transformed data requiring 'substantial investment', inferred or derived data or information due to 'additional investment', and readily available data if it requires 'disproportionate effort going beyond a simple operation' (rec 15; arts 2(17), 4(1), and 5(1) Data Act).

93 Kerber (n 17).

user free of charge,[94] the legislature must assume that the relevant costs, including building data-sharing infrastructure, will be passed on to the consumer, i.e. factored into the price of the product or service. Otherwise, this requirement would not be rational or economically viable. While these costs can be calculated within the market price of a product or service, data holders can also charge additional compensation for making data available to third-party data recipients. Here we do not question the economic logic of this model. Our point is that removing constraints on 'readily available data' would not impose on data holders additional costs relative to what is already required under the Data Act. Neither would this interpretation require the data holder to provide additional data processing beyond what already occurs within the product or service to ensure its functionality. In this view, it is unclear how removing constraints on readily available data – i.e. data generated and pre-processed to the point at which it is obtained from a connected product or related service – could jeopardise the economic incentives of data holders. If the restrictive criteria – 'simplicity' of operations, 'proportionality' of efforts, and 'substantiality' of investment – enable data holders to further maximise their profits at the expense of diminished data usability, one can question the current 'balance of interests' established by the Data Act.[95]

60 More broadly, protection of investment, incentives, and competitive advantage surfaces in several instances, such as when prohibiting using shared data for developing competing – interchangeable or substitutable – products;[96] when providing for the possibility for the data holders to request reasonable compensation for making data available in the context of B2B relations to 'promote continued investment in generating and making available valuable data, including investments in relevant technical tools';[97] when emphasising the importance 'to preserve incentives to invest in products with functionalities based on the use of data from sensors built into those products';[98] and when pointing to 'the lack of predictability of economic returns from investing in the curation and making available of datasets or data products' as a 'substantial hurdle to data sharing by businesses'.[99]

61 Of all these concerns, confining 'readily available data' by criteria of 'simple operations', 'disproportionate effort', and 'insubstantial investment' appears most relevant for incentives for data curation. However, it is questionable whether mandatory sharing of data puts at risk the incentives for data curation if such curation is confined to in-device or on-server data processing as part of *ensuring product functionality*, and given that the cost of processing can be factored within the product/service price, as well as the compensation for making data available. Given that the Data Act provides limited grounds for refusing an access request,[100] the restrictive criteria of 'simple operations' and 'disproportionate effort' cannot be invoked to substantiate a refusal to make data available altogether. Instead, the data holder may attempt to rely on these constraints to limit the readily available data in terms of its scope and technical state. However, from a practical perspective, it might be more feasible and beneficial for the data holder to make data available in the technical state it is obtained from a product or service and factor the related cost into the amount of 'fair compensation', rather than splitting data flows into two tracks – one with data in its 'natural' condition and the other one satisfying the restrictive qualitative criteria of 'readily available data'.

62 In summary, all other things being equal, removing constraints on the shareable data could have been more net-positive. Recognising that amending the Data Act remains a distant prospect, this consideration could be incorporated into dispute resolution and judicial practices, as well as future sectoral legislation. This could involve either removing the above-discussed constraints on the scope of shareable data or applying a stricter standard for defining what qualifies as 'disproportionate effort' or 'substantial investment'. To emphasise, this paper does not delve into the analysis of whether and to what extent the compromise reached within the Data Act is economically sound and balanced from a broader perspective of innovation incentives, including beyond those of data holders. Instead, we consider the existing deal as a baseline and explore the option of omitting constraints from the definitions of 'readily available data' and 'pre-processed' data, relative to this baseline. At the same time, it is worth noting that concerns have been raised about whether the baseline is optimal and justified from an incentives perspective, whether the compensation is needed to 'promote continued investment in generating' data,[101] and whether the latter is at risk at all.[102]

E. Conclusion

94 art 3(1) Data Act.

95 For a critical perspective on the overemphasis on the protection of incentives for data holders, see Kerber (n 17).

96 recs 32, 39, and 57; arts 4(10) and 6(2)(e) Data Act.

97 rec 46 Data Act.

98 rec 30 Data Act.

99 rec 26 Data Act.

100 Namely based on security reasons and trade secrets protection (art 4(2) and (8) and art 5(11)).

101 rec 46.

102 Kerber (n 17).

63 From the outset, the Data Act was conceived as a horizontal instrument, leaving the door open for further legislation to accommodate sectoral specifics, provided that sector-specific rules align with the Data Act.[103] Despite the Commission's engagement with stakeholders during the preparatory stage, the adopted horizontal, top-down approach had to maintain a generic – agnostic to the specific requirements of individual sectors or use cases – stance regarding the rules. The limitations of this 'access-in-the-abstract' strategy became evident during the late stage of the legislative process when it became apparent that some vital technical details had been overlooked. The late attempt to pivot and align the Data Act with the technical practicalities of data-sharing and usage resulted in populating the statutory text with ambiguous and hardly practical notions, including 'readily available data', 'disproportionate efforts', 'simple operation', 'pre-processed data', and 'significant investment'. This initiated a cycle of perpetual clarification, wherein the introduction of 'clarifying' terms necessitates further clarification.

64 In this paper, we examined how the Data Act addresses the need to enable data usability, apart from data accessibility, both of which are equally important for the maximisation of the value of data. As shown, the definition of the technical state of data constitutes a parameter of data access and usage rights, directly bearing on the scope of data subject to data-sharing obligations under the Data Act. However, the limiting criteria applicable to 'readily available data' pose a challenge in delineating this scope and might offset data usability. As an alternative approach, we have considered omitting such criteria from the definition of readily available data and argued that this holds the potential to yield a more positive overall outcome in terms of technical usability, legal certainty, and a balance of interests.

103 SWD(2022) 34 final 7. However, considering that subsequent rules should align with the Data Act, the concern is that the Data Act might pre-emptively limit the flexibility of these rules to accommodate for the specifics of the sector or use cases.

1 Table Annex

Some data pre-processing steps and their contribution to and dependence on data usability.

The type of data transformation	Changes to data	Possible contributions to the usability of the transformed data in future steps	Possible dependence on the usability of the data being transformed	Cost considerations
Calibration	Converts raw sensor data (unitless signal strength) to calibrated data with known accuracy and an interpretable unit of measurement such as degree Celsius for temperature.	Usually an early step, any future step that builds upon a well-calibrated dataset will benefit from the better accuracy so acquired. With interpretable data, relevant physical laws might be applied to treat the data in a future data pre-processing step.	Calibration requires sensor data to be available so that comparisons can be made between the sensor's readings and the standard values being calibrated.	Calibration equipment cost or calibration service charge.
De-noising	Reduces the fluctuation in data caused by noise to increase the signal-to-noise ratio.	Usually, an early step, as any future step that builds upon a dataset with minimal noise will benefit from the better precision so acquired. Revealing the signals helps discover patterns in the extraction pre-processing step. Imprecise data is bad for many machine learning algorithms.	Missing values can degrade the performance of de-noising algorithms that rely on aggregating existing data values.	Labour cost in research and development, involving examination of the characteristics of the data being treated, as well as selecting and configuring the best-performing approach through experimentation with various possible approaches.
Missing value imputation	Fills the values that are missing due to reasons such as sensor or device downtime, communication loss, or data corruption.	Increase the percentage of available data, which is important for statistically based machine learning algorithms; Many machine-learning algorithms cannot deal with missing values.	Many imputation algorithms make use of existing values (from any co-working sensors) to estimate the missing ones. Therefore, inaccurate and/or imprecise existing values will result in poor estimations.	
Selection (including techniques such as outliers detection, feature selection, data reduction, and instance selection)	Filters out unusable data such as irrelevant data, or data samples with outlier values or too many missing values.	Removing unhelpful data may improve the performance of a machine-learning model.	Inaccurate or imprecise data might lead to wrong decisions.	
Extraction (including techniques such as feature engineering and data fusion)	Creates new data from the existing dataset, e.g., temperature and relative humidity can be combined to get the amount of water vapour in the air.	New data, which is a strong indicator of the variable being predicted by a machine learning model, can boost the model's performance. Aggregation of data can reduce network traffic.	Garbage-in, garbage-out: the quality of the selected and extracted data depends on the quality of the data being transformed.	

Copyright and eLending in public libraries: an incomplete revolution?

by **Matteo Frigeri, Martin Kretschmer, Péter Mezei ***

Abstract: The central purpose of public libraries can be described as the need to meet the informational and knowledge needs of societies, which has both an economic and a cultural dimension. These fundamental policy concerns underpin the interventions at EU level, such as the Public Lending Right (Rental and Lending Rights Directive 92/100/EC, codified as 2006/115/EC), and the jurisprudence of the Court of Justice of the European Union (CJEU). However, the understanding has been muddied in subsequent rulings by the CJEU that address the new possibilities of digital libraries. While in VOB (C-174/15), the Court adopts a dynamic or evolving interpretation by extending the concept of Lending to eLending, Tom Kabinet (C-263/18) reduces the possibility of libraries to access digital copies of books by narrowing the scope for digital exhaustion. This article traces the policy context of the Public Lending Right in this light and assesses what lawful sources may be available for libraries to obtain access to digital copies of books for the purposes of eLending. The findings are bleak: Libraries following VOB are free to lend electronically to the public, however in practice they have been left without a digital collection. The article argues that it is in the public interest to maintain the equivalence of Lending and eLending and offers a range of possible interventions (under copyright, consumer and contract law) that may support the goals of libraries in the digital space.

Keywords: eLending, copyright, digital exhaustion, digitalisation, and communication to the public

Recommended citation: Matteo Frigeri, Martin Kretschmer, Péter Mezei, Copyright and eLending in public libraries: an incomplete revolution?, 15 (2024) JIPITEC 156 para 1.

A. Introduction

1 The digitalisation of print media has radically reshaped the way literary works, notably books, magazines, and scientific papers, are disseminated and consumed, opening up fresh possibilities and challenges for access to knowledge.[1] The knock-on effects of this transformation have instigated a

* Matteo Frigeri is Research Associate, Centre for IT & IP Law (CiTiP), KU Leuven; Martin Kretschmer is Professor of Intellectual Property Law and Director of the CREATe Centre, University of Glasgow; Péter Mezei is Professor of Law, Faculty of Law and Political Sciences, University of Szeged and Chief Researcher, Vytautas Kavolis Transdisciplinary Research Institute, Vytautas Magnus University. The research was funded by the project "The Law and Economics of eLending in Europe" at the CREATe Centre, University of Glasgow, under a grant by Knowledge Rights 21/ Arcadia – a charitable fund of Lisbet Rausing and Peter Baldwin. An empirical market study and a competition law analysis of eLending will complement this copyright paper. Prof. Mezei's research was supported by the Digital Society Competence Centre of the Humanities and Social Sciences Cluster of the Centre of Excellence for Interdisciplinary Research, Development and Innovation of the University of Szeged. The author is a member of the Legal, Political Aspects of the Digital Public Sphere research group.

1 For an overview of an early account of the changes in the publishing industry brought by digitalisation, see generally Jean-Claude Guédon, *In Oldenburg's Long Shadow: Librarians, Research Scientists, Publishers and the Control of Scientific Publishing* (Association of Research Libraries, 2001).

shift in the prevailing social, economic, and legal paradigms (e.g., Open Access).[2]

2 The legal framework continuously strives to adapt to these advancements in technology and social practices. Reflecting these changes, new concepts are developed: 'digital exhaustion'[3] 'digital content',[4] and 'digital users',[5] are just a few examples. Similarly, the lending of eBooks ('eLending') has become increasingly more widespread.[6] From the perspective of libraries, pursuing their mission of promoting 'education, research and access to information'[7] requires them to offer eLending[8] as a service complementary to the lending of printed books. Nonetheless, while there is a general agreement among librarians that eLending should be part of the library's services, eLending is not a monolithic concept: different eLending models – e.g., one-copy/one-user - coexist in Europe[9] and beyond,[10] and its essential features still remain largely contested.[11]

3 There is no doubt eLending poses difficult questions, and is characterised by conflicting interests and views. It forces us to balance private and public interests. If the development of an eLending service is left entirely to a negotiation with publishers, there are questions on the economic affordability of this model, especially when the decreasing budgets of libraries are considered.[12] As a result, local libraries may be priced out of this service.[13] Even when libraries can afford to pay for the eLending licences, they still have no redress if publishers refuse to license access to the eBook,[14] with some recent examples symbolising the lack of legal redress in such cases.[15] Publishers, on the other

2 The principles of the Open Access Movement are outlined in the Declaration by the Budapest Open Access Initiative (BOAI) – BOAI, 'Declaration' (2002) https://www.budapestopenaccessinitiative.org/read/.

3 Broadly stated, digital exhaustion refers to the legal doctrine according to which the first sale or transfer of ownership of digital content (e.g., eBooks) exhausts the right of the rightholders to control further resales of the digital content. The first case recognising a form of digital exhaustion was C-128/11 UsedSoft (CJEU) ECLI:EU:C:2012:407. For an in-depth discussion of the doctrine, see Péter Mezei, *Copyright Exhaustion: Law and Policy in the United States and the European Union* (Cambridge University Press 2022); Caterina Sganga, 'A Plea for Digital Exhaustion in EU Copyright Law' (2018) 9 JIPITEC 211, para 1; Simon Geiregat, *Supplying and Reselling Digital Content – Digital Exhaustion in EU Copyright and Neighbouring Rights Law* (Edward Elgar 2022).

4 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.

5 L Oprysk and K Sein, 'Limitations in End-User Licensing Agreements: Is there a Lack of Conformity Under the New Digital Content Directive?' (2020) 51 IIC 594.

6 Andrew R Albanese, 'Frankfurt Spotlight: Library E-books Have Leveled Up' (*Publishers Weekly*, 2022) <Frankfurt Spotlight: Library E-books Have Leveled Up (publishersweekly.com)>.

7 WIPO, 'Objectives and principles for exceptions and limitations for libraries and archives' (Document presented to SCCR Committee, 2013) p. 2.

8 This mission was also stressed by AG Szpunar in his Opinion to C-174/15 - Vereniging Openbare Bibliotheken (AG Opinion C-174/15 VOB) ECLI:EU:C:2016:856, para 1-3.

9 Dan Mount, 'Research for cult committee – eLending: Challenges and opportunities' (EU Parliament, 2016) ('eLending Report').

10 O'Brien et al.., 'E-books in Libraries: A Briefing Document Developed in Preparation for a Workshop on eLending in Libraries' (Berkman Center Research Publication, 2012) ('US eLending report'), p. 29.

11 For example, publishers may consider that access to an eBook on the basis of a subscription model may act as a substitute for libraries, giving access to a collection of eBooks for a monthly fee. Similarly, platforms such as OverDrive may be deemed to already offer a viable lending model for eBooks.

12 This may be described as an ''affordability'' problem – see Manon A Ress, 'Open-Access Publishing: From Principles to Practice' in G Krikorian and A Kapczynski (eds.), *Access to Knowledge in the Age of Intellectual Property* (Zone Books 2010), p. 477-478.

13 AG Opinion C-174/15 VOB (n. 8), para 38.

14 Ibid. For libraries, eLending is framed as an existential crisis. This is well captured by the words of AG Szpunar in C-174/15 VOB, where he stated that 'If libraries are unable to adapt to this trend, they risk marginalisation and may no longer be able to fulfil the task of cultural dissemination which they have performed for thousands of years'. See AG in C-174/15 VOB (n. 8) para 3. A similarly ominous warning had also been raised by Sieghart: 'the inability to offer eLending will make libraries increasingly irrelevant in a relatively short time'. See William Sieghart, An Independent Review of eLending in Public Libraries in England ('Sieghart Review') (Report of Department for Culture, Media and Sport, 2013), p. 7. Iterations of this statement are widely found in the literature. See Séverine Dusollier, 'A Manifesto for an eLending Limitation in Copyright' (2014) 5 JIPITEC 213, para 3: 'libraries will lose a great part of their role in society, and most of their soul'.

15 See Wiley case for a recent example. Hohoyanna (2022) Wiley withdrawing key eBook titles from library collections – evidence required please available at: https://academicebookinvestigation.org/2022/09/07/wiley-withdrawing-key-ebook-titles-from-library-collections-evidence-required-please/.

hand, lament that by allowing the public to freely access books digitally, a displacement of sales will occur, thus negatively affecting the growth of their eBook markets.[16] More ambiguous is the position of authors – but this is mostly due to the opacity of their contractual arrangements with publishers; however, secondary evidence suggests that they may be worse off in terms of remuneration for digital consumption of their works when compared to print,[17] in a market that has long sinceshown a reduction in authors' long-term earning potential.[18]

4 These clashes are not new to the publishing industry. As an illustration, both 'private lending'[19] and 'dollar books'[20] have been similarly characterised as existential threats to publishers.[21] Such demands to resist economic and technological changes need therefore to be carefully assessed based on the available evidence.[22] The focus of this Article will move however in a different direction, looking at how the law regulates and adapts to these changes.

5 The context is based on the relatively recent judgments issued by the CJEU in C-174/15 VOB (2016)[23] and C-263/18 Tom Kabinet (2019).[24] The Court's decisions offered an interpretation of how copyright law regulates the temporary distribution of digital copies of books. As this Article demonstrates, these two decisions are closely interlinked; the piecemeal approach taken by the Court, which fails to regulate consistently temporary digital distribution of books – whether commercial or non-commercial – raises significant issues that need to be urgently addressed. No evidence is more telling than the fact that, despite that in C-174/15 VOB the Court offered Member States the possibility to allow libraries to offer eLending on the same basis as the lending of printed books, no Member States has seized that opportunity. While this may well be due to a lack of political appetite, this Article demonstrates how legal equivalence between lending of books and eBooks cannot be implemented in practice. Some policy recommendations will be canvassed at the end to redress this issue.

6 The scope of this Article will therefore be to evaluate the recent judicial interventions of the CJEU (C-174/15 VOB; C-263/18 Tom Kabinet) against the background of the wider EU policy on the lending of digital and physical books. In doing so, the implications of the Court's judgment in C-174/15 VOB on eLending will be assessed in light of C-263/18 Tom Kabinet judgment.

7 The analysis will be developed in different stages. The lending of books by libraries to the public will be the starting point of the discussion.[25] The Article

16 In particular, see Breemen et al., 'Online uitlenen van e-books door bibliotheken: verkenning juridische mogelijkheden en economische effecten' ('Dutch eLending report') (2012) AmsterdamSEO Economisch Onderzoek/IviR, p. 51-52.

17 In relation to eLending, see AG Opinion C-174/15 VOB (n. 8) para 34. The format of the books affects the share of royalty to which authors are entitled, including for sales of books. For paperback titles, earnings are divided in a 50-50 split, whereas standard contracts for eBooks entitles author to a 25% share of the list price. See The Authors Guild, 'Half of Net Proceeds Is the Fair Royalty Rate for E-Books' (*The Authors Guild, 9th July 2015*). <https://authorsguild.org/news/half-of-net-proceeds-is-the-fair-royalty-rate-for-e-books/>; Jane Friedman, 'What Do Authors Earn from Digital Lending at Libraries?' (*Jane Friedman*, 30th October 2021). https://www.janefriedman.com/what-do-authors-earn-from-digital-lending-at-libraries/.

18 See Thomas et al., 'Authors' Earnings in the UK' (PEC, 2023) p. 8. See also generally CREATe's ongoing Project monitoring of authors' earnings: 'Authors' Earnings and Contracts' <https://www.create.ac.uk/project/creative-industries/2022/12/08/authors-earnings-and-contracts/>.

19 'The fate of a book after it is sold is an important one for the book industry, reflecting as it does the possibility of lost sales' in L A Wood, 'The Pass-Along Market for Books: Something to Ponder for Publishers' (1983) Publishers Weekly.

20 'Dollar books' refers to the pricing policy adopted by new publishers on the market (including Simon & Schuster, founded in 1924) to 'reduce the price of their new hardcover fiction books to one dollar in order to compete with remainders and proliferating cheap reprint series'. At the time, a study carried out by the Book Publishers Research Institute forecasted that dollar books would result in the 'death of six thousand book retailers'. See Ted Striphas, *The late age of print: Everyday book culture from consumerism to control* (Columbia University Press 2009), p. 34-35, relying on the account provided in Edward L Bernays, *Biography of an Idea: Memoirs of Public Relations Counsel Edward L. Bernays* (Simon & Schuster 1965), p. 485.

21 A notable proponent of this narrative was George Orwell, who once described 'cheap books' as a 'disaster' for publishers. See Milton Friedman, *Price Theory* (New Brunswick 2008).

22 Access to data is a major obstacle in testing claims made on either side – whether libraries or publishers. However, several empirical studies focus on demand substitution in the book sector. As an example, see: Anindya et al., 'Internet Exchanges for used Books: An Empirical Analysis of Product Cannibalization and Welfare Impact' (2006) 17/1 Information Systems Research 3; K Kanazawa and K Kawaguchi, 'Displacement Effects of Public Libraries' (2022) 66 Journal of the Japanese and International Economies 101219.

23 C-174/15 – Vereniging Openbare Bibliotheken (VOB) [2016] (CJEU) ECLI:EU:C:2016:856.

24 C-263/18 Nederlands Uitgeversverbond and Groep Algemene Uitgevers ('C-263/18 Tom Kabinet') (CJEU) ECLI:EU:C:2019:111.

25 This practice has both long-established social and historical foundations and is a classic example of a form of non-

will describe how the EU regulated public lending, what policy goals the legislation was meant to promote, and the nature and the scope of the rights it established – first and foremost, the Public Lending Right (PL right)[26] in the Lending Right Directive.[27] A second crucial step is then to determine the extent to which the identified policy goals were intended to be exported into the digital world, adapting the PL right to new developments in 'technology, market, and behaviour'.[28] The policy and judicial developments reviewed in this section will culminate in the analysis of the CJEU's judgment in C-174/15 VOB, a landmark case in so far as the scope of the PL right was proactively extended to cover acts of lending of digital copies of books, subject to some conditions.

8 Despite the fact that this judgment promised to ensure legal equivalence between lending and eLending, little changed following this ruling. The third section will proceed with examining the causes of the lack of effectiveness of the Court's ruling. Emphasis will be placed on a specific condition introduced by the CJEU for extending the PL right to eLending: that libraries first obtain the digital copies of the books from a lawful source.

9 It is submitted that unless libraries are granted independent powers to obtain digital copies of books, eLending will remain largely shaped by market forces, potentially negatively impacting the public goals that the Lending Right Directive was meant to promote. To solve this, the Article will conclude by highlighting several policy options to either increase or even guarantee libraries independent means of access to digital copies when offering an eLending service.

commercial access to knowledge.

26 PL right refers to the right to authorise the making available for use to the public of copyright works, for a limited period of time and not for direct or indirect economic or commercial advantage, through establishments accessible to the public – see Art 1 and 2 of the Lending Right Directive. In simpler terms, it regulates the ability of publicly accessible libraries to lend copyright works (e.g., books) to the public.

27 Directive 2006/115/EC on rental right and lending right and on certain rights related to copyright in the field of intellectual property (2006) L 376/28 ('Lending Right Directive').

28 AG Opinion C-174/15 VOB (n. 8) para 27.

B. Regulating access to knowledge – the introduction of the Public Lending Right

I. The Origins of the Public Lending Right

10 The public lending of literary works, especially books, is one of the core activities of libraries.[29] Although part of a library's collection may be composed of public domain works, a considerable portion remains protected by copyright.[30] Following the harmonisation of the PL right[31] in 1992[32] across the EU, the lending of books to the public has been added to the exclusive rights of authors.

11 It is not altogether evident why authors should be able to prevent the public lending of books, an activity traditionally held to be a prerogative of libraries. Unsurprisingly, the justification for the creation of this right has been 'one of the most disputed issues' of the Lending Right Directive, with critics highlighting how lending does not create any additional economic value to be redistributed back to authors.[33]

12 Considering that, following C-174/15 VOB, this Directive may also regulate the lending of digital copies of books by public libraries ('eLending'),

29 Dusollier (n. 14) para 7.

30 The extensive duration of the term of copyright – extending to the life of the author + 70 years – means that almost all books written after 1950 are still currently protected by copyright; As acknowledged by Recital 10 of Commission, Recommendation 2006/585/EC on the digitisation and online accessibility of cultural material and digital preservation O.J.C.E. L 236/28, 31 August 2006. See also Commission, 'i2010:Digital Libraries' (Communication, 2005), p. 6.

31 The ''right to authorise ... the lending of originals and copies of copyright works', with lending meaning 'making available for use, for a limited period of time and not for direct or indirect economic or commercial advantage, when it is made through establishments which are accessible to the public'. See, respectively, Directive (EU) 2006/115/EC on rental right and lending right and on certain rights related to copyright in the field of intellectual property ('Lending Right Directive') [2006] OJ L 376, artt 1(1) and 2(1)(b).

32 The lending right was harmonised by the Directive (EU) 92/100/EC, codified in Lending Right Directive (n. 27).

33 Silke von Lewinski, 'Rental and lending rights directive' in MM Walter and S von Lewinski (eds), *European Copyright Law: A Commentary* (OUP 2010), para 6.1.7; Ansgar Ohly, 'Economic rights' in Estelle Derclaye, *Research Handbook on the Future of EU Copyright* (Edward Elgar 2009), p. 224.

understanding its drafting history and the nature of the legislative compromise is essential.

13 The arguments in favour of harmonising the PL right at the EU level were first canvassed by Dietz in an Article in 1978.[34] In the Article he maintained that, unless authors are granted a non-exhaustible PL right, there is a 'high risk that editions of works would be greatly reduced' due to the growing resort to public libraries to access copyright-protected works'.[35] His concerns did not appear to be grounded in empirical evidence, being rather a matter of logical deduction from general principles: that copyright should cover 'mass utilization of works' and that authors be compensated for it.[36] Yet this does not automatically lead to a conclusion that authors should be granted an exclusive right to control lending; in fact, a remuneration right was considered equally satisfying by many Member States at the time[37].

14 Dietz's arguments were rejected by the Commission in the 1988 Green Paper.[38] The reasons were as follows:

15 1) minimal economic importance - public lending schemes generated small revenues, and, at the time, book rental was almost non-existent;

16 2) lack of consensus at the national level – only a minority of Member States had lending schemes in place at the time, and the Commission felt harmonisation would have interfered with national cultural policies;

17 3) the subject matter of harmonisation was considered inappropriate – the PL right was construed as involving the regulation of public financing of the cultural sector rather than harmonisation of the copyright system; and

18 4) the lack of a negative effect on the free circulation of books or on the development of the book publishing industry.[39]

19 The later decision to add the Lending Right Directive Proposal[40] ('the Proposal') to the legislative pipeline bears witness to a shift in the Commission's evaluation of the above factors. In particular, the Proposal describes lending as a 'considerable use' of copyrighted works both in terms of economic value and quantity of works affected, resulting in the 'displacement of sales'.[41] Despite the fact that a sufficient level of consensus had been gathered around the need for such a right, a division on exactly how this right should be defined and what exceptions should be provided persisted. The broadly worded definitions in the Directive and its permissive exceptions are a direct consequence of that.

II. Understanding the Public Lending Right

20 In the Lending Right Directive, lending is defined as 'making available for use, for a limited period of time and not for direct or indirect economic or commercial advantage, through *establishments ... accessible to the public*'.[42] As apparent from this definition, the PL right only covers a limited part of what we would normally define as non-commercial digital access to knowledge. For example, the policy of academic and research libraries more generally to allow users to permanently download full or part of eBooks would need to be reconsidered if such acts are to qualify as eLending, falling foul of the condition of temporary access.

21 Given what appears to be quite a demanding condition that the lending is of a non-commercial nature - 'not for direct or indirect economic or commercial advantage' - it should be noted that often these provisions have been subject to a more relaxed interpretation.[43] Interestingly, the lending right does not extend to inter-library loans, as specified by Recital 10 of the Directive.[44] Alongside a PL right, the Directive also introduced the possibility for Member States to allow libraries to carry out acts of public lending as long as authors received

34 Adolf Dietz, *Copyright Law in the European Community* (Alphen aan den Rijn 1978).

35 Ibid para 250.

36 Ibid.

37 In fact, several countries had already adopted 'library royalties': Germany, Denmark, and the Netherlands. Germany, for example, had introduced a 'sustainable compensation for hiring/loaning' of books under s 27, para 1 of the Federal German Copyright law of 1972. Other countries had similar system (Italy), and the UK was considering the enactment of a new regulation. See Dietz (n. 34) para 253-255.

38 Commission, 'Green Paper on Copyright and the Challenges of Technology' (Green Paper, 1988), COM(1988) 172.

39 Ibid para 4.4.4 to 4.4.10.

40 Proposal for a Council Directive on rental right, lending right, and on certain rights related to copyright (Lending Right Directive Proposal) COM/90/586 final.

41 Ibid para 9. The authors do not know whether the Commission relied on empirical evidence to draw such conclusions.

42 Lending Right Directive Art 2(b).

43 For example, it is generally accepted that the application of a yearly administrative fee for access to the library services will not be sufficient to give commercial character to the acts of making available. See Von Lewinski (n. 33) para 6.1.18-6.1.26.

44 Ibid Recital 10.

'remuneration' for such use[45] – a derogation from the PL right ('PL right exception').[46]

22 Notwithstanding its non-mandatory nature, the carving out of a specific PL right Exception for public libraries is an integral component of a harmonised PL right. In other words, the right and the exception work in tandem, resulting thus in the creation of a 'remuneration right'.[47] This means that rather than a right to control, the authors receive a right to obtain remuneration.

23 Since the explicit aim of the Lending Right Directive is to promote both economic and cultural values,[48] the exclusive nature of the PL right should not frustrate the ability of Member States to pursue their national cultural policies – for example, the promotion of access to works in public libraries.[49] Economic and cultural goals are deemed to complement each other: the remuneration of authors is considered to stimulate the creation of new works without limiting distribution.[50]

24 It is unclear whether this interpretation of the Directive coincides with the initial intentions of the Commission, which seemed to be more concerned about the negative impact of public lending on the ability of authors to exploit copyrighted works by rental.[51] However, the Court's expansive interpretation of the PL right in C-174/15 VOB shifted the emphasis on the importance of the cultural goals as a telos of the exception.[52]

25 It is also important to note that, while this paper and C-174/15 VOB focused exclusively on one category of works – namely, literary works in the form of books – the Directive is applicable more generally to different types of works, including films and recordings. It is therefore possible that a wider derogation in favour of eLending may be justified by the cultural and informative content of the work excluded from protection.[53] A flexible interpretation is also justified by the historic context of the Directive. At the time of its first entry into force, it represented an attempt to regulate the growing market for the renting of 'cassettes, CDs and DVDs'; shortly after being adopted, it increasingly became obsolete as the result of technological progress outstripping the pace of the legislative process.[54]

26 Even before harmonisation, some Member States already provided in their legislation for a PL right, either in the form of an exclusive right or a remuneration right[55] (most Member States had opted for the latter).[56] Public lending as a practice has long been 'deeply rooted in the national cultural traditions of the Member States'[57] and generally considered to strike a fair balance between the interests of the authors and the public – two notions which sometimes overlap. Its intrinsic connection with cultural policy makes it an area where the

45 Lending Right Directive Art 6(1). Some categories of establishment may be exempted from the need to provide remuneration - see Lending Directive Art 6(3).

46 There is an inherent confusion in the use of the term PL right. In fact, PL right may both cover the exclusive right under Art 2 and the remuneration right provided by Art5 of the Lending Right Directive. The right in Art 2 of could be described as a public Lending right in so far as it only applies to lending by publicly accessible establishments – it does not cover the lending by private parties (hence, a Public Lending right); the derogation in Art 6(1) of the Directive is more easily construed as an exception, although it contains a right to remuneration. For the sake of clarity, it would have been better had the legislation introduced a non-mandatory remuneration right, rather than this 'right + exception' configuration.

47 For some limited categories of establishments, Member States may even remove the obligation to remunerate authors (see Art 6(3) Lending Right Directive). This derogation should be interpreted restrictively – see *inter alia* C-198/05 Commission vs Italy [2006] ECLI:EU:C:2006:677 para 17-18. See Report from the Commission to the Council, the European Parliament and the Economic and Social Committee on the Public Lending Right in the European Union ('EU Report on PL right') (2002) COM(2002) 502 final, p. 5.

48 bid Recital 3: 'the adequate protection ... of lending rights ... [is] of fundamental importance for the economic and cultural development of the Community'.

49 Von Lewinski (n. 33) para 6.1.6.

50 Ibid Recital 5.

51 EU Report on PL right (n. 47) p. 4: 'the steady increase in public lending activities in the music and film sector might have a considerable negative effect on the rental business and thereby deprive the rental right of its meaning'.

52 C-174/15 VOB para 51: the extension of lending to cover digital lending was deemed justified by the 'the importance of the public lending of digital books' and 'the contribution of that exception to cultural promotion'. See also Lending Right Directive Art 6(1), which allows fixing the level of the remuneration in accordance with the Member State 'cultural promotion objectives'.

53 In other words, the recognition of the functional equivalence of digital and physical lending does not force us to recognise the equivalence between lending a videocassette and streaming music. Since its inception, some Member States were in favour of recognising lending rights only for some specific categories of media – Von Lewinski (n. 33) para 6.1.7.

54 The expression paraphrases the Opinion of AG in C-174/15 VOB at para 28.

55 The first country to introduce a PL right was Denmark in 1946. See EU Report on PL right (n. 47) p. 3.

56 Triaille et al., 'Study on the application of Directive 2001/29/EC on copyright and related rights in the information society' (Commission, 2013), p. 328.

57 Ibid p. 3.

Commission needs to exercise a degree of deference towards the competences of Member States.

27 It is interesting to contrast the PL right with the Communication to the Public right ('CP right'), harmonised under Art 3 InfoSoc.[58] The latter contains a different set of exceptions and safeguards that, from the perspective of libraries at least, may well be considered as much narrower than their counterpart in the Lending Right Directive. As such, the achievement of important cultural and societal goals specifically supported by the PL right exception does not find a corresponding counterpart in any of the exceptions in the InfoSoc For this reason, it is worth spending a considerable amount of time discussing under which regulatory regime certain acts should fall and whether there is any overlap between the PL right and the CP right.

28 As an initial remark, it can be maintained that the PL right does not seem to have ever been originally intended to cover digital access to books, despite that the question was considered.[59] Undoubtedly, this is partly due to the belief that the market will satisfactorily regulate and provide incentives to digitalise, distribute and make available eBooks to libraries for eLending, and any regulation at the time could prematurely stifle those attempts.[60] It remains an open question whether this rather liberalist approach is still warranted in light of the significant developments both in the eBook and eLending market.[61]

III. Does the Public Lending Right regulate eLending? Policy discussion before C-174/15 VOB

29 Before the judgment in C-174/15 VOB, the Commission had explicitly ruled out the possibility that the PL right could extend to eLending.[62] While recognising that – 'in practical economic terms' – digital and physical lending are functionally equivalent, it is desirable that such an extension should be 'confirmed in legislation'.[63] At the same time, the Commission also warned about the importance not only of reinforcing copyright in the context of digital forms of exploitation but also to 'recognise the interests of the different parties concerned', including users and libraries.[64] It is remarkable that already at the time of drafting InfoSoc in 1995, thus before the development of an eBook market, the Commission was already considering the regulation of eLending by public libraries.

30 It should also be noted that the CP right – due to its 'umbrella nature'[65] – is generally deemed to exclusively regulate the 'on-demand transmission of works', a category also capable of encompassing eLending.[66] This conclusion is also supported by the international obligations to which the signatories of the WIPO treaties[67] are subject, and is further justified in light of the impact of eLending on the economic interests of rightholders.[68]

31 It is therefore without surprise that for a long time, this question was considered settled. Many Member States had long held eLending to fall beyond the scope of the Lending Right Directive.[69] In its Communication on Digital Libraries in 2005, the Commission expressed its belief that 'a substantial change in the copyright legislation, or agreements [with rightholders]' would be necessary for libraries to be able to provide digital access to their collection.[70] The academic literature also generally leaned towards such view, although never explicitly excluding this possibility.[71]

32 While recognising that eLending 'may well play a major role' for libraries in the future, for the

58 Directive (EU) 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society ('InfoSoc') [2006] OJ L 167.

59 Caterina Sganga, 'Public eLending and the CJEU: chronicle of a missed revolution foretold' (2016) 1/2 Opinio Juris in Comparatione, p. 10. In building her argument, she refers to Lending Right Directive Proposal, p. 4.

60 Von Lewinski (n. 33) para 6.1.28.

61 Giblin et al, 'Available, but not accessible? Investigating publishers' eLending licensing practices' (2019) 24 Information research, p. 16.

62 EU Report on PL right (n. 47) p. 12.

63 Green Paper on Copyright and Related Rights, COM(1995) 382, p. 58.

64 Ibid p. 59.

65 'Guide to the Copyright and Related Rights Treaties Administered by WIPO' (WIPO, 2003), p. 207.

66 Commission, 'Follow-up to the Green Paper on Copyright and Related Rights in the Information Society' (Policy Document, 1996) COM(1996) 568, p. 12-14.

67 WIPO Copyright Treaty (WCT) art 10 and WIPO Performances and Phonograms Treaty (WPPT) art 16.

68 Commission, 'Travaux préparatoires for the Proposal for a Directive on the harmonization of certain aspects of copyright and related rights in the Information Society' ('Commission travaux préparatoires') (1997) COM(97) 628, p. 31.

69 See Sieghart Review (n. 14) p. 9 and 'Government response to the public consultation on the extension of the Public Lending Right to rights holders of books in non-print formats' (Department for Culture, Media & Sport, 2014), p. 10. See also Dutch eLending report (n. 16) p. 11.

70 i2010:Digital Libraries (n. 30) p. 6.

71 Dusollier (n. 14) para 28; Dutch eLending report (n. 16) p. 35.

Commission the organisation of this service was better regulated on a 'contractual basis, whether individual or collective agreements'.[72] At the same time, it was also recognised how the provision of digital access by '*public libraries* should not be subject to undue financial or other restrictions'.[73] Along the same line also follows Recital 40 InfoSoc, which while echoing the desire to leave the regulation of 'on-line delivery of protected works' to private ordering,[74] also reiterates that 'specific contracts or licences should be promoted which, *without creating imbalances*, favour such establishments and the disseminative purposes they serve'.[75]

33 Nonetheless it remains an open question which instruments are available to reconcile the possible negative effects of private ordering and IP rights with wider societal interests in access to knowledge. Even more so, considering that the CP right does not foresee any exception to support libraries in offering digital access to eBooks.[76]

34 At the time of writing, these policy aspirations seem to remain largely unachieved; undue restrictions and imbalances remain a prominent feature of the eLending market(s).[77] The tendency of private ordering to override rather than promote limitations and exceptions is also a process that would require a reconsideration of the effectiveness off market-based solutions.[78]

72 Ibid.

73 Ibid p. 32: 'Authors must be able to control the use of their works, libraries must ensure the transmission of available documents and users should have the widest possible access to those documents while respecting the rights or legitimate interests of everyone'.

74 This is partly due to the lack of exemption to the benefit of libraries for the exclusive CP right for online delivery of protected material to remote users, the economic importance of these uses and what at the time were considered 'new promising involving licenses, based on contracts' which showed the potential to arrive at mutually satisfactory solutions for all parties involved, including libraries'. See Commission travaux préparatoires (n. 68) p. 17-18.

75 InfoSoc Recital 40.

76 See ibid: 'Such an exception or limitation should not cover uses made in the context of on-line delivery of protected works or other subject-matter'.

77 Daniel A. Gross, 'The Surprisingly Big Business of Library E-Books' (The New Yorker, 2nd September 2021) <https://www.newyorker.com/news/annals-of-communications/an-app-called-libby-and-the-surprisingly-big-business-of-library-e-books>; Giblin et al, 'What can 100,000 books tell us about the international public library eLending landscape?' (2019) 24/3 Information research.

78 Lucie Guibault, 'Why Cherry-Picking Never Leads to Harmonisation The Case of the Limitations on Copyright under Directive 2001/29/EC' (2010) 1 JIPITEC 55, para 33.

79 See eLending Report (n. 9).

80 Sieghart Review (n. 14) p. 9.

81 The following principles are a summary of the recommendations made in the Sieghart Review. See Sieghart Review (n. 14) p. 8-9.

82 At the moment, the 'metered by loans' is a widely model adopted to calculate the duration of the license. This reflects both the nature of the right (e.g., each individual act of eLending is subject to authorisation) and the desire to implement a set of 'frictions' into eLending.

C. C-174/15 VOB – the Evolution of the Concept of Lending from Print to Digital

I. Prequel to the judgment in C-174/15 VOB

35 When the CJEU issued its judgment in C-174/15 VOB, different forms of eLending had already been tested in Europe. As eLending moved from concept to operation, a body of evidence and studies have emerged attempting to map the different models of eLending and how these work in practice, with one report being commissioned by the EU parliament.[79]

36 The salience of these studies lies in the fact that they all contributed to developing a conception of what eLending should be, defining the common principles that should underpin the provision of this service. Notable in this regard is the independent review of eLending carried out in England, where it was recommended that PL right should be extended to the lending of eBooks – in the words of the author, a critical step to 'allow libraries to progress with their digital strategies'.[80]

37 Among the variety of existing models, the study also extracted a common set of principles[81]:

- eLending should emulate its printed counterpart, in terms of 'friction' and the non-commercial nature of the lending books;
- eLending should allow access to books remotely, beyond the library premises;
- to reduce its economic impact on rightholders, the one-copy-one-user model should be adopted;
- to reflect the deterioration to which printed books are subject, the number of loans of digital copies of books should also be capped accordingly;[82] and
- the remuneration of authors should be ensured by the extension of PL right to both physical and digital

formats.[83]

38 As will be shown, these same principles were later to inform the notion functional equivalence between lending and eLending developed in C-174/15 VOB. The judgment refrains from citing directly any of these studies, yet they constitute an argumentative space within which the Court had to operate. Interesting in this respect is a study by the University of Amsterdam, that looked specifically at whether the (at the time) existing EU legislative framework could be relied upon to introduce an exception, and therefore enable, eLending by public libraries.[84]

39 The findings of the study – arguing, in contrast with the judgment in C-174/15 VOB, that the Lending Right Directive applies exclusively to physical copies of books – further cement the conclusion that the decision of the CJEU was surprising in its outcome,[85] and may be regarded as a remarkable instance of judicial activism. In light of what has so far been discussed, it is difficult not to see implicit in the Court's reasoning an impatience vis-à-vis the lack of legislative intervention in the regulation of eLending in Europe.

II. The interpretation of the concept of lending in C-174/15 VOB - a missed r/evolution?

40 The CJEU's judgment in C-174/15 VOB has already been the object of extensive analysis.[86] We will focus only on the most important elements relevant to the present discussion. In a nutshell, the CJEU held that the concept of lending in the Lending Right Directive extends to the 'lending of a digital copy of a book', provided that only one copy can be downloaded and that such a copy is made inaccessible after the expiry of the lending term.[87] The salience of the judgment stems from the promise to relieve libraries from reliance on publishers for offering their eLending service in so far as it will allow Member States to develop a governance framework within which eLending can be carried out under substantively the same conditions as the lending of printed books ('ePL right scheme').[88] However, the fulfilment of such a promise requires a degree of political goodwill from the national legislature, with little progress having been made so far.

41 The CJEU reached this judgment on the basis of a negative reasoning: it held that there is no decisive ground for excluding, *in all cases*, the lending of digital copies from the scope of the Lending Right Directive.[89] This conclusion was reached by looking at both international law,[90] and the drafting history of the Directive. The arguments in favour of a broader interpretation of the concept of 'lending a digital copy' were considered:

- the adaptation of copyright to 'new economic development' is presented as an explicit aspiration of the Directive – and, in the words of the CJEU, eLending 'indisputably forms part of those new forms of exploitation';[91]
- the extension of the scope of the Lending Right Directive to eLending is considered important both for ensuring the effectiveness of the PL right exception and meeting the objectives of the Directive - the promotion of culture;[92] and
- the recognition that assimilation of digital and physical lending cannot be ruled out in light of eLending's characteristics, which are 'essentially similar to the lending of printed books'.[93]

83 Sieghart Review (n. 16) p. 8-9.

84 Dutch eLending report (n. 16).

85 For an overview of C-174/15 VOB in the context of the Dutch eLending report, see Breemen (n. 16).

86 Breemen (n. 16) p. 249-253; Emma Linklater-Sahm, 'The Libraries Strike Back: The "right to e-Lend" Under the Rental and Lending Rights Directive: Vereniging Openbare Bibliotheken' (2017) 54/5 Common Market Law Review 1555; Caterina Sganga (n. 3); Rita Matulionyte, 'Lending e-Books in Libraries: Is a Technologically Neutral Approach the Solution?' (2017) 25/4 Int. J. Law Inf. Technol. 259.

87 C-174/15 VOB para 54.

88 Public Lending schemes for printed books exist in several Member States countries, including Germany, France, and Italy. See EU Report on PL right (n. 47) p. 7-10. for an updated and international view of countries having established PL schemes, see 'Established Schemes' (*Public Lending Right International*) <https://plrinternational.com/established>.

89 Ibid para 39-40.

90 The Court found that neither the WIPO Treaty nor the agreed statement did preclude the concept of lending to include the lending of intangible (digital) copies. In doing so, it treated the lending right as independent of the rental right which, on the contrary, under international law cannot be interpreted as extending to digital copies (WIPO Treaty art 7 and agreed statement). See C-174/15 VOB para 31-39.

91 C-174/15 VOB para 45.

92 Ibid para 51.

93 Ibid.

42 The reasoning of the Court is not free from criticism. Contrary to the account provided in the judgment,[94] the Proposal was quite explicit in its desire to exclude all forms of immaterial exploitation from the scope of the Directive, believing rather that questions 'related to the economic data transmission' should be regulated by a different legislative framework to ensure consistency (see InfoSoc).[95] While the CJEU correctly states that the 'explanatory memorandum finds no direct expression in the actual text of the proposal',[96] the Court fails to recognise that: 1) eLending had been harmonised by Art 3 InfoSoc, providing 'authors with the exclusive right to authorise or prohibit any communication to the public of their works'; and – as previously shown - 2) the common understanding, shared by the Commission, Member States, and the academic literature, that the extension of the PL right regime to eLending would require a legislative intervention.

43 By not acknowledging how the eLending of books is, even before the CJEU's intervention, an act fully governed by copyright (under InfoSoc), the Court was able to claim that excluding 'eLending entirely from the scope of Directive 2006/115 would run counter to the general principle requiring a high level of protection for authors'.[97] *Ex contrario*, the non-extension of the PL right to eLending did not leave an unregulated legal void. Rather, had the authors' PL right not been recognised to extend to eLending, they would simply have exercised control on eLending via the very expansive CP right.[98] At least, this was how eLending operated – and still operates – in practice. eLending in public libraries is built on licensing agreements with publishers – exercising the rights conferred by copyright law – and with commercial digital platforms – granting licences to allow library's members to access eBooks for a limited period of time.[99]

44 The judgment then moves on to provide further guidance on how a PL right for eLending may be implemented in national law. Member States have the option of setting additional conditions to PL right beyond the minimum threshold of protection for authors envisaged by the Directive.[100] For example, national legislation could incorporate the requirement of consent of authors in order to reduce the risk of prejudicing 'the legitimate interests of authors'.[101] Beyond the specificities of the referred question, this implies an obligation on Member States to consider how the PL right may affect the interests of authors and to minimise any prejudice thereof.[102] It follows from this – inter alia – that the application of the PL right exception is precluded when *a digital copy of a book* has been obtained from an unlawful source.[103]

45 Two important observations are drawn. First, a specific assessment is called for to determine how a national ePL right scheme specifically affects the legitimate interests of the authors.[104] This determination will be particularly challenging for Member States: while eLending and lending may be objectively considered functional equivalents,[105] it is a much more complex question to ask in what different ways they affect the interests at stake.[106] It also remains unclear to what extent and how the interests of authors should be balanced with the interests of libraries – and the public, by extension – for example by ensuring that the substance of eLending is not eroded by overriding contractual terms,[107] by adding unnecessary frictions or compromising the privacy of libraries' digital users.

46 Secondly, a condition of obtaining a copy from a lawful source effectively ensures that eLending remains largely regulated by the CP right, and subject exclusively to the exceptions and limitations in InfoSoc. This is a point of significant importance, and it will be fully explored later.[108]

94 C-174/15 VOB para 41-42.

95 Lending Right Directive Proposal p. 34-35.

96 C-174/15 VOB para 43.

97 Ibid para 46.

98 See C-466/12 Svensson and Others (CJEU) EU:C:2014:76, para 32; C-351/12 OSA (CJEU) EU:C:2014:110, para 41. See more generally Péter Mezei, 'Enter the matrix: the effects of the CJEU's case law on linking and beyond' (2016) 10 JIPLP 778.; J p. Quintais, 'Untangling the hyperlinking web: In search of the online right of communication to the public' (2018) 21/5-6 J. World Intellect. Prop. 385.

99 Dusollier (n. 14) para 22.

100 Ibid para 51.

101 Ibid para 63.

102 Ibid para 61-64

103 Ibid para 66-72.

104 It remains unestablished to what extent account should also be taken of the interests of other parties in the eLending market – most notably, the interests of publishers.

105 AG Opinion C-174/15 VOB (n. 8) para 30-31.

106 Chris Reed, 'Online and offline equivalence: Aspiration and achievement' (2010) 18/3 Int. J. Law Inf. Technol. 248, p. 260-261; AG Opinion C-174/15 VOB (n. 8) para 73.

107 Linklater-Sahm (n. 86) p. 1567.

108 Discussed later in section 3(d) – 'Communication to the public or lending right - lex specialis to the rescue?'

III. ePL right after C-263/18 Tom Kabinet – a timeline of the rise and fall of a Public Lending Right for eLending

47 While in some respects lending and eLending may be considered functionally equivalent, they are not legally equivalent. The regulation of the material exploitation of copyright enjoys a conceptual and analytical coherence that finds little correspondence in its digital counterpart. In other words, the distribution and use of physical and digital copies are treated very differently by the law, as the distinction between the right of distribution (physical works) and CP right (digital works) well exemplifies. The exclusive rights afforded by copyright are particularly far-reaching in the digital world; while historically the use of a work (e.g., reading) and specific acts of distribution (e.g., private lending) were considered as prerogatives of users and direct expression of their ownership over these works, and therefore unregulated by copyright, the digital transition significantly alters the legal analysis and results in a more extensive control of users' relationships with the literary works they consume.[109] This control is exacerbated by the use of private law instruments such as contracts to further erode the liberties of users and their conception of digital ownership.[110]

48 In the context of physical copies, copyright distinctly regulates different uses of a work. Rightsholders have the right to control the (first) sale of a book under the public distribution right,[111] as long as it takes place within the EU. Ignoring for present purposes the expansive interpretation of the concept of distribution by the CJEU, the kernel of this right could be considered to be the transfer of ownership of the physical copy.[112] Regardless of exhaustion, the owner of a book does not need the rightsholder's permission to lend a copy of that book. In fact, it should be noted how the lending right discussed in this paper only refers to the making available through '*establishments accessible to the public*'.[113] The exhaustion of the distribution right and the liberty to lend books have positive effects on the dissemination of books.

49 The rental of the same book, on the other hand, would require the author's permission, even in those circumstances when the distribution right has been exhausted by a first transfer of ownership of the physical copy of the book.[114] There is, in other words, no exhaustion for the right to rent a book.

50 Both rental and lending exclusively refer to a temporary use of the work – namely, access is provided to the copy only for 'a limited period of time'.[115] This limited temporal dimension constitutes an important distinction with the distribution right, thus ensuring there is no possible overlap between distinct rights and legal regimes. The two regimes coexist without interfering with each other. This is summarised in the below table.

109 G Greenleaf and D Lindsay, *Public Rights: Copyright's Public Domains* (Cambridge University Press 2018) p. 280. See also Jessica Litman, 'The Exclusive Right to Read' (1994) 13 Cardozo Arts & Ent LJ 29; and Martin Kretschmer 'Digital Copyright: The End of an Era' (2003) 25/8 EIPR 333, p. 340.

110 A Perzanowski and J Schultz, The End of Ownership: Personal Property in the Digital Economy (MIT Press 2017).

111 Art 4(2) InfoSoc.

112 C-456/06 Peek & Cloppenburg (CJEU) ECLI:EU:C:2008:232 para 34- 36; although see the wide interpretation of 'transfer of ownership' in C-5/11 Donner (CJEU) ECLI:EU:C:2012:370 para 26 as well as in C-516/13 - Dimensione Direct Sales and Labianca (CJEU) ECLI:EU:C:2015:315 para 33; and C-572/17 Syed (CJEU) ECLI:EU:C:2018:1033 para 25-33.

113 Lending Right Directive art 2(1)(b).

114 Lending Right Directive art 1(2).

115 Lending Right Directive art 2(1)(b).

51 As mentioned, the legal treatment of 'functional equivalent' uses of physical and digital copies of book differs significantly.[116] A first question which arises is whether a digital copy of a book can be sold or whether ownership can be transferred. This point has only recently been adjudicated by the CJEU in C-263/18 Tom Kabinet.[117] Rather than speaking of 'sale of an eBook', the Court characterises this act as 'the supply to the public by downloading, for permanent use, of an e-book'.[118] Such acts would be covered by the CP right, more specifically the 'making available to the public right'.[119]

52 Prior to the Court's decision, some specific forms of permanent access to an eBook were considered by several scholars to be better conceptualised as a distribution to the public,[120] mostly drawing analogies to the recognition of *de facto* transfer of ownership in contracts for the licensing of software sanctioned by CJEU in C-128/11 UsedSoft.[121]

53 On the other hand, before C-174/15 VOB eLending was regulated by the CP right, regardless of whether such lending was carried out through publicly accessible establishments or by private parties. Similarly, the rental of a digital copy of a book was also covered by the CP right, not the rental right.[122] In other words, InfoSoc was the sole instrument regulating immaterial forms of exploitation.[123] Prior to C-174/15 VOB, the situation could be thus summarised as follows:

Table summarising how different acts are construed by InfoSoc and Lending Right Directive

	Making available for use for limited period physical copies of a book (via public establishment)	**Transfer of ownership in physical copies of a book**
Non-commercial	Lending	Private use/Distribution (e.g., donation)[116]
Commercial	Rental	Distribution

54 The conceptual clarity of this *summa divisio* was altered by the extension of the PL right to eLending. In this discussion, it should be made clear that by eLending we exclusively mean 'the lending (making available for a limited time without any commercial/economic advantage by public establishment) of a digital copy of a book'. Accepting this premise, it should be already clear that C-174/15 VOB did not establish an eLending right; more correctly, it only recognised the extension of the PL right to eLending whenever the functional equivalence of the lending of digital and printed books is preserved. We will henceforth refer to this newly recognised right as 'ePL right'.

55 According to the Court, this functional equivalence is present when four conditions are met:

- a digital copy is placed on the server of a public library;
- the digital copy is then downloaded to a new computer;
- only one copy can be downloaded during the lending period (One-copy/One-user model, ensuring no multiplication of copies);
- the copy can no longer be used after the period expires.

56 The clarification on the further conditions that Member States may add in implementing the PL right exception are not relevant for the assessment of the scope of PL right in Art 1(1) of the Lending Right Directive and can therefore be ignored for present purposes. Our focus is on the following question: what is the scope of the PL right, as interpreted by the CJEU in C-174/15 VOB?

57 The Court held that 'it cannot therefore be ruled out that … [the lending right] may apply where the operation carried out by a publicly accessible library … has essentially similar characteristics to

116 While recognising the legal uncertainty that surrounded the legal interpretation of the sale of eBooks, as well as the developing jurisprudence of the CJEU expansively interpreting the right of communication to the public, in the following analysis we will take into account the CJEU's clarification of the rights conferred by the InfoSoc

117 C-263/18 Tom Kabinet (n. 24).

118 Ibid para 72.

119 Ibid.

120 Péter Mezei, 'Digital First Sale Doctrine Ante Portas: Exhaustion in the Online Environment' (2015) 6 J Intell Prop Info Tech & Elec Com L 23; Sganga (n. 3).

121 C-128/11 UsedSoft (CJEU) ECLI:EU:C:2012:407 para 45-46.

122 Rental right cannot be extended to immaterial forms of exploitation due to how such a right is interpreted in international law – see WIPO Copyright treaty art 7, which refer 'exclusively to fixed copies that can be put into circulation as tangible [physical] objects', stated in C-174/15 VOB para 31-35. This interpretation has been criticised in Linklater-Sahm (n. 86) p. 1564.

123 See InfoSoc Recital 20: 'This Directive is based on principles and rules already laid down in the Directives currently in force in this area … and it develops those principles and rules and places them in the context of the information society'. For further development of this argument in the context of C-174/15 VOB, see Catherine White, 'Backlash over CJEU's "dangerous" eLending decision', (2017) Intellectual Property Magazine 14.

the lending of printed works'.[124] The characteristics to which the Court is referring here are: 1) the constant ratio between acquired copies and lent copies – whether physical or digital, and 2) the ability to ensure that access to the copy remains limited in time.

58 Despite Courts treating these two conditions as distinct, they arguably refer to one property shared by the lending of both physical and digital copies: the non-multiplication of usable copies. When lending books, there is no reproduction and no multiplication of the book itself. With ePL right, on the other hand, there is a reproduction but there is no multiplication of usable copies.[125] Therefore, it is submitted that as long as there is no simultaneous 'multiplication of usable copies', the lending right should cover all forms of eLending.

59 The condition of 'limitation in time' of lending is not intrinsically connected with the notion of functional equivalence nor with the property of physical and digital copies; rather, it is just a condition for lending, as important as all other conditions (e.g., 'no economic advantage' etc.). It follows directly from the non-multiplication of usable copies that, after the lending period expires, such a copy can no longer be used. Focusing on the concept of ''non-multiplication of usable copies'' also explains why eLending has generally not been considered to fall within the PL right: in the words of AG, only recent advancements in technological protection measures have ensured that risks associated with eLending are 'substantially reduced'.[126]

60 Part of the difficulty in extracting broader principles from the CJEU's judgment is that the discussion of the PL right, and the corresponding PL right exception, is intrinsically connected: by giving a more expansive interpretation to the lending right, the Court sets the ground for the implementation of the PL right exception, transforming thus a right to control (CP right) into a remuneration right (under an ePL right scheme). To some extent, this directly results from the nature of the PL right which, as discussed, has always been considered to coexist and be justified by the possibility of Member States to derogate in pursuit of their cultural policy.

61 The cogency of the conclusions of the Court may also be criticised for effacing the significantly different characteristics between lending and eLending. For example, it is accepted that digital copies do not deteriorate as physical books; it is therefore possible to lend a copy for an infinite amount of time without any form of deterioration. Another example is the lower transaction costs involved in eLending – eBooks can be read directly from home and can better be adapted to the specific preferences of the reader (e.g., font size can be increased), not to mention the additional potential functionalities offered by eBooks.

62 From this perspective, it could be claimed that the ePL right is functionally but not technically equivalent to the lending of printed books.[127] Notwithstanding these considerations, it would be quite undesirable to adjust and redefine the scope of protection of the PL right based on whether the degree of functional equivalence is met. A better approach would be either 1) to recognise the unique features of eLending and regulate it as such, or 2) to identify the essence of the equivalence of ePL right and lending to clearly define the scope of the right in all circumstances.

63 The condition of 'non-multiplication of usable copies' could serve exactly that purpose, thus instilling a sufficient degree of legal certainty in the scope of the ePL right. This does not mean however that the characteristics of eLending (e.g., no marginal decrease in the quality of the copy) should be completely ignored. On the contrary, as demonstrated by the reasoning of the Court, these are important considerations for Member States when implementing a PL right exception, assessing how best to safeguard the legitimate interests of authors. The table below summaries the legal taxonomy of eLending after C-174/15 VOB. The conceptual and practical issues raised by the judgment are discussed in the sections to co

Table summarising how different acts are construed by InfoSoc and Lending Right Directive before C-174/15 VOB

	Supply to the public by downloading of copy of book, for temporary use (acts carried out by 'public establishment')	**Supply to the public by downloading of copy of book, for permanent use** ('public establishment')
Non-commercial	CP right	CP right
Commercial	CP right	CP right

124 C-174/15 VOB para 51.

125 While there is no multiplication of *usable copies,* there is a reproduction of copies in so far as two copies exist: one on the library's server and one on the reader's server.

126 AG Szpunar's Opinion in C-263/18 Tom Kabinet ('AG Opinion C-263/18 Tom Kabinet') ECLI:EU:C:2019:697, para 73.

127 Matulionyte (n. 85) p. 273.

Table summarising how different acts are construed by InfoSoc and Lending Right Directive after C-174/15 VOB

Functional equivalent of....	Making available for limited time		Making available for unlimited time	
	Physical	Digital copy	Physical	Digital copy
Non-commercial	Lending[129]	ePL right and CP right	Private use/Distribution	CP right
Commercial	Rental	CP right	Distribution	CP right

IV. Communication to the public or lending right - lex specialis to the rescue?

64 As clear from the above table, there seems to be a degree of overlap between the CP right and the ePL right. C-174/15 VOB left the conceptual boundaries of this right undefined. Due to divergence in the set of exceptions and limitations applicable to CP right and ePL right, this overlap risk rendering any ePL right scheme ineffective in practice. In fact, no corresponding exception in InfoSoc enables public libraries to offer digital access to eBooks to the public. This conflict is acknowledged in the AG Opinion to C-174/15 VOB.[128] The AG maintains that the Lending Right Directive, in so far as it codifies the earlier 1992 Directive, constitutes a *lex specialis* vis-à-vis InfoSoc – a conclusion reinforced by Recital 20 and Art 1(2)(b) InfoSoc. In essence, this means that, similarly to what the CJEU held in C-128/11 UsedSoft,[129] the later directive 'in no way affects provisions of EU law *already in force*'.[130] A contrary interpretation would render the PL right exception impossible to implement – unless new exceptions are introduced to the CP right.

65 The argument is sound: the exercise of the CP right is pre-empted whenever an act falls within the scope of the PL right. A few difficulties nevertheless remain. First, it is legitimate to question the extent to which the eLending right was *already in force* at the time of the enactment of InfoSoc. The expansive interpretation of the lending right was achieved through what the AG defined as a 'dynamic or evolving' interpretation – thus considering the developments in technology, markets, and behaviour.[131] Such an approach is explicitly supported by Recital 4 Lending Right Directive, which affirms that copyright protection 'must adapt to new economic developments such as new forms of exploitation'.[132]

66 Despite never acknowledging so in the judgment, it is difficult to maintain that ePL right was not covered by the CP right; the Court in C-174/15 VOB can be assumed to be aware of this. From this perspective, it thus appears that the CJEU was not merely extending the scope of the right to cover a new form of exploitation; on the contrary, it removed acts that had hitherto been considered to fall within the scope of the CP right, and declared that from now on those specific acts should be regulated by the eLending right. For this reason, the doctrine of *lex specialis* cannot be used to interpret the scope of the PL right.

67 The entry into force of InfoSoc did not cause 'prejudice to the provisions' of the Lending Right Directive by introducing a CP right.[133] On the contrary, the expansive interpretation of the PL right proactively created such conflict, despite that InfoSoc was considered to extend the principles of the Lending Right Directive and develop them 'in the context of the information society'[134] – InfoSoc specifically addresses the issues of digital uses of works left open by the Lending Directive.

68 Moreover, the reliance in C-174/15 VOB on the arguments elaborated in C-128/11 UsedSoft[135] conceals important differences between these judgments. In C-128/11 UsedSoft, the CJEU invokes the *lex specialis* principle merely to assert that even if 'the contractual relationship at issue (...) or an aspect of it might also be covered by the concept of 'communication to the public' the principle of exhaustion of the distribution right of that copy still subsists' – not to the exclusion of the CP right, rather in addition to it.[136]

69 In that case, the potential conflict between these two rights was resolved on the interpretative level, not by applying the *lex specialis* doctrine: the CJEU, relying on the analysis of the AG, argued that the wording of Art 6(1) of the WIPO Copyright Treaty ('WCT')[137] is 'unequivocal' and 'the existence of a transfer of ownership clearly changes a mere act of communication to the public into an act of distribution'.[138] Drawing a comparison with C-174/15 VOB, it is far from 'unequivocal' that the PL right covers acts of eLending – even when conceding that such a right may retain a *lex specialis* priority. On the contrary, a literal interpretation of both Art 8

128 AG Opinion C-174/15 VOB (n. 8) .
129 C-128/11 UsedSoft (CJEU) ECLI:EU:C:2012:407.
130 Ibid para 55.
131 AG Opinion C-174/15 VOB (n. 8) para 28.
132 Lending Right Directive Recital 4.
133 InfoSoc Recital 20.
134 Ibid.
135 C-128/11 UsedSoft.
136 Ibid para 51.
137 WIPO Copyright Treaty, 1996.
138 AG Opinion C-128/11 UsedSoft, para 73; C-128/11 UsedSoft para 52.

WCT[139] and InfoSoc seems to unequivocally point to the fact that eLending is to be considered an act of communication.

70 After C-174/15 VOB, this conflict remains mostly unresolved, especially as the ePL right constitutes a test of the limits of the CJEU's judicial discretion in the creation of new rights. Regardless of how this matter will be determined, it is argued that without any form of digital exhaustion a PL right exception is an impossible proposition in practice. This controversial argument will be explored in the next section.

D. eLending without digital ownership – a legal Chimera?

71 In C-174/15 VOB, the CJEU held that an eBook cannot be made available under the PL right exception unless that 'copy was obtained from a lawful source'.[140] Again, this proposition is justified by the duty of Member States not to 'unreasonably prejudice copyrightholders'.[141] This conclusion was reached rather summarily. The public nature of the establishments to which such derogation is addressed – libraries – 'may legitimately be expected' to respect the law.[142] While it is difficult to disagree with this point, its consequences were difficult to gauge at the time; in fact, the CJEU may have reasonably assumed that libraries had multiple options for lawfully sourcing digital copies of books. For example, by digitising part of their collection or introducing a form of digital exhaustion, thus creating a secondary market for digital copies of books. In the following sections, options available to libraries will be assessed to determine their compatibility with EU law.

I. Could libraries digitise literary works in their collections under Art 5(2)(c) Info Soc?

72 A first option is for libraries to digitise a book in their collection, an act that would normally require the permission of the rightsholders. The AG in C-174/15 VOB maintained that libraries have a right to digitise their physical collection by relying on the reproduction exception in Art 5(2)(c) InfoSoc, as long as such reproduction is carried out for the purpose of offering an eLending service.[143] The application of this exception in this scenario is not uncontroversial, and its application needs to be further qualified.

73 First, the wording of Art 5(2)(c) states that this exception applies only 'in respect of specific acts of reproduction'. In interpreting this 'condition of specificity', the CJEU clarified that 'as a general rule, the establishments in question may not digitise their entire collections'.[144] This is a considerable limitation, at least in so far as it limits the potential impact of this exception in allowing libraries to build a substantial collection of digitised resources independently from agreements with rightsholders.

74 At the same time, considering that library's users are likely to be interested in only a portion of the catalogue of libraries – typically only the most recent/famous titles – a mass-digitisation of the collection may be desirable but not necessary. While it is clear that mass-digitisation projects cannot be carried out on the basis of this exception, the term 'specific acts of reproduction' does not prescribe any threshold beyond which the exception can no longer be used. A more careful look at the jurisprudence of the CJEU, therefore, is needed to shed more clarity on the extent to which libraries can rely on the exception to carry out their digitisation strategy.

75 The essential question to ask is whether the specific purpose to be pursued justifies the digitisation of the *individual* work, requiring thus an *individual* assessment of the necessity of its digitisation;[145] it is not possible to treat automatically the whole collection as fulfilling the condition of specificity. However, it is also important to state that the judgment does not rule out *a priori* such a possibility, as long as such an individual assessment is carried out. Yet, admittedly, it is unlikely or exceptional for the condition of 'necessity for a specific purpose' to be met for the whole collection.[146]

76 A few examples can be found when specific acts of digitisation may be justified. The AG's Opinion in C-117/13 Ulmer refers to instances when a digital copy of the work does not yet exist[147] – a proposition that forces us to consider whether the possibility of licensing the use of an already

139 See WIPO Copyright Treaty Art 8.

140 C-174/15 VOB para 72.

141 C-435/12 ACI Adam and Others (CJEU) EU:C:2014:254, para 31, 35, 40.

142 AG Opinion C-174/15 VOB (n. 8) para 88.

143 Ibid para 57.

144 C-117/13 Eugen Ulmer (CJEU) ECLI:EU:C:2014:2196 para 45.

145 AG Opinion in C-117/13 Ulmer para 38.

146 See C-117/13 Ulmer para 46: 'the digitisation of some of the works of a collection is *necessary for the purpose ... of research or private study*'.

147 AG Opinion C-117/13 Ulmer para 37. In the same paragraph, the AG provides a further example: when the printed version would otherwise be subject to disproportionate wear due to repetitive use.

digitised copy may render reliance on the exception unjustified.[148] Dealing with a similar question, the Commission hinted that this condition may be met if the digitisation is 'necessary for the preservation of works contained in the libraries' catalogue'.[149] These examples are illustrative, yet they should not be considered to remove all the uncertainty over the application of the 'condition of specificity'.

77 Not only does the limited scope of the exception raise some concerns; InfoSoc also seems to indicate that the reproduction exception was never intended to apply to acts of digitisation carried out for the purpose of granting digital access. This prospect will be now confronted and discussed.

78 Recital 40 InfoSoc states that while exceptions for libraries for 'certain special cases covered by the reproduction right' should be provided for, they should not extend to 'uses made in the context of on-line delivery of protected works or other subject-matter' – a description that seems perfectly to fit eLending.[150] Finally, the Recital concludes by saying that 'specific contracts or licences should be promoted which, without creating imbalances, favour such establishments and the disseminative purposes they serve'.[151] In light of the specific wording of the recital, it is difficult to dismiss the conclusion that InfoSoc explicitly prohibits to rely on an exception to digitise books in the library's collection for the purpose of offering an eLending service. Despite not being legally binding, this Recital may carry significant interpretative weight in case such a question is in the future referred to the CJEU.

79 An alternative interpretation of the Recital however exists. It is possible to read in the inclusion of this Recital simply an intention to specify that the exception contained in Art 5(2)(c) only covers the reproduction right, without extending to the right 'to make available over the Internet the works held by libraries', which is – in some specific circumstances – covered instead by Art 5(3)(n).[152] Although this point cannot be conclusively established, the ambiguity of the Recital may be fertile ground for an expansive interpretation of the provision in order to ensure the effectiveness of the PL right exception.

80 After all, a blanket exclusion of eLending from the purposes of the reproduction right seems unnecessary and unwarranted, especially in those cases when reliance on the exception is necessary to guarantee non-commercial access to copyrighted works and the cultural promotion objectives enshrined in Art6(1) of the Lending Right Directive.

81 In light of this, it is useful to speculate about circumstances when such a digitisation may be permissible and sufficiently specific, and how it may contribute to relieving the pressure off libraries. Assuming that an ePL right scheme for eLending exists, Member States may provide for a digitisation exception under Art 5(2)(c) InfoSoc in those cases when the license offered for the supply of the digital copy of the file is unfair or the price is excessive, provided these concepts are operationalised ex ante to ensure a sufficient level of legal certainty. Such legislation would incentivise publishers to better balance the interests of all parties in determining the terms and conditions of the license, as well as to digitise their own catalogue to pre-empt acts of external digitisation by public institutions.

82 Going back to C-117/13 Ulmer, the assessment of the 3-step test under Art 5(5) encourages the idea that such conditions are likely to be met. In fact, the CJEU states that such acts of reproductions do

148 In this respect, it is submitted that the CJEU in C-117/13 Ulmer ruled that the concept of 'purchase or licensing terms' in Art 5(c)(n) InfoSoc does not extend to the 'mere offering to conclude a licensing agreement' is immaterial to the interpretation of the question at hand. The reason to exclude 'works … subject to purchase or licensing terms which are contained in their collections' is likely to be to avoid the sanctioning by national legislation of infringement of existing contracts. For example, this means that in those cases when libraries have obtained access to a digital copy of a book under a licensing agreement, the exception in question should not be used to override the license. Art 5(2)(c) does not include any wording to such effect and the context of the exception is different. For this reason, the possibility to obtain access to a digital copy under a license could be consistently considered as sufficient for disapplying the exception to the reproduction right.

149 Commission, 'Report on the harmonisation of certain aspects of copyright and related rights in the information society' (Commission Staff Working Paper, 2007) SEC (2007) 1556, p. 5.

150 Admittedly, this phrase is then followed by claim that this 'should be without prejudice to the Member States' option to derogate from the exclusive public lending right'. However, the *Travaux* reveal that the inclusion of that specification only reflects the understanding of the drafters that – in descriptive terms – this limitation does not 'of course' causes prejudice to the PL right Exception. The Recital is almost reproduced *verbatim* in the Travaux (n. 68) p. 32. See also ibid p. 31: 'This exception does not apply to the communication to the public right. In view of the economic impact at stake, a statutory exemption for such uses would not be justified … the making available of a work or other subject matter by a library or an equivalent institution from a server to users on-line *should and would require a licence* of the rightholder or his intermediary *and would not fall within a permitted exception*'.

151 InfoSoc Recital 40.

152 Support for this interpretation comes from the Commission Staff Working Paper (n. 151), p. 5.

not prejudice the normal exploitation of the work or cause unjustified harm to their legitimate interests in so far as 1) the ratio between the analogue and digital copy of the book remains constant – again, giving due weight to the property of non-multiplication, and 2) an obligation to adequate remuneration for the further use of the work enabled by the digitisation.[153] Both conditions seem to comply with how an ePL right scheme reflecting the conditions of ePL right will work in practice.

83 While the prospect of the introduction of such a measure surely is cause for hope for many libraries in Europe, its implementation depends on the political goodwill at the national level. The authors are not aware of any such legislation having been yet proposed – whether due to lack of willingness or awareness, it is hard to judge.

II. Recognising digital exhaustion to increase competition in the market for digital copies of books

84 In the present system, the requirement of 'lawful source' is automatically translated into an obligation to license the supply of the digital copy; no exception in fact exists to cover the necessary digitisation to render the source lawful. In other words, Member States are mandated to introduce a requirement which – regardless of how it is formulated – 'is likely to restrict the scope of the derogation'.[154] This creates an internal conflict between the principle of effectiveness and the need to safeguard the legitimate interests of rightsholders.

85 It is argued that this is the major limitation of the C-174/15 VOB judgment, rendering an effective PL right system for eLending a legal chimera. In practice, eLending will therefore continue to be based on the licensing mechanisms that characterise the current eLending market, frustrating what the AG saw as a solution to liberate the lending of electronic books from 'the laws of the market' and allowing libraries to benefit, in the digital environment, from 'the same favourable conditions' enjoyed for the lending of physical books.[155] Yet the judgment of the CJEU in the C-174/15 VOB case was difficult to predict and, when reading through the arguments of the Court, it is reasonable to assume that the CJEU considered exhaustion to provide a third possible lawful source of digital copies of eBook, on which libraries could rely on to build an eLending service.[156]

86 A recognition of digital exhaustion, as well as a notion of digital ownership on which such a concept must necessarily be based, would be therefore instrumental in increasing competition for the supply of digital copies, and reduce the undue influence of publishers of libraries eLending practice. In addition, digital exhaustion does not seem necessary in antithesis with the author's interests, at least not more detrimental than the doctrine of exhaustion with regard to printed copies. As clear from the analysis so far, the legitimate interests of authors may be respected by the ability to control the multiplication of copies offered by technology, an attribute on which the CJEU has relied to provide an expansive interpretation of exception in both C-117/13 Ulmer and C-174/15 VOB. In light of the issues, in the eLending market, it is worth discussing future potential developments on digital exhaustion. From a copyright perspective, this seems one of the only solutions currently available to solve some of the issues identified in the eLending market.

1. The role of exhaustion in the C-174/15 VOB case – a difficult balance that can no longer be avoided

87 In the EU, most eBooks are provided as a service on the basis of the licensed access model, often within closed ecosystems (e.g., Kindle books). It is an open question whether it is legally possible to transfer or claim ownership of an eBook; so far, it appears that publishers do not consider this a suitable business model. Reflections on digital ownership now need to confront C-263/18 Tom Kabinet, where the CJEU said that 'the supply to the public by downloading, for permanent use, of an e-book',[157] cannot be characterised as a distribution to the public but an act of communication, covered by the CP right. An important consequence is that each supply of the digital copy of the book will give rise to an independent new act of communication, requiring permission from the owner. There is therefore no 'digital exhaustion'.

153 In the case at hand, this use consisted in the subsequent making available of that work in digital format, on dedicated terminals, gives rise to a duty to make payment of adequate remuneration. See C-117/13 Ulmer para 48.

154 AG Opinion C-174/15 VOB (n. 8) para 88.

155 Ibid para 79.

156 Later AG Szpunar in his Opinion to C-263/18 Tom Kabinet considered the effects of the judgment in C-174/15 VOB, adding that the 'Court seems to have accepted the exhaustion of the distribution right as regard eBooks', and if 'the Court were to rule, in the present case, that the distribution right does not apply to the supply of works by downloading, that condition [of exhaustion of the distribution right in the digital copy, which the Court accepted as lawful] would be rendered meaningless'. AG Opinion C-263/18 Tom Kabinet (n. 127) 697, para 72.

157 Ibid para 72.

88 Without digital ownership, copyright law shifts the focus from digital content to digital access, relegating the eBook market to a market for the provision of a service.[158] This however does not directly follow from a literal interpretation of InfoSoc. As stated by Recital 29 InfoSoc, rental and lending of copies of work are 'services by nature', independently of whether such copies are physical or digital.[159] The fact that lending is treated as a service, does not affect the possibility that the sale of an eBook may be construed as the sale of a 'digital good', thus covered by the right of distribution. Vice versa, 'the lending right is completely independent of the exhaustion of the distribution right'.[160] This is probably why the CJEU in C-174/15 VOB never dealt with the complex issue of digital exhaustion and the scope of the distribution right.

89 Reading the AG's Opinion, it is apparent that exhaustion only creeps in when discussing the importance of the consent of the author as a mechanism to safeguard his legitimate interests.[161] This led the CJEU to conclude that Member States may include a condition that the 'digital copy of a book (...) must have been put into circulation by a first sale'[162] – a proposition which, after the judgment in C-263/18 Tom Kabinet, has become plainly legally incorrect or 'meaningless'.[163] Alternatively, despite the exercise of self-restraint in its answers, and its paucity, we could read into the judgment an assumption operating underneath the surface of the explicit text: the possibility for libraries to obtain digital ownership in copies.[164]

90 Whether we interpret the judgment as not tackling the question or implicitly supporting exhaustion, we are confronted with the same quandary: how does C-263/18 Tom Kabinet affect the assessment carried out by the CJEU in C-174/15 VOB? Specifically, would a condition that a copy is obtained from a lawful source still be justified in a world without exhaustion? How do we balance the principle of effectiveness of the PL right Exception and the legitimate interests of rightsholders 'not to tolerate infringements of their rights'? The CJEU stated that the requirement of lawful source follows from one of the objectives of the Directive, namely, to combat piracy.

91 Without exhaustion, another objective of the Lending Right Directive – the promotion of access to knowledge – is under threat. Member States lack the means to resolve this conflict; the EU copyright acquis now significantly limits how copyright-relevant acts are to be construed under national law. Despite that no stare decisis rule strictly binds the EU judiciary, the breadth and contested nature of the questions at hand makes the CJEU unfit to solve this impasse. With no prospect of legislative reform in sight, we will nonetheless consider the status of exhaustion in EU law, and what arguments may be available to the CJEU to open up lawful sources of access to digital copies of eBook.

2. The future of digital exhaustion in the case law

92 It is not altogether clear how the concept of sale and ownership can be translated in the digital world, partly due to the ease with which data can be duplicated at no marginal cost. Albeit data can be easily reproduced, it does not necessarily mean that we lack the means to exercise control. In fact, it is arguable that in the digital environment rightsholders have more far-reaching means to control uses of digital content. Lack of digital ownership does not stem from our inability to control data; on the contrary, it is premised on the considerable capabilities of digital technologies to enable the exercise of control.[165] Physical copies can be owned *by default;*[166] digital copies cannot be owned *by design*.

93 Several options are open to publishers desiring to market eBooks, allowing them to choose if and on how many devices it can be downloaded, its functionalities (e.g., ability to write notes on it,

158 Kevin Dong, 'Developing a Digital Property Law Regime' (2020) 105 Cornell L Rev 1745, 1764-1766.

159 The Recital exclusively refers to a 'material copy of a work'; this point becomes obvious once it is recognised that, at the time of enactment of the Directive, the concept of lending covered only physical copies of a work. The inclusion of digital copies under the lending right does not alter the legal analysis.

160 AG Opinion C-174/15 VOB (n. 8) para 83.

161 AG Opinion C-174/15 VOB (n. 8) para 81-88.

162 C-174/15 VOB para 62.

163 AG Opinion C-263/18 Tom Kabinet (n. 127) para 72.

164 AG Szpunar is more explicit in considering the issue of digital exhaustion, hinting to the fact that 'a simple solution to the problem' does not exist (see AG Opinion C-174/15 VOB para 52). However, he fails to recognise the importance of digital exhaustion for libraries in creating alternative lawful sources of access to digital copies of books.

165 Both the judges and AG in C-263/18 Tom Kabinet exclusively focus on the opposite narrative, namely that distribution of digital copies carries an inherent risk of uncontrolled multiplication of perfectly substitutable copies. See AG Opinion C-263/18 Tom Kabinet (n. 127), para 91-92, a reading supported by the Court at para 57-58 of their judgment.

166 In other words, often ownership is not a choice and cannot be designed. After transfer of a physical copies, the original owner retains little actual control over further uses of such copies; potential control is exercised through personal (contract) and quasi-property rights (intellectual property).

highlighting, searching functions etc); it is difficult to imagine any limits that cannot be imposed on the user's ability to use an eBook. Digital ownership therefore reflects the rights of the user, and its terms and conditions are dictated by a licensing agreement.[167] Once a certain threshold of rights and liberties is reached, then a substantive notion of digital ownership can emerge and be recognised by the law.[168] This process is well-illustrated by recent examples of recognition of digital ownership in computer programs,[169] and videogames.[170]Given its intrinsic link with consumer rights, it is unsurprising that consumer protection legislation appears often more advanced and sophisticated in dealing with this question than, for example, copyright law.[171]

94 Despite being a pressing issue, it is not the purpose of this section to reflect on whether digital exhaustion should be introduced in the EU copyright framework. Here digital exhaustion is discussed considering the specific issues faced by libraries: there is currently no mechanism for libraries to obtain a copy of a book from a lawful source which guarantees sufficient independence from publishers. Without such a mechanism, it is argued that eLending remains subject to 'the laws of the market'. This status quo is unlikely to be an issue Courts alone can help solve. As also recognised by AG Szpunar, some of the arguments made refer to 'general economic policy',[172] and it would be unfitting for the CJEU to be led in its adjudication by such considerations.[173]

95 On the other hand, legislators are not so constrained. Yet lack of legislative intervention may force Courts to adopt a more dynamic interpretation and proactively extend the scope of the existing legal provisions if such an outcome is warranted by the specific factual situation of the case – following its own precedent in the VOB case. The following analysis will be divided into two sections. First, we will consider the limits of digital exhaustion under the current legal regime; in the second part, the limits of the judgment will also be acknowledged to assess what is the possible future of digital exhaustion.

3. Limits to digital exhaustion

96 It is difficult to overstate the importance of the WCT in the interpretation of the rights conferred by InfoSoc, which must be interpreted in compliance with international law. Art 6(1) WCT covers the right to distribute a work to the public. As specified in the Agreed Statements annexed to it, the distribution right refers 'exclusively to fixed copies that can be put into circulation as tangible [physical] objects'.[174] Nevertheless, and as acknowledged by the AG, the WCT establishes a minimum level of protection and does not preclude *per se* the extension of the distribution right to cover the transfer of ownership in a digital copy.[175]

97 However, contradicting his previous statement, the AG then proceeds with stating that substituting the CP right with the distribution right would entail a lower level of protection and thus be inconsistent with its obligations under the WCT. This statement, in so far as it is understood as ruling out future recognition of digital exhaustion, is problematic on two fronts. First, the validity of that proposition depends on the characterisation of 'sale of an eBook' as 'making available to the public'; it does not conclusively mandate the categorisation of all forms of online distribution as 'making available'. Secondly, adopting such an interpretation would

167 Given the connection between ownership and user's rights, it is possible to 'create' a de facto digital exhaustion by granting rights to consumers. In certain instances, refusal to recognise exhaustion may breach consumer protection law or be considered an unfair terms & conditions as in TGI de Paris UFC-Que Choisir vs Valve (2019) N° RG 16/01008. However, it is unclear whether this judgment should be reinterpreted in light of C-263/18 Tom Kabinet.

168 This is well expressed by AG Szpunar when he says that 'modern technical means allow copyright holders to exercise a very firm control on the use which purchasers make of their works (...) and permit the development of commercial models which, often without openly saying so, transform the full enjoyment of the copy of a work into a mere limited and conditional right to use it'. See AG Opinion C-263/18 Tom Kabinet (n. 127), para 6. In his monograph, Mezei argued that the combination of two technological solutions might guarantee the proper control of the downstream market of used digital files. These are the use of a unique ID number for each lawfully sold file; and, second, the application of a functioning forward-and-delete technology. See Mezei (n. 3) p. 191.

169 C-128/11 Usedsoft.

170 Rogers Communications Inc. v. Society of Composers, Authors and Music Publishers of Canada, 2012 SCC 35, [2012] 2 R.C.S. 283.

171 See, for example, the Consumer rights Directive 2011/83/EU. For a more detailed analysis, see S Ghosh and p. Mezei, 'The Elusive Quest for Digital Exhaustion in the US and the EU-The ruling of the CJEU in Tom Kabinet Ruling a Milestone or Millstone for Legal Evolution?' (2020) 8/1 Hungarian Yearbook of International Law and European Law 249, 256-257. See also Geiregat (n. 3).

172 AG Opinion C-263/18 Tom Kabinet (n. 127) para 85.

173 See also AG Opinion C-263/18 Tom Kabinet (n. 127) para 86, where he says that copyright should not 'serve as a corrective factor of the alleged dysfunctions for the market for the supply of works'.

174 WIPO, 'Agreed statements concerning the WIPO Copyright Treaty' (Geneva, 1996).

175 AG C-263/18 Tom Kabinet para 33-34.

violate the essence of the 'umbrella solution' on which the agreement on the right covering instances of 'making available' was built. The Guidelines, in fact, specify that the 'Contracting Parties are free to implement the obligation to grant an exclusive right to authorize such ''making available to the public'' also through the application of *a right other than the CP right* [...] as long as the acts of such 'making available' are fully covered by an exclusive right (with *appropriate exceptions*)'.[176]

98 The interpretation suggested by the AG would, in practice, mandate signatories to the WCT to protect such acts with a right substantively identical to the CP right, which seems not to be the approach adopted in the Guidelines. This is therefore not a limit to a recognition of digital exhaustion in EU law. Therefore, it is open to legislation to harmonise such a right. Nonetheless, without a legislative intervention, the CJEU is correct in pointing to the unambiguous language of Recital 28, which limits the application of the distribution right to tangible [physical] copies.[177] Despite that the Recitals of InfoSoc contain 'certain ambiguities',[178] Recital 28 directly reproduces and thus incorporates the Agreed Statement; it is possible to extract an intention not to diverge from the minimum interpretation of the right of distribution as contained in the WCT.

99 Another fundamental challenge to digital exhaustion is the technical dependency of the distribution of the digital file to its reproduction; in other words, there is an overlap between the concept of transfer of ownership – distribution – and the downloading that is necessary to transfer the file – the reproduction, that would require the author's permission. There is currently no exception covering the right of reproduction in all circumstances, and the right cannot be exhausted.[179] The problem identified is the result of the extreme level of control that rightsholders can exercise online, which extends over control of the 'use a copy'. For this reason, Art 5(1) of the Software Directive provides for an exception to the right of reproduction of a computer program whenever such reproduction is necessary to 'the use of the computer program by the lawful acquirer in accordance with its intended purpose'.[180]

100 In C-128/11 Usedsoft, this provision was broadly interpreted to ensure the effectiveness of exhaustion of the distribution right.[181] In particular, the CJEU was ready to emphasise the 'invisible link' between the copy and the licensing agreement, and the 'invisible whole' constituted by the act of downloading a copy on the customer's server and the conclusion of the user's license agreement.[182] In contrast, there appears to be no such exception in InfoSoc, possibly further reinforcing the distinction drawn between physical distribution and digital communications to the public. The lack of such a provision will likely significantly hinder the ability of the CJEU to recognise digital exhaustion.

101 Finally, even the extension of the right of distribution to digital copies may not result in libraries obtaining alternative lawful sources of access to eBooks. In fact, we discussed how the classification of a licensing agreement as 'sale' may depend on the terms & conditions of the agreement; since most publishers are likely possess a sufficient degree of bargaining power, it will not be difficult for them to exclusively promote business models whereby users are provided with on-demand access to the eBooks, never upgrading the status of the digital consumer to owner of these items. In practice, this will allow publishers to keep exercising control over acts of communication by strategically defining 'in different ways the modes of use of the copy of the work' to rule out the possibility of distribution of copies.[183] A related point has been made by AG in C-263/18 Tom Kabinet , where the Court emphasised that exhaustion cannot limit 'the scope of freedom of contract',[184] and that such rule may not 'automatically have the consequence of cancelling all the contractual terms governing the use of that copy'.[185]

102 Again, consumer protection seems to have a role to play in ensuring stronger rights for digital consumers, thus indirectly benefiting the emergence of a secondary market for eBooks on which libraries can rely on. Another solution would be to alter the scope of the reproduction right of digital copies to

176 'Guide to the Copyright and Related Rights Treaties Administered by WIPO', (WIPO, 2003), p. 209.

177 C-263/18 Tom Kabinet (n. 24) para 51.

178 AG Opinion C-263/18 Tom Kabinet (n. 127) para 38.

179 Ibid, para 45-49. This point was also raised in the questions of the referring Court. See C-263/18 Tom Kabinet (n. 24) para 30.

180 Directive (EU) 2009/24/EC on the legal protection of computer programs (Software Directive) OJ L 111 art 5(1).

181 C-128/11 UsedSoft para 78-85.

182 C-128/11 UsedSoft para 84.

183 AG C-263/18 Tom Kabinet para 44.

184 Ibid.

185 AG C-263/18 Tom Kabinet para 87; citing as further support for his position: Agnès Lucas-Schloetter, 'La revente d'occasion de fichiers numériques contenant des œuvres protégées par le droit d'auteur', in Bernault et al. (eds), *Mélanges en l'honneur du Professeur André Lucas* (LexisNexis, 2014). This opinion might be not without criticism. The doctrine of exhaustion has historically played a role to limit author's right to control redistributions that take place following the conclusion of the initial contract for the sale of goods. As such, exhaustion worked as a safety valve against extensive contractual stipulations. Compare to Mezei (n. 3) p. 11.

cover only 'multiplication of usable copies'. This remains particularly challenging, despite that some jurisdictions have come close to such an interpretation.[186]

103 Before canvassing a list of concrete policy solutions, the limitations of C-263/18 Tom Kabinet should be highlighted. At the same time, it is also possible that further development in technologies and business models may address remaining concerns over digital exhaustion, altering 'the interests of the rightsholders in obtaining appropriate reward for their works'.[187]

4. Limits to the judgment in C-263/18 Tom Kabinet itself

104 Despite the difficulties outlined above, C-263/18 Tom Kabinet does not conclusively rule out digital exhaustion. On the contrary, it considers the advances that the Court has made in 'recognising the exhaustion of copyright in the digital environment', adjudicating however on the specific facts of the case that the acts in question fall fully under the CP right.[188] In that sense, the judgment has a limited scope of application. For a start, the judgment only deals with the conduct of the platform rather than individual users. Desptie this, the judgment also highlights the limits of the CP right vis-à-vis new forms of one-to-one distribution of digital content - e.g., sale of an eBook.

105 These limitations come to the fore at para 69 of the judgment. In considering whether making an eBook available amounts to a communication directed to ''an indeterminate number of potential recipients' – the public – the Court implicitly accepts the possibility that not all forms of digital distribution – of communication of a work – will necessarily involve the public. Relying on C-174/15 VOB, the Court leaves open the possibility that in some circumstances – namely when, as a result of technological measures ensuring that there is no multiplication of usable copies, the eBook is not made available to a substantial number of people – such an act may fall beyond the scope of the CP right.[189]

106 This raises the question of how we should construe acts of digital distribution when the digital copy is made available to one individual only – thus, not a public. Is this the sign of a black hole in the harmonisation of digital copyright, and would the distribution right occupy that space?

107 The Court is able to sidestep this issue in C-263/18 Tom Kabinet by concluding that, due to the lack of 'technical measures' limiting access to the digital copy, the work should be treated as having been communicated to a sufficiently large amount of persons, especially considering 'how many of them may access it in succession'.[190] Despite this, the limits of the CP right is undoubtedly an issue likely to surface again and may offer to the CJEU to refine the taxonomy of digital copyright protection.

108 Finally, assessing the implications for and possible reinterpretation of C-174/15 VOB in light of the judgment in C-263/18 Tom Kabinet is a difficult task. The *lex specialis* approach harms consistency and coherence, in so far as it prevents a broader conceptualisation of how digital copies are to be regulated by copyright – whether as part of software, eBooks, or any type of literary work.

109 In future judgments, there is arguably a greater scope for the principle of effectiveness to be used as a tool to mitigate the negative effects of the strict interpretation of the law.[191] The principle was used in C-128/11 Usedsoft to give a broad interpretation to the concept of sale in the Software Directive in order to safeguard the effectiveness of the provision against attempts by suppliers 'to circumvent the rule of exhaustion'.[192] In C-174/15 VOB, the AG highlighted the role of effectiveness in ensuring that 'the anachronistic character of obsolete legal rules' remain updated in front of 'rapid technological and economic development';[193] this led ultimately the AG to advise in favour of extending lending right

186 A notable example is Canada. In Théberge v. Galerie d'Art du Petit Champlain Inc., [2002] 2 S.C.R. 336 para 50, the majority held that a multiplication of copies is an essential element of the 'reproduction' right of copyright owners. This is the opposite of the judicial interpretation provided by the U.S. District Court in *ReDigi* - Capitol Records, LLC v. ReDigi Inc., 934 F. Supp. 2d 640 (S.D.N.Y. 2013). For an in-depth analysis, see Ariel Katz, 'Digital exhaustion: North American observations' in John A. Rothchild, *Research Handbook on Electronic Commerce Law* (Edward Elgar, 2016).

187 C-263/18 Tom Kabinet (n. 24) para 58, perfectly reflecting the Opinion of the AG at para 89.

188 AG Opinion VOB para 77.

189 C-263/18 Tom Kabinet (n. 24) para 69. The conditions are the same as in C-174/15 VOB: 1) only one copy of a work may be downloaded in the period during which the user of a work actually has access to the work; 2) after that period has expired, the downloaded copy can no longer be used by that user.

190 C-263/18 Tom Kabinet (n. 24) para 69, applying C-610/15 Stichting Brein (CJEU) EU:C:2017:456 para 41.

191 AG Opinion C-174/15 VOB (n. 8) para 47. See also C 403/08 and C 429/08 Football Association Premier League and Others (CJEU) EU:C:2011:631 para 163, and C201/13 Deckmyn (CJEU) EU:C:2014:2132 para 23.

192 C-128/11 UsedSoft para 44.

193 AG Opinion C-174/15 VOB (n. 8) para 28.

to cover the lending of digital copies, a conclusion supported by the Court.

110 It remains to be seen how this principle will be exploited to secure the ability of Member States to set up an ePL right scheme without the need to resort to commercial licensing with publishers. C-263/18 Tom Kabinet per se does not make digital exhaustion more difficult, as the most important arguments contained in the judgment were already well established in the literature and hinted at by previous Courts. On the contrary, the judgment provides an additional reason to rethink EU copyright approach to digital exhaustion by showing the limits of the CP right. When digital exhaustion and eLending are considered together, the urgency of such a reform is apparent and it is unclear whether Courts can really solve this or if they will merely add to the confusion.

E. Looking forward: avenues to ensure the effectiveness of CJEU's judgement in VOB

111 This paper has reviewed the evolving EU regulatory framework on eLending. It contributes to the existing literature by revealing how, despite the judicial efforts to interpret dynamically the PL right in the Lending Right Directive, an effective PL right exception – allowing libraries to offer eLending independently of the market in functionally equivalent terms as the lending of printed books – is not possible. Member States are prevented from developing ePL right schemes, which would entitle authors to a remuneration right while allowing libraries to carry out acts of eLending without the need for negotiating a license with rightholders (publishers). In other words, eLending is still controlled by the exclusive rights of authors, and any attempt to transform it into a remuneration right is foiled by the extensive control that rightsholders can exercise on digital copies of books under the CP right.

112 This finding calls for a more comprehensive evaluation of how a PL right Exception under Art6(1) Lending Right Directive could be implemented in practice. It would require a reflection on how libraries can get access to digital copies of books, the rights they enjoy over such copies, and the level of control that rightsholders (e.g., publishers) still retain over the provision of eLending services when this is carried out within the scope of a PL right Exception. In very simple terms: the 'right' of libraries to lend eBooks to the public will be completely ineffective unless they can get access to the digital file necessary for such lending. Drawing a parallel with the physical world, it is similar to expecting libraries to offer a lending service without possessing any physical book. Currently, publishers fully control the provision of any eLending service.

113 This situation is unfortunately not the outcome of a well-defined policy; instead, it was brought about by a doctrinal issue at the core of copyright: the conceptualisation of the right to the temporary or permanent transfer of digital copies of works – respectively, eLending and sale of digital content.

114 Despite the efforts of the CJEU in C-174/15 VOB to afford Member States more manovure in defining their national cultural policies by recognising an eLending right (temporary transfer of a digital file), the judgment remains an incomplete revolution. This is not to underestimate its significance, which represents a positive precedent in ensuring that EU legislative instruments retain relevance and cogency in front of new technological developments. Nonetheless, it is apparent how subsequent developments in C-263/18 Tom Kabinet significantly limited the effectiveness of Art 6(1) of the Lending Right Directive. C-174/15 VOB needs to be reconsidered in light of this. In particular, after C-263/18 Tom Kabinet it is difficult to imagine how libraries could get a sufficiently permanent control of digital copies to be able to develop an independent eLending service – to independently and temporarily make a digital copy of a book accessible to the public. While solving these doctrinal issues seems to go beyond the power of the CJEU, less ambitious but effective solutions are possible.

115 The first step is defining the goal that is intended to be achieved. Member States should be able to create ePL right scheme in a way that 'has essentially similar characteristics to the lending of printed works'.[194] This is particularly desirable in light of the important public goals served by eLending, most notably cultural promotion. While various eLending models are currently offered by commercial actors, they may not sufficiently guarantee the (non-market) cultural objectives that eLending promotes. Therefore, measures should be introduced in order to ensure its effectiveness; specifically, 'to safeguard ... the effectiveness of the PL right Exception referred to in Art 6(1)' of the Directive.[195]

116 Considering the non-territorial nature and potential for cross-border use of digital content, a more convincing solution would be to have a harmonised eLending policy at the EU level. This would ensure that there is no discrimination between citizens across Member States in terms of access to knowledge, avoiding the implementation of geo-

194 VOB para 51.

195 Ibid.

blocking. Given well-known counterarguments relating to the limited competence of the EU in matters of cultural policy and the fact that any eLending policy will be influenced by national language and other idiosyncrasies, the most realistic solution appears to be to ensure the effectiveness of Art 6(1) of the Lending Right Directive.

117 It is the core argument of this paper that the limited current scope of exceptions available for libraries and the extensive control of digital forms of consumption by rightsholders hamper the full realisation of the cultural values underpinning the Directive. There are possible legislative and judicial interventions that could make the PL right Exception in Art 6(1) effective, and to these we will now turn to.

I. Judicial intervention

118 A so-minded Court would be able to dynamically interpret the existing EU copyright acquis to realise a more balanced copyright system. Strong arguments have been raised in favour of the recognition of some forms of digital exhaustion. The CP right, as demonstrated in this Article, cannot and should not be expected to cover all forms of digital distribution; this point is reinforced in light of the need for copyright to adapt to ''new forms of exploitation'' (e.g., sale of digital content). Developments in this direction would steer copyright towards promoting a more balanced notion of digital ownership.

119 In light of the conflicting interests at stake and the political significance of such developments, the intervention of the legislative bodies would be the most welcome solution. However, the CJEU could still play a considerable role as there is scope to interpret the existing exceptions and limitations more favourably towards public libraries. In particular, if given the opportunity the Court should:

- clarify that Art 5(2)(c) of InfoSoc allows libraries to digitise physical books in their catalogue for the purpose of carrying out eLending in all those specific instances either when:

  a) no genuine commercial access to the digital copy of the book exists at the time of digitalisation, or

  b) such access is subject to the acceptance of unfair terms and conditions.

- clarify that an act of making available a copy of a work to one single user, as opposed to a public is not to be considered a communication to the public; it is therefore not covered by InfoSoc. In other words, it is an area as yet not harmonised either by EU or international law. Not only is this consistent with earlier case law but it would enable the Commission – or individual Member States – to introduce a new form of copyright covering the distribution or sale of digital content.

120 A judicial intervention depends on referral by a national Court in the context of national proceedings,[196] which means that doctrinal issues may only be partially solved by the judgment of the Court; instead, the interventions of the CJEU are generally tailored to clarifying a point of law necessary to enable the national Court to give judgment. Pending a reference to the CJEU, Member States may be discouraged or reluctant to introduce such an exception; not only would a legislative intervention require significant political goodwill – after all, defining what terms are unfair is inherently controversial – but would expose the legislative body to potential infringement proceedings by the Commission.[197] In order to restore legal certainty and provide an authoritative – yet not binding – interpretation of EU law, the Commission may instead consider to intervene pre-emptively) supporting such an interpretation of Art 5(2)(c) of the InfoSoc.

II. Legislative intervention

121 At the EU level, a general legislative intervention in the field of copyright is unlikely in the immediate future. More specific interventions are likely to be considered by the next legislature.[198] The policy interventions here considered are limited in scope and aim solely to make Art 6(1) effective in the context of digital lending, mostly by allowing libraries independent access to digital copies.

1. Consumer protection

122 A mandatory clause could be introduced in consumer contracts for eBooks allowing resale/donation of eBook to public libraries for the purpose of eLending. In practice, this could take the form of a contractual right to consumers to grant a non-exclusive license in eBooks contracts for the benefit of public libraries, allowing them to store a copy of such an eBook on their server and lend it digitally to the public in

196 Treaty on the Functioning of the European Union (TFEU) art 267. See Chalmers et al., *European Union Law: Text and Materials* (Cambridge University Press, 2019), p. 328-363.

197 TFEU art 258. See Chalmers (n. 198) p. 328-363.

198 Tsakonas et al., 'Secondary Publishing Rights in Europe: Status, Challenges and Opportunities' (2023) Knowledge Rights 21; See WIPO, 'Proposal by African Group for a Draft Work Program on Exceptions and Limitations' (Document submitted to SCCR, 2023) SCCR/43/8 p. 3.

the context of an ePL right scheme on a one-copy/one-user basis. The expected outcome is to enable independent access to digital copies of books.

2. Contract law

123 An obligation could be introduced for publishers to ensure that, whenever licensing access to digital copies for the purpose of eLending, all terms of the license are reasonable and fair, taking due account of the cultural objectives pursued by ePL right schemes in Art 6(1). This suggestion follows a similar example of US State legislation (e.g., Maryland).[199] It would maintain the publishers' role as exclusive lawful source of digital copies of books while also ensuring that the conditions demanded for such access does not frustrate the purpose of the PL right Exception in Art 6(1) - e.g., a remuneration grossly exceeding the cost of digitalisation of the books and extending to potential loss sales due to the eLending.

3. eBook altruism

124 This solution is more complex as it requires the setting up of a governance framework for eBooks, involving both legislative and non-legislative interventions. A legislative measure may be used to introduce a form of digital exhaustion applicable only for eBooks; it would be however a limited form of exhaustion, allowing private parties to transfer their copies of eBooks to public libraries whenever they have acquired them in pursuit of a contract of sale. In order to do so, it would be necessary to set up a secured infrastructure – similar to the one set up by the Tom Kabinet platform (cf. case C-263/18) – where eBooks can be stored after purchase.

125 In practice, it would allow ''owners'' of eBooks to donate them to an ePL right scheme after they read it in essentially a similar way that they would do for physical books, which could then use them as a source of digital copies for carrying out eLending. The one-copy/one-user approach seems recommended in light of its functional equivalence with physical books and its more limited impact on the interests of publishers and authors (the latter, and potentially even the former – see suggestion below – could still receive a remuneration for each act of eLending in the context of an ePL right scheme). This solution takes inspiration from the notion of data altruism (leveraging on eBook altruism), an emerging concept in data legislation (Data Governance Act).[200]

III. Concluding thought

126 Intellectual property law is premised on a paradox: it is a system that aims to promote knowledge dissemination by restricting it. This article explored the changing conditions for knowledge dissemination in one crucial and under-researched setting: the digital lending of books, or 'e-lending'. We show that libraries are no longer able to build stable collection over time. Rather, the informational needs of societies increasingly are regulated by complex licensing mechanisms, granting different levels of access to the public, often in bundles and limited in time. Following the CJEU's ruling in Tom Kabinet (C-263/18), the lack of digital exhaustion appears to entrench licensing as the sole option available to public libraries. This state of affairs leaves user interests particularly vulnerable, with no agreed standard available to define reasonable conditions of access and control.[201] We offer a range of possible solutions, reflecting different kinds of juridical and political appetite for change in this area. We argue that proportionate and feasible interventions are possible under copyright, consumer and contract law.

199 A Albanese and J Milliot, 'With New Model Language, Library E-book Bills Are Back' (*Publishers Weekly*, 23rd February 2023) <https://www.publishersweekly.com/pw/by-topic/industry-news/libraries/article/91581-with-new-model-language-library-e-book-bills-are-back.html#:~:text=Passed%20unanimously%20in%20March%20of,of%20tension%20in%20the%20digital>.

200 Data Governance Act art 2(16). See also in particular Recitals 45, which explains that data altruism taps into the potential for serving ''objective of general interest in the use of data made available voluntarily''.

201 Natali Helberger, 'Standardizing consumers' expectations in digital content' (2011) 13/6 info 69.

Civil Society Actors as Enforcers of the GDPR: What Role for the CJEU?

by **Valentina Golunova and Mariolina Eliantonio ***

Abstract:

This article examines the interaction between the CJEU and civil society actors in data protection cases. It first reflects on the role of such actors in legal actions concerning the protection of personal data before national and EU courts, stressing their key potential to address power imbalances between individuals and Big Tech companies. Then, it critically assesses the CJEU's contribution to fostering the role of civil society in the GDPR enforcement. It demonstrates that non-governmental organizations are excluded from participation in infringement proceedings against Member States for failing to fulfil their obligations under the GDPR, which can be launched by the Commission under Article 258 TFEU. Furthermore, such organizations cannot bring direct actions against the Commission's delegated and implementing acts due to the lack of standing under Article 263 TFEU. Additionally, civil society actors have a limited ability to intervene as third parties in the legal proceedings before the CJEU. However, this article contends that a greater involvement of these actors in legal proceedings before the CJEU is key to enhancing its responsiveness to the demands of civil society. It therefore reflects on the ways to make the CJEU a more effective avenue for legal mobilization in the field of data protection.

Keywords: civil society, data protection, GDPR, CJEU, mobilization, standing, preliminary ruling, third-party intervention

Recommended citation: Valentina Golunova and Mariolina Eliantonio, Civil Society Actors as Enforcers of the GDPR: What Role for the CJEU?, 15 (2024) JIPITEC 180 para 1.

A. Introduction

1 Civil society actors play a vital role in advancing democratic values and paving the way to a more just and equitable society.[1] They draw attention to failures of the legal system and hold both public institutions and corporations accountable for actions which have a negative impact on society at large. Among other endeavours, NGOs, individual activists, and other watchdogs commonly engage in legal mobilization, which is understood as a strategic use of law and institutional mechanisms to advance a particular cause.[2] In the EU, such actors are active in many different regulatory domains, including environment,[3] migration,[4] and, more recently, data

* Valentina Golunova is an Assistant Professor of Digital Democracy at the Maastricht University. Mariolina Eliantonio is a Professor of European and Comparative Administrative Law and Procedure at the Maastricht University. The authors would like to sincerely thank Evangelia Psychogiopoulou and Federica Casarosa for their helpful comments on the earlier version of the article.

1 Rachel A Cichowski, *The European Court and Civil Society: Litigation, Mobilization and Governance* (Cambridge University Press 2007).

2 Emilio Lehoucq and Whitney K. Taylor, 'Conceptualizing Legal Mobilization: How Should We Understand the Deployment of Legal Strategies?' (2020) 45 Law & Social Inquiry 166, 168.

3 See, for instance, Dutch Supreme Court (Hoge Raad), Urgenda Foundation v. the Netherlands, Judgment of 20 December 2019, No. 19/00135, ECLI:NL:HR:2019:2006; Brussels Court of Appeal (Cour d'appel de Bruxelles), VZW Klimaatzaak v. the Federal State of Belgium and others, Judgment of 30 November 2023, No. 2023/8411; Tribunale Ordinario di Roma (Civil Court of Rome), A Sud et al v. Italy, writ of summons, filed on 5 June 2021.

4 See, among others, Sentenza Tribunale di Roma, Prima sezione civile. n. 22917/2019, RG n. 5615/2016; *S.S. and*

protection.[5] A growing number of organizations are mobilizing various legal avenues to challenge unfair or exploitative data-driven practices and assist data subjects in exercising their right to an effective remedy.[6]

2 As deftly noted by the European Data Protection Supervisor (EDPS) Wojciech Wiewiórowski, civil society actors are the "natural allies of the data protection authorities".[7] At the same time, the General Data Protection Regulation (GDPR) explicitly empowers not-for-profit bodies, organizations and associations to bring complaints on behalf of data subjects not only before national supervisory authorities but also national courts of Member States.[8] The importance of representative actions for addressing the GDPR infringements has also been underscored in the case law of the CJEU.[9] Indeed, civil society actors have shown remarkable achievements in ensuring that the GDPR not only barks but also bites those who do not comply with its provisions. In May 2023, Meta was fined a record € 1.2 billion by the European Data Protection Board (EDPB) for transferring personal data to the US in breach of the GDPR following an enquiry by the Irish Data Protection Authority.[10] Notably, this enquiry was originally initiated by noyb – a prominent non-governmental organization (NGO) focusing on data protection. Civil society actors have also helped expose many other major GDPR infringements that would likely remain undiscovered otherwise.[11] Yet both EU institutions and Member States have occasionally showed resistance to the participation of civil society actors in the GDPR enforcement. For example, European Commissioner for Justice Didier Reynders has questioned the NGOs' contribution to enhancing the protection of personal data in the EU, suggesting that some of them bring GDPR complaints "as a business model".[12] Many civil society organizations also face considerable procedural obstacles when litigating data protection cases at the Member State level.[13] Accordingly, there is a growing claim that reaffirming and broadening the opportunities for civil society to participate in legal proceedings concerning the rights of the data subjects is crucial for achieving better enforcement of the GDPR.[14]

3 While there is a vast body of scholarly literature addressing the GDPR implementation in general,[15]

Others v Italy App No 21660/18 (ECtHR), communicated on 14 October 2019; UN Human Rights Committee, Denny Zhao v. the Netherlands, U.N. Doc. CCPR/C/130/D/2918/2016 (2020).

5 'Première Sanction Contre Google Suite à Nos Plaintes Collectives' (*La Quadrature du Net*, 21 January 2019) <https://www.laquadrature.net/2019/01/21/premiere-sanction-contre-google-suite-a-nos-plaintes-collectives/> accessed 26 January 2024; 'Belgian Authority Finds IAB Europe's Consent Pop-Ups Incompatible with the GDPR' (*European Digital Rights (EDRi)*, 16 February 2022) <https://edri.org/our-work/belgian-authority-finds-iab-europes-consent-pop-ups-incompatible-with-the-gdpr/> accessed 26 January 2024.

6 Inbar Mizarhi-Borohovich, Abraham Newman and Ido Sivan-Sevilla, 'The Civic Transformation of Data Privacy Implementation in Europe' [2023] West European Politics 671, 672–673.

7 Wojciech Wiewiórowski, 'Civil Society Organisations as Natural Allies of the Data Protection Authorities' (*European Data Protection Supervisor*, 15 May 2018) <https://edps.europa.eu/press-publications/press-news/blog/civil-society-organisations-natural-allies-data-protection> accessed 26 July 2023.

8 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) (GDPR), art 80.

9 Case C-40/17 *Fashion ID* [2019] ECLI:EU:C:2019:629; Case C-319/20 *Meta Platforms Ireland* [2022] ECLI:EU:C:2022:322.

10 Binding Decision 1/2023 on the dispute submitted by the Irish SA on data transfers by Meta Platforms Ireland Limited for its Facebook service (Art. 65 GDPR) [2023].

11 See, for instance, 'Wij komen op voor jou: Spotify krijgt boete van 5 miljoen euro' (*Bits of Freedom*, 13 June 2023) <https://www.bitsoffreedom.nl/2023/06/13/wij-komen-op-voor-jou-spotify-krijgt-boete-van-5-miljoen-euro/> accessed 26 January 2024; 'Digital Rights Ireland Takes DPC to Court Over Facebook's 530 Million Users' Data Leak' (*Digital Rights Ireland*, 10 January 2023) <https://www.digitalrights.ie/dri-takes-dpc-to-court-over-facebook-data-leak/> accessed 26 January 2024.

12 'Open Letter: Commissioner Reynders Asked to Correct Unacceptable Accusations against NGOs' (11 July 2023) <https://noyb.eu/en/open-letter-commissioner-reynders-asked-correct-unacceptable-accusations-against-ngos> accessed 14 July 2023.

13 '5 Years of the GDPR: National Authorities Let down European Legislator' (*noyb*, 23 May 2023) <https://noyb.eu/en/5-years-gdpr-national-authorities-let-down-european-legislator> accessed 26 July 2023.

14 Marie-Pierre Granger and Kristina Irion, 'The Right to Protection of Personal Data: The New Posterchild of European Union Citizenship?', *Civil Rights and EU Citizenship* (Edward Elgar Publishing 2018) 292; Maryant Fernández, 'BEUC's Recommendations on Harmonising Cross-Border Procedural Matters in the GDPR' (European Consumer Organisation 2023) 2 <https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-034_recommendations_on_harmonising_cross-border_procedural_matters_in_the_GDPR.pdf> accessed 31 October 2023.

15 See, among others, Benjamin Greze, 'The Extra-Territorial Enforcement of the GDPR: A Genuine Issue and the Quest for Alternatives' (2019) 9 International Data Privacy Law 109; Brian Daigle and Mahnaz Khan, 'The EU General Data Protection Regulation: An Analysis of Enforcement Trends

the interrogation of the role of civil society actors in this area remains rare. Some academic writings have undertaken to examine how NGOs can foster the protection of personal data across the EU.[16] However, these writings focus primarily on the NGOs' participation in legal proceedings before national DPAs and national courts in the Member States. At the same time, the interaction between civil society groups and the CJEU remains largely overlooked.

4 The role of the CJEU as a venue of legal mobilization has been subject to academic debate. Some describe it as a promising avenue for bottom-up legal action.[17] Others, on the contrary, have exposed and critiqued the CJEU's scant engagement with civil society organizations.[18] The CJEU's potential is often argued to be circumscribed by the provisions of the Treaty on the Functioning of the EU (TFEU), which strictly defines who, and under what circumstances, can bring cases before the CJEU and be involved in the proceedings before it.[19] Accordingly, it is necessary to examine whether and how civil society actors have engaged or could engage with the CJEU in data protection cases. This analysis is especially crucial since procedural obstacles faced by these actors when trying to reach the CJEU could severely impact the latter's receptiveness to their substantive legal arguments.

5 The objective behind this article is therefore twofold. On the one hand, it examines the existing pathways for interaction between civil society actors and the CJEU in the data protection context. In this respect, this article analyses how such actors can mobilize the CJEU to remedy the gaps in the GDPR enforcement and whether the CJEU has upheld or rather undermined their efforts to either initiate or participate in relevant proceedings. On the other hand, this article reflects on whether and how a greater involvement of NGOs and individual activists specializing in the protection of personal data in proceedings before the CJEU could strengthen the existing mobilization initiatives at the national level. In this respect, it argues that enhancing the CJEU's capacity to thoughtfully address the claims put forward by civil society is instrumental for bolstering the protection of fundamental rights in the digital realm.

6 This article is structured as follows. Section B underscores the essential importance of civil society actors in ensuring the effective implementation of the GDPR. It analyses Article 80 GDPR, which secures the right of NGOs to represent data subjects in legal proceedings and explores the CJEU's case law elucidating the scope of this right. In turn, section C investigates the opportunities and obstacles to the civil society groups' involvement in the proceedings concerning the protection of personal data before the CJEU. On the one hand, it gives examples of how civil society actors and the CJEU have engaged in indirect dialogue in preliminary reference proceedings. On the other hand, it observes that the possibilities for a more direct and hence meaningful interaction between the two remain extremely limited due to the exclusion of civil society groups from infringement proceedings, their inability to bring direct actions against the Commission's delegated and implemented acts, including adequacy decisions, and procedural hurdles to third-party interventions. To conclude, section D considers ways of increasing the CJEU's responsiveness to claims made by civil society groups by ensuring better access of these actors to the proceedings before the CJEU.

by EU Data Protection Authorities' (2020) 2020 Journal of International Commerce & Economics 1; Giulia Gentile and Orla Lynskey, 'Deficient by Design? The Transnational Enforcement of the GDPR' (2022) 71 International and Comparative Law Quarterly 799.

16 Peter Rott, 'Data Protection Law as Consumer Law – How Consumer Organisations Can Contribute to the Enforcement of Data Protection Law' (2017) 3 Journal of European Consumer and Market Law 113, 113–114; Federica Casarosa, 'Transnational Collective Actions for Cross-Border Data Protection Violations' (2020) 9 Internet Policy Review 1; Emilio Lehoucq and Sidney Tarrow, 'The Rise of a Transnational Movement to Protect Privacy' (2020) 25 Mobilization: An International Quarterly 161; Woojeong Jang and Abraham L Newman, 'Enforcing European Privacy Regulations from Below: Transnational Fire Alarms and the General Data Protection Regulation' (2022) 60 JCMS: Journal of Common Market Studies 283; Mizarhi-Borohovich, Newman and Sivan-Sevilla (n 6).

17 Jos Hoevenaars, *A People's Court? A Bottom-up Approach to Litigation before the European Court of Justice* (Eleven Publishing 2018); Virginia Passalacqua, 'Legal Mobilization via Preliminary Reference: Insights from the Case of Migrant Rights' (2021) 58 Common Market Law Review 751, 771–772.

18 Sergio Carrera and Bilyana Petkova, 'The Potential of Civil Society and Human Rights Organizations through Third-Party Interventions before the European Courts: The EU's Area of Freedom, Security and Justice' in Mark Dawson, Bruno De Witte and Elise Muir (eds), *Judicial Activism at the European Court of Justice* (Edward Elgar Publishing 2013) 262–263; Mariolina Eliantonio, 'The Role of NGOs in Environmental Implementation Conflicts: "Stuck in the Middle" between Infringement Proceedings and Preliminary Rulings?' (2018) 40 Journal of European Integration 753, 763; Kris van der Pas, 'All That Glitters Is Not Gold? Civil Society Organisations and the (Non-)Mobilisation of European Union Law' [2023] JCMS: Journal of Common Market Studies 1, 3–4.

19 Consolidated version of the Treaty on the Functioning of the European Union [2012] OJ C 326/47, arts 251-281.

B. Civil Society Actors as Mechanisms of Bottom-Up GDPR Enforcement

7 The adoption of the GDPR marked a transition from a rigid, top-down regulatory regime to one that relies heavily on bottom-up enforcement. The purpose of this section is to shed light on the role of civil society actors in strengthening the protection of personal data across the EU. Section B.I reflects on the significance of Article 80 GDPR, showing how the involvement of NGOs in proceedings concerning the GDPR infringements can help safeguard the rights of data subjects. Section B.II analyses the CJEU's case law dealing with the right of not-for-profit organizations and other entities to bring action against persons who are potentially responsible for the violations of the GDPR.

I. The role of civil society in enhancing the protection of personal data

8 Civil society organizations are increasingly seen as 'decentralized enforcers of EU law'.[20] However, until recently, the role of such organizations in ensuring the effective protection of personal data remained limited. The GDPR's predecessor – Directive 95/46/EC 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 ("the DPD") – did not expressly envision the right of civil society organizations to bring legal proceedings in relation to the alleged infringements of the protection of personal data.[21] This blind spot has drawn criticism. Most notably, in its Opinion on the Commission's proposal for a GDPR issued in 2012, the EU Agency for Fundamental Rights (FRA) advocated recognizing the right of non-profit bodies acting in the public interest to lodge complaints regarding breaches of the data protection regime.[22] In response to the growing calls for enabling civil society to take an active part in data protection litigation, the EU legislator undertook to guarantee the right of all entities acting in the public interest and active in the field of the protection of data subjects' rights and freedoms to bring complaints on behalf of data subjects. Article 80 GDPR empowers data subjects to mandate not-for-profit bodies, organizations and associations to lodge complaints with a supervisory authority (Article 77 GDPR) or bring legal proceedings before a competent judicial authority, either against a supervisory authority (Article 78 GDPR) or against a controller or processor (Article 79 GDPR).[23] Additionally, the said entities are entitled to exercise the right to receive compensation (Article 82 GDPR) on behalf of these data subjects where provided for by domestic law of Member States. It is further specified that Member States can recognize the right of not-for-profit bodies, organizations and associations to exercise the said rights independently of the data subject's mandate, which is understood as an authorization issued by the latter to act on their behalf.[24]

9 Article 80 GDPR is a powerful instrument against breaches of data protection rules.[25] As extensively argued by scholars, representative actions significantly enhance access to justice for individuals.[26] The reasons why data subjects may not be willing or able to engage in litigation on their own are manifold. Many citizens are unaware of their rights under the GDPR as well as legal remedies available to them in case these rights are breached. Even when data subjects suspect that they might have become a victim of a GDPR infringement, they are often discouraged from lodging a complaint against the person responsible for this infringement due to the high costs of litigation or considerable

20 Konstantin Reiners and Esther Versluis, 'NGOs as New Guardians of the Treaties? Analysing the Effectiveness of NGOs as Decentralised Enforcers of EU Law' (2023) 30 Journal of European Public Policy 1518.

21 See, however, 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 L 281/31 (DPD), art 28(4) (obliging supervisory authorities to hear 'claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data').

22 European Union Agency for Fundamental Rights, 'Opinion 2/2012 on the Proposed Data Protection Reform Package' (2012) 29 <https://fra.europa.eu/sites/default/files/fra-opinion-data-protection-oct-2012.pdf> accessed 1 August 2023.

23 GDPR, art 80(1).

24 GDPR, art 80(2). See also GDPR, recital 142.

25 Gloria González Fuster, 'Article 80 Representation of Data Subjects' in Christopher Kuner and others (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2020) 1143; Jang and Newman (n 16) 294.

26 Mauro Cappelletti (ed), *Access to Justice and the Welfare State* (Sijthoff 1981); Carol Harlow, 'Public Law and Popular Justice' (2002) 65 The Modern Law Review 1, 8–9; Rebecca Money-Kyrle and Christopher Hodges, 'European Collective Action: Towards Coherence?' (2012) 19 Maastricht Journal of European and Comparative Law 477, 481–482; Fernando Gascón Inchausti, 'A New European Way to Collective Redress? Representative Actions under Directive 2020/1828 of 25 November' (2021) 18 Zeitschrift für das Privatrecht der Europäischen Union 61, 79–80.

delays on obtaining effective redress.[27] Civil society actors can step in to both clarify the GDPR provisions to data subjects as well as relieve them of the heavy burden of pursuing complaints concerning the alleged GDPR breaches themselves.[28] Bringing representative actions by these actors can make data protection litigation more efficient, since data-driven practices violating the GDPR typically affect a broad circle of individuals. Importantly, civil society groups can also help mitigate the power asymmetry between data subjects and Big Tech companies. Many individuals feel intimidated by the prospect of lodging a complaint against powerful market players operating on a transnational basis.[29] Having more resources and influence than data subjects, non-profit bodies and organizations specializing in the protection of personal data can effectively confront Big Tech companies before national DPAs or national courts of Member States.

10 Yet the role of civil society actors in upholding the protection of personal data is not limited to bringing representative actions on behalf of data subjects. Non-profit bodies and organizations focusing on data protection offer invaluable support to national DPAs tasked with the supervision of the application of the GDPR. DPAs often lack staff, resources and expertise to properly identify and investigate GDPR infringements.[30] NGOs can therefore assist with monitoring the compliance with the GDPR and supplying the evidence of the GDPR breaches to DPAs.[31] Civil society actors have also been actively engaging in legal mobilization in order to advance a stricter enforcement of the GDPR across in the EU. In this respect, some critique Article 80(2) GDPR for allowing Member States the discretion to determine whether civil society actors can bring complaints without the data subject's mandate under their national law, thus failing to harmonize the right of NGOs to launch strategic litigation.[32] Kang and Newman also argue that NGOs are uniquely position to "raise awareness and salience of data protection enforcement".[33] Indeed, apart from bringing complaints against the GDPR infringements, civil society organizations have also successfully leveraged media attention to attract public attention to data protection disputes and put pressure on the EU institutions to enhance the compliance with the GDPR within the EU. Additionally, the work of Lehoucq and Tarrow has provided insight into how civil society groups specializing in data protection have been building mechanisms of transatlantic cooperation, which are expected to stimulate "activism-induced policy making" and secure a higher level of protection of personal data around the world.[34] As a result, the active role of representatives of civil society in detecting and acting on infringements of data protection rules both contributes to the effective GDPR implementation across the EU and fosters the respect for fundamental rights of data subjects on a global scale.

II. The CJEU's perspective on the role of civil society actors in enforcing the GDPR

11 The case law of the CJEU reveals its firm conviction that enabling civil society actors to take legal action against potential infringers of data subjects' rights is instrumental for the effective enforcement of the data protection regime in the EU. For the first time, the CJEU turned to this matter in *Fashion ID*, which was decided in 2019.[35] The request for a preliminary ruling was made in the course of the national legal

27 European Agency for Fundamental Rights, 'Access to Data Protection Remedies in the EU Member States' (Publications Office of the European Union 2013) 32 <https://fra.europa.eu/sites/default/files/fra-2014-access-data-protection-remedies_en_0.pdf> accessed 1 August 2023.

28 Gloria González Fuster and others, 'The Right to Lodge a Data Protection Complaint: OK, but Then What? An Empirical Study of Current Practices under the GDPR' (Data Protection Law Scholars Network, Access Now 2022) 60 <https://www.accessnow.org/wp-content/uploads/2022/07/GDPR-Complaint-study.pdf> accessed 1 August 2023.

29 See, most notably, Elinor Carmi and Simeon Yates, 'Data Citizenship: Data Literacies to Challenge Power Imbalance Between Society and "Big Tech"' (2023) 17 International Journal of Communication 19, 3626–3634.3626\\uc0\\u8211{}3634.","plainCitation":"Elinor Carmi and Simeon Yates, 'Data Citizenship: Data Literacies to Challenge Power Imbalance Between Society and "Big Tech"' (2023

30 'Data Protection: 80% of National Authorities Underfunded, EU Bodies "Unable to Fulfil Legal Duties"' (*Statewatch*, 30 September 2022) <https://www.statewatch.org/news/2022/september/data-protection-80-of-national-authorities-underfunded-eu-bodies-unable-to-fulfil-legal-duties/> accessed 1 August 2023.

31 Jang and Newman (n 16) 287.

32 Orla Lynskey, 'The Role of Collective Actors in the Enforcement of the Right to Data Protection under EU Law' in Elise Muir and others (eds), *How EU law shapes opportunities for preliminary references on fundamental rights: discrimination, data protection and asylum* (EUI Working Papers 2017/17) 96–97 <https://cadmus.eui.eu/bitstream/handle/1814/49324/LAW_2017_17.pdf?sequence=3&isAllowed=y> accessed 10 August 2023; Fuster (n 25) 1150."plainCitation":"Orla Lynskey, 'The Role of Collective Actors in the Enforcement of the Right to Data Protection under EU Law' in Elise Muir and others (eds

33 Jang and Newman (n 16) 292.

34 Lehoucq and Tarrow (n 16) 179.

35 *Fashion ID* (n 9).

proceedings between the online clothing retailer Fashion ID and the public-service association Verbraucherzentrale NRW, which sued the former for unlawfully transmitting personal data belonging to the visitors of their website to the social network Facebook (now Meta).[36] While the Regional Court of Düsseldorf found that Verbraucherzentrale NRW had standing to bring the relevant legal proceedings, the Higher Regional Court of Düsseldorf, to which Fashion ID appealed, was unsure about the conditions upon which the association should be entitled to represent data subjects and referred relevant questions to the CJEU.[37] The CJEU ruled that Articles 22 to 24 DPD, which stipulated rules on judicial remedies, liability and sanctions, did not preclude national legislation enabling consumer-protection associations to initiate legal proceedings against a person allegedly responsible for an infringement of this directive.[38] It underlined that the possibility to bring actions on behalf of data subjects contributes to the realization of the effective and complete protection of the fundamental rights and freedoms affected by the processing of personal data.[39] Even though the DPD did not expressly authorize consumer-protection associations to commence legal proceedings against data protection infringements, neither did it provide for an exhaustive harmonization of judicial remedies, and Member States enjoyed a margin of discretion in implementing that directive.[40] The CJEU also indicated that the involvement of the said bodies in defending the rights of data subjects would not curtail the independence of supervisory authorities which would still have "freedom to take decisions" and "freedom to act".[41] Accordingly, it supported the Advocate General Bobek's view that private actions brought by an association do not impact on the work of the DPAs, making them complement, not undermine public enforcement of data protection rules.[42]

12 The CJEU has reaffirmed its viewpoint in C-319/20 *Meta Platforms Ireland* delivered in 2022.[43] The request for a preliminary ruling arose from the dispute between the technology company Meta Platforms Ireland and the Federal Union of German Consumer Organizations ('the Union'). While the latter succeeded in obtaining an injunction against the former for violating data protection and consumer protection legislation, the Federal Court of Justice hesitated whether the Union had standing to bring legal proceedings before German domestic courts and asked for the CJEU's input on this matter.[44] The CJEU clarified that Article 80(2) GDPR did not preclude domestic law of Member States empowering consumer protection associations to bring legal proceedings concerning the alleged infringements of the GDPR in the absence of a mandate conferred on it for that purpose and regardless of the existence of a specific infringement of rights of the data subjects.[45] As rightly noted by Yakovleva, the CJEU was called upon to strike a fine balance between precluding fragmentation of not only substantive but also procedural rules and providing conditions for more robust enforcement of data subjects' rights.[46] Even though the GDPR aims at maximum harmonization of data protection rules, the CJEU found that Article 80(2) GDPR, being an "open clause", exceptionally enables Member States to exercise discretion when laying down the rules concerning representative actions in the national law.[47] The contours of the Member States' discretion were delineated rather broadly. First, the CJEU indicated that the notion of not-for-profit body, organization or association which has statutory objectives which are in the public interest and is active in the field data protection under Article 80(1) GDPR encompasses a wide range of entities, including consumer protection associations, which seek to stand for the data subjects' rights.[48] These entities are neither required to conduct a prior identification of persons concerned by allegedly unlawful data processing nor establish the existence of a specific infringement of these persons' rights.[49] Additionally, the CJEU ascertained that Article 80(2) GDPR does not preclude the bringing of a representative action alleging the infringement of data protection rules along with the rules on consumer protection given their interconnected nature.[50] By affording Member States a wide margin of discretion, the CJEU evidently strived to eliminate any excessive obstacles to representative actions in defence of data subjects' rights.

13 The clarifications provided by the CJEU in its case law did not put a definitive end to uncertainties regarding the interpretation of the rules on representative actions. Even after the German Federal Court of Justice obtained guidance from the CJEU in *Meta Platforms Ireland*, it found that the uncertainty regarding the interpretation of Article 80(2) GDPR persisted and proceeded to request another

36 ibid paras 25-29.
37 ibid paras 30-42.
38 *Fashion ID* (n 9) para 63.
39 ibid para 51.
40 ibid para 56.
41 ibid para 60.
42 Case C-40/17 *Fashion ID* [2019] ECLI:EU:C:2018:1039, Opinion of Advocate General Bobek, point 44.
43 *Meta Platforms Ireland* (n 9).
44 ibid paras 40-44.
45 ibid para 83.
46 Svetlana Yakovleva, 'Standing of Consumer Organizations in Data Protection Representative Actions - Case Note: C-319/20, ECLI:EU:C:2022:322' (2022) 1 Mass Claims: An International Journal with a European Focus 51, 53.
47 *Meta Platforms Ireland* (n 9) paras 57-60.
48 ibid paras 64–66.
49 ibid paras 67–73.
50 ibid paras 77–79.

preliminary ruling.[51] In its judgment delivered on 11 July 2024, the CJEU clarified that Article 80(2) GDPR does not preclude consumer protection associations from bringing representative actions alleging the breach of information obligations under Articles 12 and 13 GDPR. Accordingly, the CJEU further solidified the position of civil society actors as guardians of data subjects' rights.

C. The Interaction between Civil Society Actors and the CJEU in Data Protection Cases

14 As seen in section B, civil society actors play a vital part in the GDPR enforcement by bringing collective actions against persons responsible for GDPR infringements before national DPAs and national courts of Member States. However, the role of these actors is not limited to the representation of data subjects. They also engage in the transnational mobilization efforts to advance a greater protection of personal data and contribute to the appropriate implementation of the GDPR across the EU. The CJEU is an important point of attraction for such efforts.

15 This section reflects on the interplay between civil society actors and the CJEU in order to uncover the opportunities and challenges of using the proceedings before the CJEU as a mechanism of bottom-up GDPR enforcement. It first outlines the role of the preliminary reference procedure by examining how NGOs call upon national courts to send preliminary questions to the CJEU as a means of facilitating effective GDPR enforcement (section C.I). Then, it examines the existing obstacles precluding NGOs from participating in the proceedings before the CJEU (section C.II). It argues that, while NGOs have established pathways for indirectly mobilizing the CJEU to deal with various issues related to the GDPR compliance, their possibilities of directly engaging with the CJEU are extremely limited. However, the exclusion of civil society actors from the proceedings before the CJEU can ultimately compromise the effective protection of personal data in the EU.

I. Preliminary reference proceedings as a means of bottom-up GDPR enforcement

16 Civil society actors play a prominent role not only in the data protection litigation before the national DPAs and courts of the Member States but also before the CJEU itself. This section puts a spotlight on the role of these actors in preliminary reference proceedings (Article 267 TFEU). It focuses on the two objectives pursued by non-profit bodies and organizations when urging national courts to send preliminary questions to the CJEU. On the one hand, the preliminary reference procedure is used to ensure accountability of private companies for GDPR violations (section C.I.1). On the other hand, it allows civil society groups to indirectly mobilize the CJEU to review the validity of EU acts (section C.I.2).

1. Advocating corporate GDPR compliance

17 Civil society actors have successfully mobilized national courts to send a request for a preliminary ruling to the CJEU as a means of ensuring compliance with the data protection rules by private entities. For example, in *Verein für Konsumenteninformation*, the Supreme Court of Austria sent a request for a preliminary ruling in the course of the national proceedings between the Austrian Association for Consumer Information ("the Association") and Amazon EU.[52] The latter, while established in Luxembourg, concluded electronic sales contracts with consumers resident in Austria via the website with the domain name extension ".de".[53] The Association applied for an injunction to prohibit the use of all allegedly unfair terms in Amazon's general terms and conditions, including the term concerning the applicability of Luxembourg law. Given the uncertainty regarding the law that must govern data protection issues, the Supreme Court of Austria asked the CJEU to assist it in the interpretation of Article 4(1)(a) DPD, which codified the rules on the applicability of national laws of Member States to the processing of personal data. The CJEU clarified that the processing of personal data by an undertaking is governed by the law of the Member State to which directs its activities only if such a processing is carried out in the context of the activities of an establishment situated in that Member State.[54] Notably, CJEU concurred with Advocate General Saugmandsgaard Øe, who indicated that, despite the fact that the notion of "establishment" must generally be interpreted broadly, the undertaking cannot be seen to be established in a Member State merely because its website is accessible there.[55] In this respect, the judgment was not a win for the

51 Case C757/22 *Meta Platforms Ireland*, Request for a preliminary ruling from the Bundesgerichtshof (Germany) lodged on 15 December 2022 (2023/C 104/19).

52 Case C-191/15 *Verein für Konsumenteninformation* [2016] ECLI:EU:C:2016:612.

53 ibid para 29.

54 ibid paras 78–81.

55 ibid para 76. See also Case C-191/15 *Verein für Konsumenteninformation* [2016] ECLI:EU:C:2016:388, Opinion of Advocate General Saugmandsgaard Øe, point 117.

Association which primarily strived to establish the applicability of the Austrian Law on data protection (the Datenschutzgesetz).[56] At the same time, the CJEU noted that should the referring court find that the establishment in the context of which Amazon EU carries out the processing of that data is located in Germany, such processing would be governed by German law.[57] Therefore, the CJEU supported the Association's contention that the determination of law governing the processing of personal data by large e-commerce undertakings calls for a rigorous analysis of whether such processing is carried out in the context of the activities of their primary establishment or may be more closely connected to their establishment in other Member States.

18 The implicit interaction between the CJEU and civil society actors also occurred in *Planet49*, where the CJEU addressed the request for a preliminary ruling made by the Federal Court of Justice in Germany in the proceedings between the German Federation of Consumer Organizations ("the Federation") and the German online gaming company Planet49.[58] The dispute revolved around latter's use of a pre-ticked checkbox indicating the user's consent to the storage of cookies in a promotional lottery.[59] The CJEU was clearly sympathetic to the Federation's concern that such checkboxes would not allow to establish whether data subjects have given their consent to the processing of their personal data both willingly and unambiguously as some of them might be reluctant to read the text accompanying the checkbox.[60] Accordingly, it interpreted Articles 4(11) and 6(1)(a) GDPR as meaning that the consent to the processing of personal data is not valid where the user is expected to deselect a pre-checked checkbox in order to refuse their consent.[61] Therefore, the Federation managed to utilize the preliminary reference procedure as a means of resisting a GDPR-infringing practice implemented by the data controller.

2. Challenging legal acts of the EU institutions and Member States

19 Apart from seeking to hold private companies accountable for their GDPR-infringing practices, NGOs have also been active in challenging EU acts incompatible with the fundamental rights to privacy and data protection. The involvement of civil society actors is particularly prominent in data retention cases. In its landmark judgment in *Digital Rights Ireland*, the CJEU invalidated the controversial Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks.[62] The request for a preliminary ruling made by the High Court in Ireland originated from the legal action launched by the NGO regarding the legality of national measures on the retention of data relating to electronic communications. Most recently, in *Ligue des droits humains,* the CJEU was called upon to provide an interpretation of several EU acts, including the GDPR, as well as rule on the validity of Directive (EU) 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime ("the PNR Directive") and Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data ("the API Directive").[63] The domestic proceedings were initiated by the NGO which challenged the Belgian law transposing into domestic law the PNR Directive and the API Directive. In both cases, the CJEU was highly receptive to the arguments made by the NGOs, leading it to prioritise the protection of personal data over national security concerns voiced by the Member States.

20 Apart from challenging EU legislative acts that are allegedly incompatible with the fundamental right to data protection, civil society actors have also contributed to the bottom-up GDPR enforcement by indirectly mobilizing the CJEU to review the validity of non-legislative acts. The GDPR grants the Commission implementing powers in respect of cross-border transfers of personal data. Most importantly, the Commission may issue decisions determining that a third country, a territory or one or more specific sectors within a third country (no longer) ensures an adequate level of data protection (Articles 45(3) and (5) GDPR). The Commission is also empowered to adopt standard data protection clauses providing safeguards for the transfer of personal data to a third country alleging in the absence of an adequacy decision (Article 46(2)(c) GDPR). The regulation of data transfers to third countries is, however, a highly sensitive political matter, and the Commission's adequacy decisions are typically subject to fierce criticism.[64]

56 *Verein für Konsumenteninformation*, Opinion of Advocate General Saugmandsgaard Øe, point 27.

57 ibid para 80.

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

59 ibid paras 25–31.

60 ibid paras 54–55.

61 ibid para 65.

62 Joined cases C-293/12 and C-594/12 *Digital Rights Ireland* [2014] ECLI:EU:C:2014:238.

63 Case C-187/19 *Ligue des droits humains* [2022] ECLI:EU:C:2022:491.

64 Peter Blume, 'EU Adequacy Decisions: The Proposed New Possibilities' (2015) 5 International Data Privacy Law 34, 35–36; Barbara Sandfuchs, 'The Future of Data Transfers to

21 Civil society actors have played a crucial role in mobilizing the CJEU to review and ultimately invalidate the two Commission's implementing decisions confirming that the US ensured an adequate level of protection of personal data provided by the safe harbour privacy principles and the EU-US Privacy Shield in 2015 and 2020 respectively.[65] In both cases, the CJEU was called upon to rule on the interpretation and validity of these decisions by the High Court in Ireland in the course of the domestic proceedings initiated by Max Schrems, the privacy activist and the founder of noyb. Despite the action being brought in his personal capacity, Schrems engaged in litigation with a clear public interest objective – to enhance the protection of personal data in cross-border data transfers.[66] He first filed a complaint concerning the transferer of his personal data by Facebook Ireland to the US before an Irish DPA, which was rejected on the ground that, according to the Commission's Decision 2000/520, the US was found to ensure an adequate level of protection. Schrems then brought judicial review proceedings against the rejection of his complaint before the High Court in Ireland, which submitted a request for a preliminary ruling to the CJEU. After the Commission's adequacy decision was declared invalid, the rejection of Schrems' complaint was annulled by the High Court, after which he submitted a reformulated complain to the Irish DPA, this time raising the validity of both the new adequacy decision – Commission Implementing Decision (EU) 2016/1250 ("the Privacy Shield Decision") – as well as Commission Decision 2010/87/EU on standard contractual clauses for the transfer of personal data to processors established in third countries ("the SCC Decision"). While the CJEU confirmed the validity of the latter decision, the former was declared invalid. Hence, the CJEU was responsive to the plea for a more far-reaching protection of data subject rights in the context of transfers of personal data outside the EU. Notably, on 10 July 2023, the Commission adopted its third adequacy decision for the EU-US Data Privacy Framework.[67] noyb has already indicated its intention to challenge the new framework.[68] Therefore, preliminary reference proceedings serve as a prominent pathway for civil society actors to resist legal acts and practices of both the EU institutions and Member States which violate fundamental rights of data subjects.

II. Challenges to the civil society actors' participation in the proceedings before the CJEU

22 Section C.I has demonstrated how NGOs instrumentalize preliminary reference proceedings as a way of indirectly inducing the CJEU to offer the interpretation of various provisions of the GDPR as well as review the validity of EU acts. At the same time, the implicit dialogue between civil society actors and the CJEU highlighted above cannot take place unless the former succeed in convincing a national court to turn to the CJEU to provide an interpretation of EU law. Where national courts fail to acknowledge the soundness of the legal arguments presented by civil society organizations and proceed with requesting a preliminary ruling, legal mobilization efforts of such organizations become futile.

23 At the same time, the possibilities of civil society actors to directly engage with the CJEU are severely constrained, which inevitably interferes with the CJEU's responsiveness to their claims. The next section examines the three substantial hurdles encountered by civil society groups when trying to access the proceedings before the CJEU, namely their exclusion from infringement proceedings (section C.II.1), the lack of standing in actions for annulment (section C.II.2), and limited possibility to intervene in proceedings before the CJEU as third parties (section C.II.3). As civil society actors face significant hurdles when trying to reach the CJEU, the latter is often unable to properly engage with the former´s legal arguments, which could ultimately weaken the effective protection of fundamental rights in the digital domain.

1. Exclusion of civil society actors from infringement proceedings

24 Being a regulation, the GDPR is directly applicable across Member States. However, Member States are required to implement the GDPR in their domestic legal systems by bringing their national legislation

Third Countries in Light of the CJEU's Judgment C-311/18 – Schrems II' (2021) 70 GRUR International 245, 248.

65 Case C-362/14 *Schrems I* [2015] ECLI:EU:C:2015:650; Case C-311/18 *Facebook Ireland and Schrems* [2020] ECLI:EU:C:2020:559.

66 Marta Requejo Isidro, 'Max Schrems against Facebook' (2018) 4 MPILux Research Paper Series 2018 9–10 <https://www.mpi.lu/fileadmin/user_upload/Requejo_Isidro_Schrems_Facebook_02July18.pdf> accessed 6 February 2024.

67 Commission Implementing Decision of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework C(2023) 4745 final.

68 'European Commission Gives EU-US Data Transfers Third Round at CJEU' (*noyb*, 10 July 2023) <https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu> accessed 2 August 2023.

in compliance with its provisions. Furthermore, Member States are responsible for ensuring that the GDPR is applied correctly by their national supervisory authorities. The failure to either implement or comply with the GDPR can result in infringement proceedings that can be launched against a Member State by the Commission under Article 258 TFEU. According to this provision, the Commission shall first deliver a reasoned opinion on the non-compliance of a specific Member State with EU law. However, if the Member State in question does not comply with the Commission's opinion in a timely manner, the latter has the right to bring the case before the CJEU.

25 So far, the Commission has never started infringement proceedings for the failure to ensure the correct implementation of the GDPR by the Member States before the CJEU. However, the Commission has triggered Article 258 TFEU in respect of some Member States which have not ensure the adapt their national legal systems to the EU-wide rules stipulated by the GDPR.[69] Certain Member States have appropriately modified their national legislation in line with the GDPR but do not fully comply with it in practice. For instance, the Commission is continuously urged to investigate the systemic failures of the Member States to enforce the GDPR against powerful market players, particularly Big Tech giants.[70] For example, on 19 December 2022, the EU Ombudsman issued a decision on the complaint lodged by the Irish Council for Civil Liberties (ICCL) against the Commission for the failure of the latter to adequately monitor Ireland's application of the GDPR, recommending that the Commission requests a bi-monthly overview from the Irish Data Protection Commission on its handling of cases involving Big Tech companies.[71] The Ombudsman also explicitly acknowledged the role of civil society actors in putting a spotlight on the inadequate application of the GDPR in Ireland.[72] In response, the Commission has committed to a new monitoring scheme, whereby it will request all DPAs to share information on large-scale cross-border investigations on a bi-monthly basis.[73] It is therefore likely that the new approach to monitoring compliance with the GDPR would lead the Commission to discover the breaches of the GDPR and launch infringement proceeding against the Member States responsible for these breaches.

26 Admittedly, infringement proceedings before the CJEU are not the only means of addressing issues of non-compliance with the GDPR by Member States. Both data subjects or NGOs representing their interests can invoke its provisions before national courts in order to challenge potentially unlawful actions or omissions of the Member States. However, the bringing of domestic proceedings arguably has a rather limited effect on stimulating the effective GDPR implementation across the EU. Decisions of national courts confirming that a Member States is in violation of the GDPR would only have an *inter partes* effect and are unlikely to lead Member States to remedy systemic infringements. Infringement proceedings, on the contrary, are more effective for putting pressure on non-compliant Member States to take measures to address structural compliance issues affecting the interests of a wide circle of persons. In 2016, the Commission indicated that, when launching infringement proceedings, it would put "particular emphasis on those infringements that have a significant impact on the attainment of important EU policy objectives".[74] This "strategic" approach indicates that infringement proceedings are not just an enforcement mechanism but also a powerful political tool.[75] Accordingly,

69 See, for instance, 'June Infringements Package: Key Decisions' (*European Commission*, 9 June 2021) <https://ec.europa.eu/commission/presscorner/detail/en/inf_21_2743> accessed 1 August 2023 (an infringement procedure against Belgium for violating Article 52 GDPR); 'February Infringements Package: Key Decisions' (*European Commission*, 9 February 2022) <https://ec.europa.eu/commission/presscorner/detail/en/inf_22_601> accessed 1 August 2023 (an infringement procedure against Slovenia for failing to authorize its DPA to use all the corrective powers under the GDPR); 'April Infringements Package: Key Decisions' (*European Commission*, 6 April 2022) <https://ec.europa.eu/commission/presscorner/detail/EN/inf_22_1769> accessed 1 August 2023 (letters of formal notice to Germany, Greece, Finland and Sweden for failing to ensure the correct implementation of the GDPR provisions in their domestic law).

70 See, for example, Johnny Ryan and Alan Toner, 'Europe's Enforcement Paralysis (2021 GDPR Report): ICCL's Report on the Enforcement Capacity of Data Protection Authorities' (Irish Council for Civil Liberties 2021) <https://www.iccl.ie/wp-content/uploads/2021/09/Europes-enforcement-paralysis-2021-ICCL-report-on-GDPR-enforcement.pdf> accessed 1 August 2023; Gentile and Lynskey (n 15) 820.

71 Decision on whether the European Commission collects sufficient information to monitor Ireland's implementation of the EU's General Data Protection Regulation (GDPR) (Case 97/2022/PB).

72 ibid 2– 3.

73 European Commission, 'Comments of DG Justice and Consumers on a Request for Information from the European Ombudsman - Complaint by the Irish Council for Civil Liberties (ICCL), Ref. 97/2022/PB' <https://www.iccl.ie/wp-content/uploads/2023/01/FOLLOW_UP_202200097_20230124_122005.pdf> accessed 1 August 2023.

74 Commission, 'Better Regulation: Delivering better results for a stronger Union' (Communication) COM(2016) 615 final 2016, 9.

75 Olivier De Schutter, 'Infringement Proceedings as a Tool for the Enforcement of Fundamental Rights in the European Union' (Open Society Foundations 2017) 65 <https://www.

the commencement of such proceedings could serve a strong incentive for improving the GDPR implementation in Member States.

27 The involvement of civil society actors in infringement proceedings against Member States could significantly enhance the effectiveness of this mechanism for strengthening the protection of personal data in the EU. Scholars have long argued that the Commission has almost no investigative power of its own, making it unable to effectively monitor infringements of EU law.[76] For this reason, the Commission's new approach to monitoring the GDPR infringements by means of biannual checks has drawn skepticism. In order to reduce the workload, the Commission refused to collect information on large-scale cross-border investigations for the full period of the GDPR's application.[77] As a result, there is a risk that the Commission would be unable to determine and take action on numerous infringements of the GDPR by various Member States which have occurred since the GDPR's entry into force. In this respect, NGOs are much better placed to uncover such infringements. When bringing complaints before the DPAs and domestic courts, they gain unique insight into how the GDPR is implemented or applied by various Member States. Therefore, the participation of civil society organizations in infringement proceedings could help address the instances of the Member States' non-compliance with the GDPR, strengthening the protection of fundamental rights of data subjects.

28 However, the possibilities for civil society groups to be involved in infringement proceedings are extremely limited. Importantly, NGOs can inform the Commission of GDPR infringements by Member States. The Commission has reiterated the important role played by private complainants, such as civil society organizations, in assisting with the detection of infringements of EU law.[78] However, the Commission enjoys full discretion to decide whether to launch an infringement procedure against Member States. Even if such a procedure is eventually opened, civil society actors acting as complainants do not have any influence on its course.[79] Accordingly, they also have no role in the infringement proceedings before the CJEU should the Commission decide to initiate them. While the Commission has acknowledged the need for greater transparency of the infringement procedure (especially in regard to the successive steps taken by the Commission in the procedure), the general public still has very limited knowledge of the motives for the Commission's enforcement actions.[80] Article 40 of the Statute of the CJEU ("the Statute") precludes the intervention of natural or legal persons in cases between Member States and EU institutions. As a result, the CJEU is effectively precluded from obtaining the civil society actors' unique perspective on the potential GDPR infringements by the Member States. The exclusion of these actors from infringement proceedings may therefore negatively affect the CJEU's potential to effectively repair the flaws of the GDPR implementation and thereby enhance respect for fundamental rights to privacy and data protection.

2. Lack of standing in actions for annulment

29 The *Schrems* saga discussed in section C.I.2 reveals how civil society actors have leveraged the preliminary reference procedure as an instrument of challenging EU acts incompatible with the fundamental right to data protection. However, this legal route has several compelling disadvantages. As argued by Advocate General Jacobs in Case C-50/00 P *UPA*, the possibility to bring issues of validity of the EU measures indirectly via national courts is incapable of providing full and effective judicial protection.[81] Indeed, in order to challenge the Commission's implementing decisions, NGOs have to engage in lengthy and costly proceedings before the national DPAs and national courts. Moreover, they are always dependent on the national court's willingness to send their request for a preliminary ruling to the CJEU.[82] As also underscored by

opensocietyfoundations.org/publications/infringement-proceedings-tool-enforcement-fundamental-rights-european-union> accessed 9 August 2023.

76 Tanja A Börzel and others, 'Obstinate and Inefficient: Why Member States Do Not Comply With European Law' (2010) 43 Comparative Political Studies 1363, 1374.

77 Johnny Ryan, 'Europe-Wide Overhaul of GDPR Monitoring Triggered by ICCL' (*Irish Council for Civil Liberties*, 31 January 2023) <https://www.iccl.ie/digital-data/europe-wide-overhaul-of-gdpr-monitoring-triggered-by-iccl/> accessed 1 August 2023.

78 Commission, 'EU law: Better results through better application' (Communication) C(2016)8600, 16; Commission, 'Enforcing EU law for a Europe that delivers' (Communication) COM(2022) 518 final, 21.

79 Ludwig Krämer, 'EU Enforcement of Environmental Laws: From Great Principles to Daily Practice – Improving Citizen Involvement' (ClientEarth 2013) 3 <https://www.clientearth.org/latest/documents/eu-enforcement-of-environmental-laws-from-great-principles-to-daily-practice-improving-citizen-involvement/> accessed 8 August 2023; Eliantonio (n 18) 756.

80 Commission, 'Enforcing EU law for a Europe that delivers' (n 79) 29.

81 Case C-50/00 P *Unión de Pequeños Agricultores v Council* [2002] ECR I-6677, Opinion of Advocate General Jacobs.

82 Stefan Thierse and Sanja Badanjak, 'Legal Mobilization Against the Data Retention Directive—Opportunity Structures, Actors and Strategies' in Stefan Thierse and

Advocate General Jacobs in the abovementioned opinion, if national courts err in their preliminary assessment of the validity of the EU acts, they can refuse to send a request for a preliminary ruling to the CJEU, leaving the applicant's claims entirely unaddressed.[83] Therefore, the preliminary reference procedure cannot be seen as a fully adequate means of bottom-up GDPR enforcement.

30 The primary reason why civil society actors have called upon national courts to send preliminary questions concerning the validity of EU acts to the CJEU despite the imperfections of this route is rooted in the extremely limited possibility for individuals and civil society organizations to challenge acts of the EU institutions with a direct action.[84] Per Article 263 TFEU, natural and legal persons can only institute proceedings against an act addressed to them or which is of direct and individual concern to them, or against a regulatory act (i.e. a non-legislative act of general application) which is of direct concern to them and does not entail implementing measures. Commission's implementing decisions under the GDPR fall into the category of "regulatory acts" which do not entail any implementing measures.[85] Even though it means that civil society actors are only required to demonstrate that the said act is of direct concern to them, they are likely to encounter serious obstacles when proving their standing. As explained by the CJEU, the requirement of a direct concern means that there should be a direct causal link between the act in question and the negative consequences suffered by the applicant.[86] In practice, it would be nearly impossible for civil society actors to obtain standing in actions for annulment of the Commission's implementing decisions since they do not have a direct adverse effect on them.[87] For instance, on 6 September 2023, the French parliamentarian Philippe Latombe brought an action for annulment of the Commission's adequacy decision relating to the EU-US Data Privacy Framework mentioned in section C.I.2.[88] According to Latombe, the decision violates, *inter alia*, Articles 7 and 8 of the Charter in view of the concerns regarding the "bulk" collection of personal data as well as Article 32 GDPR read in conjunction with Article 45(2) GDPR given the lack of safeguards concerning the security of personal data. However, the admissibility of this action remains highly uncertain since Latombe is expected to demonstrate which specific negative consequences were suffered by him due to the said adequacy decision.[89] Since civil society actors are precluded from engaging with the CJEU by bringing actions for annulment, the latter is unable to properly hear and consider their legal arguments, which could ultimately undermine effective judicial review of the Commission's implementing decisions and the protection of fundamental rights affected by them.

3. Limited possibility of third-party interventions in preliminary ruling proceedings

31 As demonstrated in section C.I, the preliminary reference procedure allows civil society actors to indirectly mobilize the CJEU to review the validity of the EU acts. However, these actors have significant interest not only in mobilizing courts of Member States to make them refer preliminary questions to the CJEU but also in participating in such proceedings as third parties. Third-party intervention – a robust mechanism of legal mobilization – allows civil society actors to advise courts on important legal aspects of the case or highlight its broader societal implications.[90]

32 Civil society actors eagerly venture to intervene in various, including high-profile, cases dealing with the interpretation and application of the protection of personal data before domestic courts of Member States.[91] Their submissions seek to

Sanja Badanjak (eds), *Opposition in the EU Multi-Level Polity : Legal Mobilization against the Data Retention Directive* (Springer International Publishing 2021).

83 P *Unión de Pequeños Agricultores v Council*, Opinion of Advocate General Jacobs (n 82) 6693.

84 Mariolina Eliantonio, 'Towards an Ever Dirtier Europe? The Restrictive Standing of Environmental NGOs before the European Courts and the Aarhus Convention' (2011) 7 Croatian Yearbook of European Law and Policy 69, 79.

85 Case T-262/10 *Microban International Ltd* [2011] ECLI:EU:T:2011:623, paras 21-25.

86 Joined Cases 41-44/70 *International Fruit Company BV v Commission* [1971] ECR 411.

87 Case T-600/15 *Pesticide Action Network Europe* [2016] ECLI:EU:T:2016:601, paras 55–62.

88 Action brought on 6 September 2023 – Latombe v Commission (Case T-553/23).

89 See, for example, Mikołaj Barczentewicz, 'Schrems III: Gauging the Validity of the GDPR Adequacy Decision for the United States' (International Center for Law & Economics Issue Brief 2023) 4 <https://laweconcenter.org/resources/schrems-iii-gauging-the-validity-of-the-gdpr-adequacy-decision-for-the-united-states/> accessed 12 February 2024.

90 Jasper Krommendijk and Kris van der Pas, 'To Intervene or Not to Intervene: Intervention before the Court of Justice of the European Union in Environmental and Migration Law' (2022) 26 The International Journal of Human Rights 1394, 1396–1397.

91 'Submission Filed by ORG and Privacy International in David Davis MP and Tom Watson MP v Secretary of State for the Home Department, CO Ref: CO/3794/2014' <https://www.openrightsgroup.org/publications/submission-filed-by-org-and-privacy-international-in-dripa-case/> accessed 9 August 2023; 'Amicus Curiae Submissions of the Co-

promote a more fundamental rights-inspired of the GDPR. For example, in its submission to the dispute between the Irish DPA, on the one hand, and Facebook Ireland and Max Schrems, on the other, the Electronic Privacy Information Center (EPIC) dealt with the issues of US privacy and surveillance law and the availability of legal remedies in the US for EU citizens, ultimately concluding that it did not provide adequate safeguards for personal data and private communications.[92] In some cases, civil society actors have also advocated a more restrictive interpretation of the GDPR with a view to ensure appropriate respect for other conflicting rights and legitimate interests at stake. For example, a wide range of NGOs submitted their observations in the dispute between Google and the French DPA CNIL before the Conseil d'Etat, arguing that the fundamental right to data protection should be properly balanced against freedom of expression.[93] The possibility of civil society actors to become parties to the dispute depends, however, on the national procedural rules in these Member States. As shown by Krommendijk and van der Pas, such rules differ significantly, with some Member States taking a rather strict approach to defining the circumstances under which third parties can intervene in the domestic court proceedings.[94] As a result, representatives of civil society do not enjoy equal opportunities to intervene in national disputes across Member States.

33 The third-party intervention of civil society actors in data protection cases could be of great value not only in proceedings before national courts of Member States but also in the preliminary reference proceedings before the CJEU. Having vast knowledge and expertise, such actors could provide the CJEU with helpful guidance on complex matters relating to the protection of personal data, thus contributing to a more nuanced, data subject-oriented interpretation of the GDPR. Furthermore, being involved in data protection litigation and advocacy "on the ground", NGOs and other similar entities could inform the CJEU of the challenges relating to the interpretation of the GDPR at the Member States level and propose effective ways of resolving them. Yet the possibility of representatives of civil society to intervene in the preliminary reference proceedings before the CJEU is extremely narrow. Section C.II.1 has already touched upon the mechanism of third-party interventions in infringement proceedings before the CJEU, noting that natural or legal persons are fully excluded from participating in them. In contrast, the intervention in the preliminary reference proceedings by NGOs is only possible where they have timely intervened in the proceedings before a national court of the Member State.[95] Should they miss the opportunity to intervene in the domestic proceedings, NGOs no longer have access to the preliminary reference proceedings once the case is pending before the CJEU. Per Article 23 of the Statute, the right to submit statements of case or written observations as third parties is reserved to the Member States, the Commission and, where appropriate, the EU institution, body, office or agency which adopted the act the validity or interpretation of which is at stake.

34 The restrictive rules on third-party interventions before the CJEU creates a situation in which civil society actors are once again fully dependent on the national courts' receptiveness towards motions to join the dispute as a third party. Given the lack of harmonized rules on the admission of intervening parties to proceedings before national courts of Member States, many of such actors may be ultimately precluded from participating in both domestic proceedings as well as the preliminary reference proceedings before the CJEU. Furthermore, when the possibility is foreseen by national law, some representatives of civil society can be simply unable to timely submit a request to join the dispute as a third-party to national courts to be able to engage with the CJEU. In this respect, enhancing the CJEU's responsiveness to third-party interventions in the preliminary reference proceedings could enable a greater range of civil society actors to submit their

Interveners Open RIghts Group and Privacy International, Dalma Dojcsak v Telenor Magyarország Zrt, Case Ref: III./537/2015' <https://www.openrightsgroup.org/app/uploads/2020/03/ORG_PI_Hungarian-Constitutional-Court-submissions_final.pdf> accessed 9 August 2023; 'En l'affaire N° 2023-850 DC Concernant La Constitutionnalité de La Loi Relative Aux Jeux Olympiques et Paralympiques de 2024 et Portant Diverses Autres Dispositions, Contribution Extérieure Commune de 7 Organisations Non-Gouvernementales Internationales et Étrangères' <https://files.inclo.net/content/pdf/84/amicus%20French%20OG.pdf> accessed 9 August 2023.

92 Electronic Privacy Information Center (EPIC), 'Amended Outline Submissions on Behalf of the Amicus Curiae (EPIC) in Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, Record No: 2016/4809P' <https://epic.org/wp-content/uploads/privacy/intl/schrems/02272017-EPIC-Amended-Submissions.pdf> accessed 9 August 2023.

93 See, among others, 'Written Observations of Internet Freedom Foundations and Others, Google LLC v Commission Nationale de l'Information et Des Libertés (CNIL)' <https://web.karisma.org.co/wp-content/uploads/download-manager-files/Google%20v%20CNIL%20Internet%20Freedom%20Foundation%20and%20other%20intervention%20brief%20(EN).pdf> accessed 9 August 2023; 'Written Observations of ARTICLE 19 and Others (2017), Google LLC v Commission Nationale de l'Information et Des Libertés (CNIL)' <https://www.article19.org/wp-content/uploads/2017/12/Google-v-CNIL-A19-intervention-EN-11-12-17-FINAL-v2.pdf> accessed 9 August 2023.

94 Krommendijk and van der Pas (n 91) 1406–1407.

95 Rules of Procedure of the Court of Justice, OJ L173, art 97.

written observations on important GDPR-related enquires, stimulating a more effective protection of fundamental rights in the digital domain.

D. Conclusion

35 This article has analysed the interplay between civil society actors and the CJEU in data protection cases. It has revealed that the role of these actors in the GDPR implementation stretches beyond the lodging of collective actions regarding the GDPR violations before national DPAs and national courts of the Member States since they also aspire to indirectly engage with the CJEU in preliminary reference cases. However, the opportunities for more direct interaction between civil society actors and the CJEU in cases concerning the protection of personal data remain severely constrained. Even though the CJEU has come to explicitly acknowledge the role of NGOs in tackling GDPR infringements by bringing legal actions on behalf of data subjects, the NGOs' involvement in the proceedings before the CJEU are extremely limited. Civil society actors, though essential for the Commission in their roles as complainants, are largely precluded from participating in infringement proceedings. They also do not have standing in actions for annulment of the Commission's acts, particularly implementing decisions relating to cross-border transfers of personal data, Additionally, civil society actors are often unable to intervene in preliminary reference proceedings dealing with data protection issues. The obstacles to the participation of civil society actors in the proceedings before the CJEU stand in stark contrast to the idea of the bottom-up GDPR enforcement and curtail the latter's ability to lend a sympathetic ear to these actors' claims. Therefore, it is necessary to empower civil society actors to mobilise the CJEU to both ensure the uniform and correct implementation of the GDPR and ensure an appropriate level of protection of other fundamental rights affected by the process of digitalization.

36 Enhancing a bottom-up approach to the GDPR enforcement by facilitating civil society actors' access to the proceedings before the CJEU should not be a single means of tackling the GDPR infringements. As rightly argued by Reiners and Versluis, the issue of non-compliance with EU law is complex and calls for both centralized and decentralized enforcement mechanisms.[96] In this respect, the Commission's recent proposal for a new regulation aimed to facilitate the cooperation between DPAs when enforcing GDPR in cross-border cases is welcome.[97] However, several steps can be taken in order to ensure that civil society actors can play a more prominent role in the proceedings before the CJEU. First, it would be necessary to enhance these actors' engagement in infringement procedure. This can be done – from the side of the Commission – by increasing transparency regarding the complaint process, so representatives of civil society, though unable to participate in the judicial proceedings, are at least made aware of the decision made on their complaint. Additionally, Article 40 of the Statute could be reconsidered so that civil society actors can participate in the infringement proceedings before the CJEU. As suggested by De Schutter, in order to overcome institutional constraints, the CJEU could also request a person or an entity which acted as a complainant to provide an expert opinion in line with Article 25 of the Statute.[98] Second, it would be beneficial if NGOs were granted standing to challenge the Commission's implementing decisions with a direct action. While the overhaul of Article 263 TFEU is rather unlikely, the CJEU could nevertheless soften its approach to the interpretation of the notion of "direct concern" in respect of civil society organizations. Finally, it is important to ensure that NGOs have a possibility to intervene in preliminary reference proceedings before the CJEU even after the request for a preliminary ruling has been submitted by a national court (and regardless of the national procedural rules applicable to third-party interventions) so as to promote a more robust and well-substantiated interpretation of the GDPR. In line with the suggestions made by Krommendijk and van der Pas, third-party interventions can be facilitated not only through the reform of the Statute but also through more informal means, such as by enabling natural and legal persons to provide the EU courts with factual and legal information relevant for the interpretation of certain provisions of EU law.[99] These measures are expected to pave the way towards a more profound interaction between the CJEU and civil society actors, enabling the former to be more receptive to the contentions made by the latter and ensuring greater protection to fundamental rights affected by the data-driven economy.

96 Reiners and Versluis (n 20) 1533.

97 Commission, Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679 [2023] COM/2023/348 final 2023.

98 De Schutter (n 76) 67.

99 Krommendijk and van der Pas (n 91) 1406.

Fundamental rights in CJEU data retention case law:

A refined regime in response to Member States' concerns, or compensating for the lack of legislative intervention in the digital age?

by **Evangelia Psychogiopoulou** *

Abstract: Data retention laws in the EU Member States entered a state of flux following Digital Rights Ireland and the annulment of Directive 2006/24/EC as a violation of the fundamental rights to respect for private life and the protection of personal data. For many Member States, it remained unclear what impact the invalidation of the directive should have on domestic data retention regimes. In subsequent case law, the CJEU sought to clarify the requirements deriving from EU law for national data retention legislation. While the CJEU has ruled that EU law in principle precludes national rules that prescribe a general and indiscriminate retention of traffic and location data by providers of electronic communications services and networks, it has also carved out exceptions that may justify interference with fundamental rights. Relevant cases have attracted much attention, with many national governments reaching out to the CJEU through observations submitted on what is admittedly a particularly complex and sensitive field of law. This article studies CJEU data retention case law and its evolution, examining the ways in which the CJEU has positioned itself vis-à-vis Member States' arguments on the balance to strike between fundamental rights' protection on the one hand and safeguarding national security and fighting (serious) crime on the other. The analysis shows how the CJEU has progressively refined and recalibrated its jurisprudence to acquiesce in part with Member States' demands. It also attests to the important role played by the CJEU in digital governance and the protection of fundamental rights in the absence of legislative intervention that addresses the particularities of the digital realm: the CJEU interprets the existing norms afresh, shaping the fundamental rights requirements applicable to Member States' data retention regimes.

Keywords: Court of Justice of the European Union (CJEU), data retention, access to data retained, fundamental rights, national security, combatting (serious) crime, e-Privacy Directive, e-Privacy Regulation, digital governance

Recommended citation: Evangelia Psychogiopoulou, Fundamental rights in CJEU data retention case law: A refined regime in response to Member States' concerns, or compensating for the lack of legislative intervention in the digital age?, 15 (2024) JIPITEC 194 para 1.

A. Introduction

1 The story of the European Union (EU)'s attempt to establish a data retention regime at the EU level has been well covered. Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services, or of public communications networks, sought to harmonize Member States' laws concerning the data retention obligations imposed on providers of electronic communications services and networks with a view to enabling access by the competent national authorities for the purpose of investigating, detecting and prosecuting serious crime.[1] In *Digital Rights*

* Assistant Professor, Department of Political Science and International Relations, University of the Peloponnese, e.psychogiopoulou@go.uop.gr; Senior Research Fellow, Hellenic Foundation for European and Foreign Policy, epsychogiopoulou@eliamep.gr. ORCID ID: 0000-0002-5326-6772

Ireland,[2] Directive 2006/24/EC was invalidated by the Court of Justice of the EU (CJEU) on the grounds that it breached Articles 7 and 8 of the Charter of Fundamental Rights (CFR) of the EU on the right to respect for private and family life and the right to protection of personal data, respectively.[3]

2 Directive 2006/24/EC was adopted after the enactment of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (the e-Privacy Directive).[4] The latter sought to harmonize Member States' laws in order to ensure an equivalent level of protection for privacy and personal data with regard to the processing of personal data in the electronic communications sector, translating the principles laid down with regard to the processing of personal data and the free movement of such data in what was then Directive 95/46/EC (the Data Protection Directive,[5] the predecessor to the General Data Protection Regulation – GDPR[6]) into specific rules for the electronic communications sector. *Inter alia*, the e-Privacy Directive established the principle of the *confidentiality of communications*, prohibiting the storing of traffic data without the consent of the user. However, it also allowed for certain derogations by Member States.[7] Directive 2006/24/EC reflected this: it sought to cope with the variation in national provisions concerning the retention of data specifically for the purpose of preventing, investigating, detecting and prosecuting criminal offences. As held by the CJEU, it did so in a manner that was not compliant with fundamental rights. In fact, Directive 2006/24/EC had several flaws.[8] Most importantly, the general and indiscriminate retention of data it envisaged was viewed as a particularly serious interference with fundamental rights, given that it was insufficiently circumscribed to ensure respect for the principle of proportionality.[9]

3 The CJEU declared Directive 2006/24/EC invalid as a result. Significantly, however, it neither outlawed data retention in general, nor addressed national legislation transposing Directive 2006/24/EC into Member States' national legal orders. National legislators could draw lessons from the CJEU ruling in *Digital Rights Ireland* regarding the compliance of rule-making with fundamental rights, but any privacy and data protection standards established by the CJEU in principle targeted only the EU legislator. This put domestic data retention regimes (enacted to transpose Directive 2006/24/EC but also adopted after its annulment) in a state of flux, which acted in turn as the catalyst for a wave of preliminary references made to the CJEU concerning national data retention laws and their compatibility with EU law, in the absence of EU secondary legislation on data retention. In this context, the focus has mostly been on the e-Privacy Directive in conjunction with general data protection law. Whereas the Data Protection Directive was intrinsically linked to the right to privacy,[10] the e-Privacy Directive states that national legislative measures regarding data retention should respect fundamental rights.[11] With the CFR acquiring binding legal effect with the Treaty of Lisbon,[12] references from national courts

1 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L 105/54 (no longer in force).

2 Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and others* ECLI:EU:C:2014:238.

3 Charter of Fundamental Rights of the European Union [2012] OJ C326/391.

4 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) [2002] OJ L 201/37.

5 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 L 281/31.

6 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 L 119/1.

7 See Article 15(1) of Directive 2002/58/EC.

8 Marie-Pierre Granger and Kristina Irion, 'The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection' (2014) 39 European Law Review 835; Federico Fabbrini, 'Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and its Lessons for Privacy and Surveillance in the U.S.' (2015) 28 Harvard Human Rights Journal 65; and Stefan Thierse and Sanja Badanjak, *Opposition in the EU Multi-Level Polity. Legal Mobilization against the Data Retention Directive* (2021 Palgrave Macmillan) 11, at 19.

9 See *Digital Rights Ireland*, paras 57-59 and 65.

10 See in particular recitals 2, 7, 9-11 and Article 1 of the Data Protection Directive.

11 According to Article 15 of the e-Privacy Directive, which was enacted before the CFR acquiring binding legal effect, any national measure concerning data retention should be in accordance with the general principles of EU law, including those referred to in Article 6(1) and (2) of the Treaty on European Union (TEU) and thus respect human rights and fundamental freedoms, which amounts to a general principle of the EU legal order. On this now see Art. 6(3) TEU [2012] OJ C326/13.

12 Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community

for a preliminary ruling increasingly revolved around compliance with the CFR provisions.

4 In its case law, the CJEU has sought to clarify the requirements deriving from EU law for national data retention rules. In *Tele2 Sverige*,[13] it ruled that EU law precludes national legislation that prescribes general and indiscriminate data retention.[14] However, in subsequent rulings, covering seminal cases like *Privacy International*, *La Quadrature du Net*, *Prokuratuur*, *Commissioner of An Garda Síochána* and *SpaceNet*,[15] it carved out exceptions that may justify interference with fundamental rights.[16] Relevant cases have attracted much attention, prompting national governments to submit observations, mostly arguing that the collection and analysis of electronic communications data by domestic authorities such as intelligence bodies and law enforcement services is an essential means for upholding national security and fighting serious crime. This article seeks to untangle the CJEU data retention case law by examining the ways in which the CJEU has positioned itself on Member States' claims and the balance to strike between fundamental rights' protection on the one hand and the public interest objectives advocated by Member States with regard to surveillance measures on the other. It shows that the CJEU has both sought to ensure a high level of protection of fundamental rights and taken Member States' concerns on board, providing some policy space for data retention measures at national level. The analysis starts with a discussion of key points in the CJEU's reasoning rejecting mass surveillance in *Tele2 Sverige* (section B). It then focuses on how the CJEU has treated the "national security card" played by Member States seeking to evade their fundamental rights obligations under the e-Privacy Directive vis-à-vis generalized surveillance (section C). The next section examines those CJEU pronouncements that create permissible exceptions for lawful surveillance at the national level in an attempt to respond to the desire of Member States to maintain (or introduce) data retention schemes (section D). What follows sheds light on the efforts of the CJEU to provide the Member States with more leeway, while at the same time setting forth substantive and procedural requirements (section E), which also take the form of safeguards for review by courts or independent administrative bodies (section F). The article then situates the CJEU's evolving case law in the context of the legislative reform of the e-Privacy Directive (section G), which has reached a standstill due to the conflicting views on the issue of data retention. It argues that against this backdrop of political (and legal) controversy, the CJEU's jurisprudence has a strong bearing on the rules and fundamental rights standards applicable to Member States' data retention schemes. The final section offers some concluding remarks on the CJEU's willingness to heed Member States' surveillance demands through its jurisprudence, and highlights the CJEU's crucial role in digital governance and the protection of fundamental rights in the digital age (section H).

B. Setting limitations on national legislation relating to data retention and access thereto: Rejecting mass surveillance

5 Two cases deriving from preliminary questions put by national courts in Sweden and the UK allowed the CJEU in *Tele2 Sverige* to provide guidance on the compatibility with EU law of domestic regimes on data retention and access thereto, ruling (and reiterating its stance in the wake of *Digital Rights Ireland*) on the non-permissibility of mass surveillance. Swedish legislation provided for the general and indiscriminate retention by providers of electronic communications services of the traffic and location data of all subscribers and registered users, with respect to every means of electronic communication, for the purpose of fighting crime. The UK legal rules at issue empowered the Secretary of State for the Home Department to adopt a general regime requiring public telecommunications operators to retain all data relating to any telecommunications service for a maximum period of 12 months, if it was deemed necessary and proportionate on grounds of national security or for the purpose of preventing or detecting crime or preventing disorder.

6 In reviewing the relevant legislation, the CJEU

[2007] OJ C 306/1.

13 Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* ECLI:EU:C:2016:970.

14 On bulk state surveillance, see Paul Bernal, 'Data Gathering, Surveillance and Human Rights: Recasting the Debate' (2016) 1(2) Journal of Cyber Policy 243; and Alena Birrer, Danya He, Natascha Just, 'The State is Watching You—A Cross-National Comparison of Data Retention in Europe (2023) 47(4) Telecommunications Policy.

15 See Case C-623/17 *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* ECLI:EU:C:2020:790; Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and others* ECLI:EU:C:2020:791; Case C-746/18 *Prokuratuur* ECLI:EU:C:2021:152; Case C-140/20 *Commissioner of An Garda Síochána* ECLI:EU:C:2022:258; and Joined Cases C-793/19 and C-794/19 *SpaceNet and Telekom Deutschland* ECLI:EU:C:2022:702.

16 On the CJJEU's evolving case law, see Adam Juszczak and Elisa Sason, 'Recalibrating Data Retention in the EU. The Jurisprudence of the CJEU – Is this the End or the Beginning?' (2021) 4 eucrim 238; Marcin Rojszczak, 'The Uncertain Future of Data Retention Laws in the EU: Is a Legislative Reset Possible?' (2021) 41(1) Computer Law & Security Report.

followed a two-pronged approach, distinguishing rules on data retention and rules on access to the data retained, considering these to be closely interrelated activities. Domestic legislation was assessed with reference to the e-Privacy Directive, which was interpreted in line with the CFR. The CJEU started its reasoning from the premise that, pursuant to Article 15(1) of the e-Privacy Directive, Member States could derogate from the principle of the confidentiality of communications laid down in Article 5(1) of the directive.[17] They could do so on a number of grounds, such as safeguarding national security (understood as state security), defence, public security and preventing, investigating, detecting and prosecuting criminal offences and the unauthorized use of electronic communications systems.[18] This list of objectives, the CJEU stated, was exhaustive. Member States should not depart from the confidentiality of communications on other grounds,[19] and any national measures derogating on the grounds set forth should respect fundamental rights,[20] and in particular the right to privacy (enshrined in Article 7 CFR), the right to protection of personal data (enshrined in Article 8 CFR) and the right to freedom of expression (enshrined in Article 11 CFR).[21]

7 The Swedish regime under review provided for the general and indiscriminate retention of traffic and location data, imposing on providers of electronic communications services an obligation to retain the data systematically and continuously, without exceptions.[22] The CJEU found that the data retained[23] enabled "very precise conclusions" to be drawn regarding the private lives of the persons concerned: their "everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the[ir] social relationships [...] and the social environments [they] frequented".[24] The "profile" of individuals could thus be established.[25] Against this background, the CJEU held that the ensuing interference with the fundamental rights of Articles 7 and 8 CFR was "very far reaching" and likely to make the persons concerned feel "under constant surveillance".[26] Moreover, although national legislation did not target the content of communication as such, it could affect the use of electronic communications and consequently the exercise of freedom of expression.[27]

8 Given such a "particularly serious" interference with fundamental rights, the CJEU ruled that only fighting *serious* crime (such as organised crime or terrorism) should be considered capable of justifying it.[28] However, while the effectiveness of the fight against serious crime could greatly depend on the use of "modern investigation techniques", such an objective of general interest could not in itself justify national legislation providing for the general and indiscriminate retention of all traffic and location data.[29] Indeed, the Swedish legislation imposed a general and indiscriminate data retention obligation with "no differentiation, limitation or exception",[30] it affected all persons using electronic communications services without requiring a link between their conduct and serious crime,[31] and contained no restrictions regarding the retention of data for a particular time period, geographical area or group of persons likely to be involved in serious crime.[32]

9 Importantly, the CJEU did not rule out data retention in general and affirmed that, interpreted in accordance with the CFR, Article 15(1) of the e-Privacy Directive did not preclude the *targeted* retention of traffic and location data as a preventive measure in the fight against serious crime. This meant that data retention should be limited to what is strictly necessary regarding the data categories to be retained, the means of communication affected, the persons concerned and the retention period adopted;[33] in addition, the CJEU offered guidance on how these proportionality requirements could be satisfied.[34]

10 Regarding access to the data retained by competent national authorities, an issue of relevance for both the Swedish and UK legislation under review, the

17 See *Tele2 Sverige*, para. 85.
18 Ibid, para. 90.
19 Ibid.
20 Ibid, para. 91.
21 Ibid, para. 93.
22 Ibid, para. 97.
23 The retained data made it possible to trace and identify the source of a communication and its destination, the date, time, duration and type of a communication, the users' communication equipment and the location of mobile communication equipment. They also included data such as the name and address of the subscriber or registered user, the telephone number of the caller, the number called and the IP address for internet services, and enabled the identification of the person with whom a subscriber or registered user had communicated, the relevant means and time of communication, the place from which communication had taken place and its frequency. See ibid, para. 98.
24 Ibid, para. 99.
25 Ibid.
26 Ibid, para. 100.
27 Ibid, para. 101.
28 Ibid, paras 100, 102-103.
29 Ibid, 103.
30 Ibid, para. 105.
31 Ibid.
32 Ibid, para. 106.
33 Ibid, para. 108.
34 Ibid, paras 109-111and 115-116.

CJEU followed the same rationale, considering only the objective of fighting *serious* crime capable of justifying the seriousness of the interference at hand.[35] To ensure respect for the principle of proportionality,[36] the national legislator should determine substantive and procedural conditions governing access to the retained data.[37] Taking note of the jurisprudence of the European Court of Human Rights (ECtHR) in this respect,[38] the CJEU held vis-a-vis substantive conditions that national authorities should only be granted access to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in serious crime,[39] though in particular situations where vital national interests are threatened (e.g. by terrorism), access can also be granted to other persons' data if there is objective evidence that the data can effectively contribute to combating the detected threats.[40] Concerning procedural requirements, the CJEU required prior review by a court or an independent administrative body (except in cases of validly established urgency[41]) and the notification of the persons affected, once the notification no longer jeopardizes the investigations undertaken.[42] It also cautioned against risks of misuse and unlawful access: providers of electronic communications services should guarantee a particularly high level of protection for the retained data, and national legislatures should ensure that the data is retained within the Union and irreversibly destroyed at the end of the retention period.[43] Whether the Swedish and UK laws satisfied such requirements was left to the referring courts to determine.

11 *Tele2 Sverige* reflects the CJEU's efforts to establish a fundamental rights-compliant framework for examining the compatibility of national data retention laws with the e-Privacy Directive. It is also important for having clarified that national legislation on both data retention and access to the retained data comes within the scope of the e-Privacy Directive. Member States which submitted written observations to the CJEU had different views on this. Whereas the Belgian, Danish, German, Estonian and Dutch governments argued in the affirmative, the UK government claimed that only legislation relating to data retention should fall within the scope of the directive.[44] Crucially, the Czech government advanced the argument that national legislation whose aim is to combat crime should not come within the scope of the directive at all.[45]

12 Determining the scope of application of the e-Privacy Directive was indeed a contentious issue, since the directive proclaims in Article 1(3) that "activities of the state" in the fields of public security, defence, state security and criminal law are excluded from its scope.[46] According to the CJEU, legislative measures derogating from the principle of the confidentiality of communications should not be deemed to be activities within the scope of Article 1(3) of the directive, as this would have deprived Article 15(1) of the e-Privacy Directive of its very *raison d'être*.[47] By enabling derogation from the principle of the confidentiality of communications, Article 15(1) of the directive necessarily presupposed that the national measures it authorized fell within the scope of the directive.[48] As both data retention and access to the retained data involved the processing of data,[49] the CJEU concluded that the e-Privacy Directive covered national measures on both.

C. Clarifying the scope of application of the e-Privacy Directive

13 In Tele2 *Sverige*, the CJEU rejected mass surveillance and unambiguously brought data retention and access thereof within the scope of EU law, despite the fact that secondary EU law on data retention no longer existed. *Ministerio Fiscal* confirmed the applicability of the e-Privacy Directive, interpreted in accordance with the CFR, with reference to domestic legislation in Spain which allowed the police to seek judicial authorization to access the subscriber data retained by providers of electronic communications services in connection with a criminal investigation.[50] In *Privacy International*,

35 Ibid, para. 115.
36 Ibid, paras 116 and 118.
37 Ibid, para. 118.
38 See ECtHR, 4 December 2015, *Zakharov v. Russia*, CE:ECHR:2015:1204JUD004714306.
39 See *Tele2 Sverige*, para. 119.
40 Ibid.
41 Ibid, para. 120.
42 Ibid, para. 121.
43 Ibid, para. 122.
44 Ibid.
45 Ibid, para. 65.
46 Ibid, para. 69.
47 Ibid, paras 72-73.
48 Ibid.
49 Ibid, paras 75 and 78.
50 In *Ministerio Fiscal*, the Spanish government, supported by the UK government, argued to no avail that the request for access to the data at issue on the grounds of a judicial decision in connection with a criminal investigation, fell within national authorities' exercise of *jus puniendi*, which constituted an activity of the State in the area of criminal law and therefore fell under the exception provided for in Article 1(3) of Directive 2002/58/EC (along with the exception laid down in the first indent of Article 3(2) of Directive 95/46/EC concerning *inter alia* processing operations on grounds of public security, defence, State

the CJEU reiterated the applicability of EU law, countering arguments put by Member States seeking to evade their obligations under the e-Privacy Directive, this time on national security grounds.

14 This case originated in proceedings between Privacy International, a non-governmental organisation, and public authorities in the UK concerning the legality of domestic legislation enabling the acquisition and use of bulk communications data by the country's security and intelligence agencies for the purpose of safeguarding national security. According to the referring court, the databases compiled by these agencies, which should be as comprehensive as possible, sought to identify unknown threats to national security and were essential in the fields of counter-terrorism, counter-espionage and counter-nuclear proliferation.[51] Accordingly, the issue for the referring court was whether national legislation fell within the scope of the e-Privacy Directive, given that pursuant to Article 4(2) of the Treaty on European Union (TEU) and Article 1(3) of the e-Privacy Directive, national security remains a responsibility of the Member States.

15 The UK, Czech, Estonian, Irish, French, Cypriot, Hungarian, Polish and Swedish governments argued, through observations, against the application of the e-Privacy Directive. They claimed that the purpose of the national legislation at issue was to safeguard national security and that the activities of the security and intelligence agencies, as essential state functions relating to the maintenance of law and order and safeguarding national security and territorial integrity, were the sole responsibility of Member States in line with Article 4(2) TEU.[52] Also, by means of Article 1(3), the e-Privacy Directive expressly excluded from its scope activities concerning public security, defence and state security, meaning that national measures in those fields were not required to meet its requirements.[53]

16 The CJEU rebuffed these arguments. The disclosure of bulk communications data amounted to processing of personal data by providers of electronic communications services,[54] and *all* processing carried out by such providers should be seen as falling within the scope of the e-Privacy Directive, including processing which results from obligations imposed by public authorities.[55] Article 4(2) TEU did not alter this. In the CJEU's view, only measures *directly implemented* by Member States in the fields of Article 4(2) TEU (i.e. without the imposition of data processing obligations on private operators) should be seen as falling outside the scope of the e-Privacy Directive.[56]

17 By endorsing such a narrow interpretation of Article 4(2) TEU, leaving "very little outside the scope of EU law",[57] the CJEU brought national measures on national security within the scope of the e-Privacy Directive (and its own jurisdiction[58]) and further developed the line of reasoning it adopted in *Tele2 Sverige*: a general and indiscriminate transfer of traffic and location data, and thus bulk access to traffic and location data, for the purpose of safeguarding national security was not congruent with EU law.[59] Still, the CJEU did acknowledge the importance of safeguarding national security which, as noted, went beyond that of the other public interest objectives referred to in Article 15(1) of the e-Privacy Directive, such as combating crime or safeguarding public security, and could therefore justify measures entailing more serious interference with fundamental rights.[60] The primary interest vis-à-vis state security, the CJEU explained, lay in protecting the "essential functions of the State and the fundamental interests of society", encompassing "the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities".[61] Nevertheless, the UK legislation exceeded the limits of what was strictly necessary, pursuant to Article 15(1) of the e-Privacy Directive interpreted in line with the CFR.[62] In particular, it did not rely on objective criteria to define the circumstances and conditions under which domestic authorities were to be granted access to the data concerned.[63]

security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law. See Case C-207/16 *Ministerio Fiscal* ECLI:EU:C:2018:788, paras 29-30.

51 See *Privacy International*, paras 25 and 29.

52 Ibid, para. 32.

53 Ibid, para. 33.

54 Ibid, para. 41.

55 Ibid, paras 44 and 46.

56 Ibid, para. 48.

57 Iain Cameron, 'Metadata Retention and National Security: Privacy International and La Quadrature du Net' (2021) Common Market Law Review 1433, at 1458.

58 On the CJEU asserting authority over national security with Privacy International, see Monika Zalnieriute, 'A Struggle for Competence: National Security, Surveillance and the Scope of EU Law at the Court of Justice of European Union' (2021) 85(1) The Modern Law Review 198.

59 See *Privacy International*, paras 80-81.

60 Ibid, para. 75.

61 Ibid, para. 74.

62 Ibid, para. 81.

63 Ibid, para. 76.

D. Carving out exceptions for national legislative measures

18 *Tele2 Sverige* and *Privacy International* made it clear that data processing for the purpose of combatting (serious) crime and safeguarding national security comes within the scope of the e-Privacy Directive and is generally prohibited. However, while it did rule in *Privacy International* that national measures adopted with the aim of protecting national security are still subject to EU law, the CJEU appeared to provide Member States with some leeway for surveillance by underscoring the importance of national security as a public interest objective that may justify particularly intrusive interference in the exercise of fundamental rights, subject to strict proportionality constraints. In *La Quadrature du Net*, which originated in two references for a preliminary ruling by the French Council of State and the Belgian Constitutional Court respectively, the CJEU, in response to Member States' wanting to uphold data retention schemes, took steps to *qualify* their powers in doing so by carving out specific exceptions according to different sets of public interest objectives pursued at the national level. Each of these public interest objectives was judged capable by the CJEU of justifying distinct data retention activities in terms of their nature, breadth and ultimately seriousness in terms of interference with CFR rights.[64] Thus, in adjusting its position, the CJEU distinguished between measures concerning national security, measures designed to combat serious crime and prevent serious threats to or attacks on public security, and measures to combat less serious crime and attacks on public security. Underlying the CJEU's reasoning was the recognition, which chimes with the ECtHR jurisprudence, that besides *negative obligations* of non-interference, *positive obligations* to secure the *effective* enjoyment of fundamental rights may also derive from the CFR, in particular Article 3 on the right to the integrity of a person, Article 4 on the prohibition of torture and inhuman or degrading treatment or punishment and Article 7 CFR on the right to respect for family and private life.[65]

I. The case for national security

19 Adopting reasoning akin to that in *Privacy International*, the CJEU first confirmed that the more far-reaching permissible exception is the one which relates to the safeguarding of *national security*.[66] The CJEU ruled that national legislation which allows an order mandating general and indiscriminate data retention by providers of electronic communications services is compatible with the e-Privacy Directive, on condition that: there are sufficiently solid grounds for considering that the Member State concerned is confronted with a serious threat to national security, which is genuine, present or foreseeable;[67] the data retention takes place for a limited period of time[68] (which can, however, be extended if the serious threat persists[69]); the data retention is not systematic[70] and is subject to limitations and strict safeguards against the risk of abuse;[71] and that provision is made for effective review by a court or independent administrative body with a view to verifying that all the necessary conditions and safeguards are actually observed.[72]

20 Importantly, the CJEU also accepted that intelligence gathering techniques enabling automated analysis and the real-time collection of traffic and location data can also be justified on national security grounds. The automated analysis at issue took the form of providers screening all the traffic and location data retained at the request of domestic authorities with a view to verifying correspondence matching certain parameters set by the latter.[73] This, the CJEU held, entailed a general and indiscriminate processing of the data of persons using electronic communications services,[74] which amounted to a particularly serious interference with CFR rights. For such measures to be justified, Member States should be facing a serious threat to national security which is shown to be genuine, present or foreseeable; the retention period should be limited;[75] and any authorizing decision should be subject to effective review by a court or independent administrative body.[76] Regarding the screening parameters used, the CJEU stated that these should be specific and reliable, making it possible to identify individuals who might be under a reasonable suspicion of participation in terrorist offences;[77] that they should be non-discriminatory; that they should not be based solely on data such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or information about a person's health or sex life;

64 Valsamis Mitsilegas, Elspeth Guild, Elif Kuskonmas, Niovi Vavoula, 'Data Retention and the Future of Large-Scale Surveillance: The Evolution and Contestation of Judicial Benchmarks' (2023) 29 European Law Review 176.

65 See *La Quadrature du Net*, paras 126 and 128.

66 Ibid, para. 136.

67 Ibid, para. 137.

68 Ibid.

69 Ibid, para 138.

70 Ibid.

71 Ibid.

72 Ibid, para. 139.

73 Ibid, para. 172.

74 Ibid, para. 174.

75 Ibid, para. 177.

76 Ibid, para. 179.

77 Ibid, para. 180.

and that they should be re-examined on a regular basis.[78] The CJEU added that any positive matches should be subject to an individual re-examination by non-automated means before the person concerned becomes adversely affected by a subsequent measure such as the real-time collection of his/her traffic and location data.[79]

21 Concerning the latter, the CJEU observed that it should only be authorized individually for a person previously identified as potentially having links to a terrorist threat and persons in the same circle. The real-time collection of traffic and location data, the CJEU explained, is particularly intrusive, given that it provides a means of accurately and permanently tracking the movements of mobile telephone users.[80] Such an interference could only be justified in respect of persons for whom "there is a valid reason to suspect that they are involved in one way or another in terrorist activities".[81] An authorization decision should thus be based on objective and non-discriminatory criteria[82] and be subject to prior review carried out by a court or an independent administrative body.[83] Moreover, the competent national authorities should notify the persons concerned, provided that the notification does not jeopardize their tasks.[84]

II. The case for combatting serious crime (and serious attacks on public security)

22 Regarding data retention measures taken in respect of the second level in the hierarchy of objectives, namely *combatting serious crime and preventing serious threats or serious attacks on public security*, the CJEU asserted, in light of *Tele2 Sverige*, that compliance with any positive obligations deriving from Articles 3, 4 and 7 CFR should not translate into legislation giving the green light to the general and indiscriminate retention of traffic and location data without differentiation, limitations or exceptions,[85] and without the requirement of a link between the data of the persons concerned and the objective pursued.[86] This line of reasoning was confirmed in *Prokuratuur*, in reference to Estonian legislation enabling law enforcement authorities to gain *access* to traffic and location data which related to fixed and mobile telephone services and had been generally and indiscriminately retained. In *La Quadrature du Net*, the CJEU found that compliance with positive obligations under Articles 3, 4 and 7 CFR permitted *targeted* data retention for the purpose of combatting serious crime and preventing serious threats or attacks on public security (and *a fortiori*, national security),[87] with proportionality safeguards set for the data categories to be retained, the means of communication affected, the persons concerned and the retention period.[88]

23 As several governments pointed to the difficulties surrounding the detection of offences committed online, especially child pornography,[89] the CJEU also accepted the compatibility with the e-Privacy Directive, read in the light of Articles 7, 8 and 11 CFR, of legislative measures providing for the general and indiscriminate retention of *IP addresses* with a view to combatting serious crime and preventing serious threats to public security (along with national security), subject to conditions.[90] The fact that IP addresses relate to the *source of connection* (and not to the recipient of communication) was deemed by the CJEU to make them less sensitive than other traffic data, on the grounds that no information is disclosed about the third parties with which communication is made.[91] Nonetheless, the ensuing interference with the CFR rights was considered to be serious, given that the IP addresses can reveal a user's clickstream and thus the user's entire online activity.[92] This led the CJEU to stress the importance of requirements limiting the retention period and substantive and procedural conditions restricting the uses to which the data are put.[93]

24 Noting that it might prove necessary to retain data beyond the time period laid down in domestic legislation for legitimate purposes (for instance, for marketing and billing communication services or for purposes under Article 15(1) of the e-Privacy Directive), the CJEU also recognized that Member States may provide for the *expedited* retention of traffic and location data (also known as *quick freeze*), for a specified period of time and subject to effective judicial review, in order to fight serious crime (and attacks on national security).[94] To comply with the principle of proportionality, the retention obligation, the CJEU held, should only relate to traffic and location data that may shed light on serious

78 Ibid, paras 180-181.
79 Ibid, para. 182.
80 Ibid, para. 187
81 Ibid, para. 188.
82 Ibid, para. 189.
83 Ibid.
84 Ibid, para. 190.
85 Ibid, para. 143.
86 Ibid, para. 145.
87 Ibid, para. 146.
88 Ibid, para. 147.
89 Ibid, para. 154.
90 Ibid, paras 155-156.
91 Ibid, para. 152.
92 Ibid, para. 153.
93 Ibid, paras 155-156.
94 Ibid, paras 161 and 163-164.

criminal offences or acts adversely affecting national security, while the retention period should be limited to what is strictly necessary, although an extension should be possible where the circumstances and objective pursued justify it.[95] Notably, the CJEU ruled that the expedited data retention need not be limited to the data of persons suspected or having committed a criminal offence (or acts adversely affecting national security); it can also cover the data of victims and their social or professional circle, and data concerning specified geographical areas such as the place where the offence or act at issue was committed or prepared.[96] The CJEU also clarified that the public interest objective that guides *access* to the retained traffic and location data should be the same as the public interest objective justifying the *retention* of data.[97] However, it should be possible to access, on national security grounds, data originally retained to fight serious crime.[98] Contrariwise, access to data whose retention was justified by the objectives of combatting serious crime or safeguarding national security should not be granted for the purpose of prosecuting and punishing ordinary crime.[99]

III. The case for combatting ordinary crime (and safeguarding public security)

25 In *La Quadrature du Net*, the third level of public interest objectives reviewed, namely the objective of preventing, investigating, detecting and prosecuting criminal offences and safeguarding public security, was found capable of justifying only legislative measures concerning the general and indiscriminate retention of data relating to the civil identity of users of electronic communications systems, namely their addresses.[100] As such data only allows for the users' identification, without disclosing any information concerning the communications made and thus the users' private lives,[101] the CJEU held that its retention constitutes a 'non-serious interference' with the rights safeguarded in Articles 7 and 8 CFR[102] and can thus be accepted, even without a specific time limit.[103]

95 Ibid.
96 Ibid, para. 165.
97 Ibid, para. 166.
98 Ibid.
99 Ibid.
100 Ibid, paras 158-159.
101 Ibid, para. 157.
102 Ibid.
103 Ibid, para. 159.

E. Refining the exceptions for national legislative measures

26 In more recent case law, the CJEU has not departed from this graduated approach whereby specific public interest objectives justify particular data retention activities. In *VD*,[104] for instance, in which the CJEU dealt with French legislation providing for the general and indiscriminate retention of traffic data for one year, the CJEU confirmed that the public interest objective of fighting common crime, that is crime which does not qualify as "serious" (here, market abuse offences), cannot justify it.

27 In *Commissioner of An Garda Síochána*, which stemmed from domestic proceedings concerning the validity of Irish data retention legislation, the CJEU reiterated, in the light of *La Quadrature du Net*, that Article 15(1) of the e-Privacy Directive, interpreted in line with the CFR, allows legislative measures that enable, for the purpose of safeguarding national security, a general and indiscriminate retention of traffic and location data, as long as the Member State concerned is confronted with a serious threat to national security which is genuine and present or foreseeable, coupled with other conditions. However, criminal behaviour, even of a particularly serious nature, should not be treated in the same way as a threat to national security.[105]

28 The CJEU thus discarded claims put forward by Ireland and France that serious crime cannot be combatted effectively in the absence of a general and indiscriminate data retention.[106] It also refused arguments advanced by the Danish government that the competent national authorities should be able to access, for the purpose of fighting serious crime, traffic and location data retained in a general and indiscriminate way to address a serious threat to national security that is genuine and present or foreseeable. In the light of the hierarchy of public interest objectives outlined in CJEU judgments, access to the retained data should in principle be justified by the same public interest objective for which the data retention was ordered, unless the importance of the public interest objective pursued through access is greater than that of the objective justifying the retention of data.[107] As a result, authorizing access for the purpose of fighting serious crime (the second-level public interest objective envisaged) to traffic and location data retained in order to safeguard national security (the first-level public interest objective identified)

104 CJEU, Joined Cases C-339/20 and C-397/20 *VD* ECLI:EU:C:2022:703.
105 See *Commissioner of An Garda Síochána*, para. 63.
106 Ibid, para. 68.
107 Ibid, para. 98.

would be contrary to the classification of public interest objectives made.[108] This is arguably a more constrained interpretation than the one provided in *La Quadrature du Net*, where the CJEU appeared to accept that access to traffic and location data for the purpose of combatting serious crime *or* safeguarding national security is allowed on condition that the data is generally considered to have been retained in a manner compatible with the e-Privacy Directive.[109] In *Spacenet*, which focused on the conformity of data retention legislation in Germany with EU law, the CJEU employed the exact same reasoning it applied in *Commissioner of An Garda Síochána*, and stated, in response to similar arguments made by the Danish government, that only when access to the retained data is in pursuit of an objective whose importance is greater (i.e. safeguarding national security) than the one for which the data was retained (e.g. fighting serious crime) can the public interest objective pursued by data retention and access to the retained data differ.[110]

29 *In Commissioner of An Garda Síochána*, however, the CJEU took steps to explain in more detail and to codify lawful forms of data retention, shedding more light on the permissible exceptions allowing data retention for combatting serious crime and preventing serious threats on public security (and by default, safeguarding national security, as this constitutes the highest public interest objective in the scaling system established). The list of measures that Member States can lawfully adopt in pursuit of these public interest objectives – which, as stressed by the CJEU, can also be combined and applied concurrently[111] – covers: a) the *targeted retention* of traffic and location data, which is limited on the basis of objective and non-discriminatory factors regarding the categories of persons concerned, or by geographical criterion, for a period that respects what is strictly necessary (which can, however, be extended); b) the general and indiscriminate retention of *IP addresses* assigned to the source of an internet connection for a limited period; c) the *expedited retention* of traffic and location data lawfully possessed by service providers for a specified period by means of the decision of a competent authority subject to effective judicial review;[112] and d) the general and indiscriminate retention of data relating to the *civil identity of users* of electronic communications systems. Relevant measures must all ensure, by means of clear and precise rules, that the retention of data is subject to compliance with the applicable substantive and procedural conditions, and that the persons concerned have effective safeguards against risks of abuse.[113] The same list of measures under the rubric of combatting serious crime, preventing serious threats to public security and *a fortiori* safeguarding national security was also sanctioned in *Spacenet*.

30 Notably, *Commissioner of An Garda Síochána* offered additional guidance on some of these exceptions, refining their characteristics and scope. The CJEU explained, for instance, that the *targeted retention* of traffic and location data does not require that the persons suspected of being involved in an act of serious crime be known in advance.[114] It can also pertain to persons who are the subject of an investigation or other surveillance measures, or who are referred to in the national criminal record in relation to an earlier conviction for serious crimes and as highly likely to re-offend.[115] In a similar vein, the CJEU declared that, in the case of a geographical criterion being used to indicate a high risk of the preparation or commission of a serious crime, the areas covered can include places with a high incidence of serious crime, as well as places which are particularly vulnerable to serious crime, such as places with a high volume of visitors or places in strategic locations (i.e. airports, stations, maritime ports, tollbooth areas, etc.),[116] with Member States being able to use the average crime rate in a geographical area as a relevant criterion.[117] Offering more room for manoeuvre, the CJEU also held that non-personal or geographical criteria can be considered by Member States, as long as they are objective, non-discriminatory and help establish a connection, even of an indirect nature, between serious crime and the persons whose data are retained.[118]

31 Along the same lines, the CJEU ruled that there is no requirement for an *expedited retention* of data to be limited to suspects identified in advance.[119] A national legislative measure may thus provide for the expedited retention of the traffic and location data of persons with whom a victim was in contact prior to a serious threat to public security arising or a serious crime being committed.[120] An expedited retention of data may also extend to specific geographic areas related to the commission of or preparation for the offence or attack in question,[121] a place or a person, including the victim of a serious crime

108 Ibid, para. 99.
109 See *La Quadrature du Net*, para. 167.
110 See *SpaceNet*, paras 128-130.
111 See *Commissioner of An Garda Síochána*, para. 92.
112 Ibid, para. 67.
113 Ibid, paras. 67 and 92
114 Ibid, para. 75.
115 Ibid, para. 78.
116 Ibid, para. 79.
117 Ibid, para. 80.
118 Ibid, para. 83.
119 Ibid, para. 75.
120 Ibid, para. 89.
121 Ibid, para. 90

who has disappeared,[122] and can be ordered when domestic authorities begin an investigation into a serious threat to public security or a possible serious crime.[123] As for the retention of data relating to the *civil identity of users* of electronic communications systems, the CJEU accepted that Member States may enact legislation for the purpose of combatting serious crime which makes the purchase of a means of electronic communication, such as a pre-paid SIM card, subject to the purchaser's identity being checked and that information being registered, with the seller being required, should the case arise, to give the competent national authorities access to that information.[124]

32 The CJEU may have provided some extra policy space for Member States' data retention measures, but this did not eradicate the legal constraints on the latter stemming from EU law. Thus, in *Spacenet*, the CJEU did not accept the German government's argument that the data retention obligation at issue amounted to targeted retention.[125] Here, the referring court had raised doubts about the incompatibility of domestic data retention legislation with EU law, given that the data retention obligation concerned a relatively short period of time and a smaller amount of data[126] which excluded the content of communications along with data relating to the visited websites, data from electronic mail services and data concerning communications of a social or religious nature in the form of telephone assistance provided to people in distress. According to the CJEU, regardless of the length of the retention period and the quantity or nature of the data retained, the German legislation mandated the general retention of what remained a "very broad set of traffic and location data" which practically covered the entire population, without providing a reason and without drawing any distinction in terms of personal, temporal or geographical factors.[127] Such data provided the means for drawing "very precise conclusions" concerning the private lives of the persons concerned[128] (e.g. their everyday habits, their permanent or temporary places of residence, their daily or other movements, the activities they carried out, their social relationships and the social environments frequented),[129] and therefore for establishing their profile.[130] For the CJEU, the safeguards built into the legal framework to protect the retained data against risks of abuse and unlawful access could not remedy the serious interference resulting from the generalized data retention at issue.

F. Review by courts and independent administrative bodies

33 In its case law, the CJEU has also consistently held that data retention activities and access thereof shall be made dependent, as a general rule, on review by a court or an independent administrative body, mandating *prior r*eview (as opposed to *ex post* review) in certain instances. In *Prokuratuur*, the CJEU took steps to clarify the requirements for such a review, particularly from the perspective of the independence of the body entrusted with oversight duties. The Estonian legislation under dispute conferred upon the public prosecutor's office the power to authorize public authorities to access traffic and location data for the purposes of a criminal investigation. The CJEU ascertained that in the context of criminal investigations, such prior review should be entrusted to a court or body that is able to strike a fair balance between the needs of the investigation and combatting crime on the one hand, and the fundamental rights to privacy and protection of personal data on the other. This should essentially translate into a status which enables objective and impartial action, is free of external influence, and is thus a third party.[131] In the case at hand, the independence requirement was not satisfied: the investigation procedure was directed by the public prosecutor's office, which also conducted the public prosecution; it did not therefore have a neutral stance vis-à-vis the parties.[132] The CJEU employed similar reasoning in subsequent rulings. In *Commissioner of An Garda Síochána*, for instance, it held that national legislation which assigned a police officer the power to centrally process requests for

122 Ibid.

123 Ibid, para. 91.

124 Ibid, para. 71.

125 See *Spacenet*, para. 84.

126 In the context of the provision of telephone services, the retention obligation laid down covered, *inter alia*, the data required to identify the source of a communication and its destination, the date and time of the start and end of the communication or – in the case of communication by SMS, multimedia message or similar message – the time of dispatch and receipt of the message and, in the case of mobile use, the designation of the cell sites used by the caller and the recipient at the start of the communication. In the context of the provision of internet access services, the retention obligation covered, *inter alia*, the IP address assigned to the subscriber, the date and time of the start and end of the internet use from the assigned IP address and, in the case of mobile use, the designation of the cell sites used at the beginning of the internet connection. The data enabling the identification of the geographical location and the directions of maximum radiation of the antennas serving the cell site in question were also retained.

127 See *Spacenet*, paras 81-83.

128 Ibid, paras 87-88.

129 Ibid, para. 90.

130 Ibid, para. 87.

131 See *Prokuratuur*, paras 53-54.

132 Ibid, para. 54.

access to data by police services for the investigation or prosecution of serious criminal offences did not fulfil the requirements for independence.[133] This was so, despite the police officer being assisted by a police unit with a certain degree of autonomy, and the fact that the decisions issued could be subject to judicial review.[134]

34 Clearly then, a body external to the authority seeking access to the retained data is necessary and should be made responsible for determining the lawfulness of the interference with the CFR rights deriving from access to the data. The independence requirement thus entails that administrative bodies embedded in the law enforcement and security hierarchy cannot constitute lawful oversight authorities. Importantly, the court or administrative body entrusted with the task of review should have all the necessary powers and provide all the guarantees required to reconcile the various interests and rights in question.[135] This implies that it has the capacity to carry out an *effective examination* of whether the surveillance measure at issue is justified, which extends to assessment of whether a situation justifying that measure exists and whether the various conditions and safeguards that must be laid down in domestic legislation are being observed.[136]

35 In the light of the CJEU's case law to date, external and independent control is required of any requirement placed on providers of electronic communications services: a) to retain, generally and indiscriminately, traffic and location data[137] and to provide access to such data;[138] b) to undertake, for a specified period of time, the expedited retention of traffic and location data;[139] c) to carry out automated analysis of traffic and location data;[140] and d) to engage in real-time collection of traffic and location data.[141] *Prior* review by a court or independent administrative body is essential in the case of automated analysis,[142] in the case of the real-time collection of traffic and location data,[143] and regarding access to data generally and indiscriminately retained.[144]

133 See *Commissioner of An Garda Síochána*, para. 111.
134 Ibid, paras 111-112.
135 See *Prokuratuur*, para. 52.
136 On this see *La Quadrature du Net*, paras 139 and 168.
137 See *Commissioner of An Garda Síochána*, para. 58.
138 Ibid, para. 106.
139 Ibid, paras 67 and 86. See also *La Quadrature du Net*, para. 168.
140 See *La Quadrature du Net*, paras 179 and 192.
141 Ibid, paras 189 and 192.
142 Ibid, paras 179 and 192.
143 Ibid, paras 189 and 192.
144 See *Prokuratuur*, paras 50-51 and *La Quadrature du Net*, para. 106.

G. Data retention case law and the CJEU's role in the digital age

36 CJEU case law on the legal constraints on Member States' data retention regimes deriving from EU law reflects a clear effort by the CJEU to strike a balance between the different rights and interests involved. In light of the arguments presented by Member States in favour of upholding data retention regimes at the national level, the CJEU has progressively refined and recalibrated its jurisprudence to acquiesce in part with the Member States' demands. This shows a somewhat receptive court – that is, one that is willing to accept and assuage Member States' concerns by recognizing that certain forms of data retention and access thereof can still be regulated at the national level. However, it also reflects a court that is willing to solve the legal problems brought to its attention through novel rule-interpretation that clarifies and elaborates on how a norm should be interpreted henceforth so as to address the challenges posed by digitalisation and concurrently uphold fundamental rights. This has to be seen in the light of the difficulties the EU legislator has keeping pace with technological developments and updating the legislative framework established by the e-Privacy Directive, while at the same time refraining from using the legislative process to *legalize* mass data retention at the national level to the detriment of fundamental rights.

37 When the European Commission (Commission) published its proposal in January 2017 for an e-Privacy Regulation to replace the e-Privacy Directive in light of the broad range of internet-based services enabling inter-personal communication, beyond traditional communication services, it did not deviate from the approach followed by Article 15 of the e-Privacy Directive. It confirmed that legislative measures on data retention that pursue public interest objectives should remain possible *under conditions*,[145] and declared that the principle

145 See Article 11(1) of the Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 final, according to which "Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 5 to 8 where such a restriction respects the essence of the fundamental rights and freedoms and is a necessary, appropriate and proportionate measure in a democratic society to safeguard one or more of the general public interests referred to in Article 23(1)(a) to (e) of Regulation (EU) 2016/679 or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests."

of confidentiality should apply to various means of communication, including "calls, internet access, instant messaging applications, e-mail, internet phone calls and personal messaging provided through social media".[146] However, when the Council agreed on the scope of its mandate to negotiate the e-Privacy Regulation with the European Parliament on 10 February 2021 after four years of stalled discussions between the Member States, it included data retention and diverted from CJEU case law.

38 The Council's mandate is as follows: Article 2(2)(a) and (d) respectively exclude from the scope of the Regulation "processing activities and operations concerning national security and defence, regardless of who is carrying out those activities whether it is a public authority or a private operator acting at the request of a public authority" and "activities, including data processing activities, of competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security".[147] Recital 26 then affirms that the e-Privacy Regulation "should not affect the ability of Member States to carry out lawful interception of electronic communications, including by requiring providers to enable and assist competent authorities in carrying out lawful interceptions, or take other measures, such as legislative measures providing for the retention of data for a limited period of time", if this is necessary and proportionate to "safeguard specific public interests, including public security and the prevention, investigation, detection or prosecution of criminal offences, or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and other important objectives of general public interest".[148] More conspicuously, Article 7(4) states that "Union or Member State law may provide that the electronic communications metadata is retained, including under any retention measure that respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society, in order to safeguard the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the safeguarding against and the prevention of threats to public security, for a limited period", adding that "[t]he duration of the retention may be extended if threats to public security of the Union or of a Member State persist".[149]

39 Rules of this sort are not in line with CJEU case law.[150] They water down the safeguards and conditions crafted by the CJEU and give the Member States *carte blanche* to retain data by creating a concrete legal basis for it. Clearly, the institutional preferences of the Council differ from those of the European Parliament, which is keen to keep data retention as an exception and to not make it the rule.[151] It should thus come as no surprise that negotiations between the two institutions have reached a political stalemate.[152] While trilogues are reported to have begun on 20 May 2021, the legislative file stagnated under the Swedish Council Presidency (1/1/2023-30/6/2023),[153] while the subsequent Spanish (1/7/2023-31/12/2023) and Belgian Council Presidencies (1/1/2024-30/6/2024) did not consider the conclusion of the negotiations a priority.[154] This

146 Ibid, Recital 1.

147 See Council of the EU, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Mandate for negotiations with EP, 6087/21, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6087_2021_INIT&from=EN.

148 Ibid.

149 Ibid. Article 6(1)(d) of the Council's mandate adds that providers of electronic communications networks and services should be permitted to process electronic communications data if it is necessary *inter alia* to comply with "a legal obligation to which the provider is subject laid down by Union or Member State law, which respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the safeguarding against and the prevention of threats to public security."

150 See Marcin Rojszczak (n 16); Maria Tzanou and Spyridoula Karyda, 'Privacy International and Quadrature du Net: One Step Forward Two Steps Back in the Data Retention Saga?' (2022) 28(1) European Public Law 123; and Gavin Robinson, 'Targeted Retention of Communications Metadata: Future-Proofing the Fight Against Serious Crime in Europe?' (2023) 8(2) European Papers 713.

151 Committee on Civil Liberties, Justice and Home Affairs, Report on the proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 20.10.2017, Rapporteur: Marju Lauristin, https://www.europarl.europa.eu/doceo/document/A-8-2017-0324_EN.html.

152 See European Parliament, Legislative Train Schedule, Proposal for a regulation on privacy and electronic communications in "A Europe Fit for the Digital Age", https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-jd-e-privacy-reform.

153 Ibid.

154 See EU23, Programme, Spanish Presidency of the Council of the European Union, Second half of 2023, Europe, closer, https://spanish-presidency.consilium.europa.eu/media/

is also the case with the current Hungarian Council Presidency (1/7/2024-31/12/2024).[155]

40 In such a context of political (and legal) deadlock, the CJEU's case law has a strong bearing on the rules and standards applicable to Member States' data retention schemes. Through its case law, the CJEU revisits the interpretation of long-established norms at EU level, creating new understandings that seek to cater for the challenges posed by digitalisation and the proliferation of communication services online, in the light of Member States' concerns in pursuit of public interest objectives and the need to safeguard fundamental rights. From this perspective, the CJEU assumes a key role in digital governance and the protection of fundamental rights in the digital era: faced with the needs brought into being by the digital realm, coupled with the inertia of the EU legislator, the CJEU jurisprudence *adapts* EU law and *shapes* the fundamental rights requirements it sets for Member States' data retention regimes – inevitably on a case-by-case basis. This confirms arguments in the literature about courts (European courts in particular) having assumed a crucial role in addressing the challenges of the digital age through rule-interpretation that responds to present-day conditions and also compensates for the absence of legislative reform.[156]

H. Conclusion

41 CJEU case law on the legal constraints deriving from EU law for Member States' data retention regimes has been growing following *Digital Rights Ireland* and the annulment, on fundamental rights grounds, of Directive 2006/24/EC, which sought to harmonize Member States' laws concerning the data retention obligations of providers of electronic communications services and networks with a view to combatting serious crime. In a gradually evolving line of rulings, the CJEU has positioned itself, in what is admittedly a particularly complex field of law, on Member States' surveillance schemes and practices in pursuit of public interest objectives ranging from protecting national security and fighting terrorism to detecting and investigating crime. Relevant case law reflects a clear effort by the CJEU to strike a balance between the distinct rights and interests involved. In light of Member States' fervent arguments in favour of upholding data retention regimes at the national level, the CJEU has progressively refined and recalibrated its jurisprudence to acquiesce in part with Member States' demands. The CJEU held at an early stage that national data retention schemes are not beyond the reach of EU law and that Member States cannot escape their fundamental rights obligations by outsourcing data retention obligations to private operators that are required to provide access thereof to security, intelligence, law enforcement and other domestic authorities.[157] At the same time, the CJEU accepted early on that there is no absolute prohibition on data retention and that derogation from the confidentiality of communications is not unthinkable. Since then, finding itself in the delicate position of having to secure fundamental rights on the one hand and cope with Member States' sensitivities on the other, it has taken steps to create some room for state manoeuvre, while considering data retention and access to the retained data as separate interferences with the exercise of fundamental rights which must be justified separately.

42 Cases like *Privacy International*, *La Quadrature du Net* and *Commissioner of An Garda Síochána* show the CJEU's willingness to recognize Member States' concerns by taking the view that they can still regulate certain forms of data retention and access thereof at the national level. The CJEU's responsiveness to Member States' calls for some leeway to be found for preserving national data retention schemes has gone hand in hand with graduation, respect for the principle of proportionality and keeping true to the basic rule that data retention should be the exception and not the rule in a democratic society, given the dissuasive effect it can have on the exercise of fundamental rights.[158] As regards the public

e4ujaagg/the-spanish-presidency-programme.pdf; and beEU, belgium24.eu, Programme, Belgian Presidency of the Council of the European Union, First half of 2024, https://belgian-presidency.consilium.europa.eu/media/3kajw1io/programme_en.pdf.

155 HU24EU, Programme of the Hungarian Presidency of the Council of the European Union in the Second Half of 2024, https://hungarian-presidency.consilium.europa.eu/media/32nhoe0p/programme-and-priorities-of-the-hungarian-presidency.pdf.

156 On the role of courts in the digital age, see Evangelia Psychogiopoulou and Susana de la Sierra, 'European Supranational Courts and Judicial Decision-Making in the Era of Digitalisation', in Evangelia Psychogiopoulou and Susana de la Sierra (eds), *Digital Media Governance and Supranational Courts. Selected Issues and Insights from the European Judiciary* (2022 Edward Elgar Publishing) 1; and Giovanni de Gregorio and Oreste Pollicino, 'Courts, Rights and Powers in the Digital Age', in Federica Casarosa and Evangelia Psychogiopoulou (eds), *Social Media, Fundamental Rights and Courts. A European Perspective* (2023 Routledge) 242.

157 On the private sector assuming tasks of generalized and indiscriminate data retention and the ensuing public-private surveillance partnership, see Valsamis Mitsilegas, 'The Privatisation of Surveillance in the Digital Age', in Valsamis Mitsilegas and Niovi Vavoula (eds.), *Surveillance and Privacy in the Digital Age: European, Transatlantic and Global Perspectives* (2021 Hart Publishing) 101.

158 See *Tele2 Sverige*, para. 104.

interest objectives in particular that may justify data retention (and access to the data retained), it is clear from the CJEU's jurisprudence that in accordance with the principle of proportionality, a hierarchy exists which accords with the importance of the public interest objective to be attained, and that the seriousness of the interference introduced by the national surveillance measure must be proportionate to the importance of the public interest objective at issue. This means that each public interest objective permits different data retention activities based on the degree of seriousness of the specific threats, which also has implications for access to the data retained. Thus, the CJEU has ruled that the importance of the objective of safeguarding national security, read in the light of Article 4(2) TEU according to which national security remains the sole responsibility of Member States, supersedes that of the objectives of combatting crime – even serious crime[159] – and of safeguarding public security.[160] The objective of safeguarding national security is therefore capable of justifying measures entailing more serious interferences with fundamental rights, such as general and indiscriminate data retention, automated analysis of personal data and real-time collection of traffic and location data, subject to stringent conditions and independent oversight.

43 Overall, the CJEU's jurisprudence contains several key pronouncements concerning national surveillance measures, and has evolved to take on board national governments' concerns whilst elaborating protective standards for upholding fundamental rights. Along with the CJEU's readiness to adapt its case law in order to reach a compromise and give consideration to Member States' stated desire for data retention schemes at the national level, the system of requirements created exemplifies the CJEU's crucial role in digital governance and the protection of fundamental rights in the digital age. Indeed, the evolution of the CJEU's case law must be viewed in the light of the failure of the EU legislator to come up with a meaningful update to the e-Privacy Directive dating back to 2002, and thereby to keep pace with the development of electronic communications services and, importantly, do so in a fundamental rights-compliant way, without risking any downgrading of the protection afforded to fundamental rights. In such a context of political tension and legislative uncertainty, with inter-institutional negotiations on the e-Privacy Regulation essentially blocked, the CJEU offers some kind of solution to the data retention impasse. This lies in defining standards for fundamental rights protection pragmatically, on a case-by-case basis, without ignoring Member States' concerns relating to the pursuit of public interest objectives. Seen in this light, through its case law, the CJEU *creates* and *remoulds* understandings of the checks and balances that should accompany national schemes for and practices of data retention, and thus provides some direction where the EU legislator – having failed to date to modernize the e-Privacy legal regime in the digital economy – does not.

159 Note however that in certain instances, it can prove challenging to distinguish serious forms of criminality from threats to national security. On this, see Gavin Robinson (n 150), at 723 and Iain Cameron (n 57), at 1462-1463.

160 See *La Quadrature du Net*, para. 136.

jipitec

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

www.jipitec.eu