jipitec

4 | 2023

Volume 14(2023)
Issue 4 ISSN 2190-3387

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

www.jipitec.eu

2023

jipitec

Journal of Intellectual Property, Information Technology and Electronic Commerce Law

Volume 14 Issue 4 February 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 **Thomas Dreier**

Recommended citation: Thomas Dreier, Editorial, 14 (2023) JIPITEC 498 para 1.

1 When JIPITEC was founded some fifteen years ago, the coverage of the new double-blind peer-reviewed open access journal was still quite clearly defined with intellectual property law, IT law and e-commerce law. In the course of the following years, however, IT law in particular has expanded in a way that was previously hardly thought possible. Data protection law has experienced a considerable increase in importance, while a largely independent data law has also emerged, which reflects nothing other than the new business models in relation to the generation, trade and utilisation of data. Last but not least, research in the field of artificial intelligence, which has rapidly gained momentum in recent years, has significantly expanded the legal issues associated with IT.

2 As a result, following on from the previous issues, which were dedicated entirely or at least in part to a single topic, the present issue 14 (4) of JIPITEC, once again brings together a colourful mix of articles on a wide variety of topics, each of which has its own unique topical relevance. In view of their variety, these articles have been arranged in the order of the topics listed in the journal's name.

3 To begin with, in intellectual property law, two articles focus on the scope of copyright limitations and exceptions. Whereas *Löbling/Schwedhelm/Handschigl/Hofmann* examine to what extent ChatGPT's use of someone else's copyrighted works as training data can be justified by the European text and data mining exceptions, *da Silva Pereira* focusses on the balancing of author's rights and acts undertaken for textual scholarship as seen from a Portuguese perspective. Moreover, *Kalenský* draws the readers' attention to what happened to digital exhaustion a decade after the famous UsedSoft-case. Finally, the contribution by *Samaranayake* examines the relationship between trademark law and NFTs also, but not exclusively, from a Sri Lankan perspective.

4 Regarding IT law, *Schulz/Ollig* focus on new hybrid approaches to govern social media platforms under the European Digital Services Act. Following, *van Daalen* undertakes to construe a „right to root", i.e. to construct a claim to control devices on the basis of the right to privacy. Thereafter *Broumas/Charalampous* cast an eye on the general regulation of emerging technologies as undertaken in Greek law. Following, *Gorbatyuk/Gils* examine to what extent blockchain technology can be used to enable and improve the transparency of patent transactions.

5 The last contribution to the present issue is a cautionary perspective by *Melian Pérez* on the viability of artificial intelligence as a replacement of judges and the courts.

Karlsruhe, January 2024 Thomas Dreier

Navigating the Legal Landscape:

Technical Implementation of Copyright Reservations for Text and Data Mining in the Era of AI Language Models

by **Lisa Löbling, Christian Handschigl, Kai Hofmann and Jan Schwedhelm ***

Abstract: The profound advancements in AI-driven language models, exemplified by ChatGPT, owe their existence to vast quantities of text and data utilized in their training. However, the origins of this data and its suitability for training AI models raise considerations in the domain of Text and Data Mining (TDM) and its associated copyright requirements.

European and German regulation provide an opt-out system for TDM: Freely available works may be used for TDM if they have not been reserved by the rightsholder. A reservation of use is effective only if it is made in a machine-readable format. On the one hand, state-of-the-art language models use large amounts of text data from different domains. On the other hand, no (de facto) standard for reservations of use has yet been established. In this paper, we will therefore

- discuss the legal requirements,
- give an insight into how usage reservations are dealt with in practice and
- suggest a possible standard.

Keywords: Copyright Law, Text and Data Mining (TDM), Artificial Intelligence (AI), Data Indexing and Crawling Restrictions, Machine-Readable Standard

Recommended citation: Lisa Löbling, Christian Handschigl, Kai Hofmann and Jan Schwedhelm, Different Navigating the Legal Landscape: Technical Implementation of Copyright Reservations for Text and Data Mining in the Era of AI Language Models, 14 (2023) JIPITEC 499 para 1.

A. Introduction

1 Text and data mining (TDM) is the process of using software to automatically analyze collections of text and data to extract information and compile insights. It has become increasingly important in recent years, as the amount of digital information available is growing exponentially.[1] Alongside simple rule-based and statistical methods, TDM also entails the application of advanced algorithms and computational techniques, specifically drawn from the field of natural language processing (NLP), to identify patterns, relationships, and trends in unstructured data like text documents. This can be, e.g., journal articles, scientific papers, press releases, social media posts, and books.

* Dr. Lisa Löbling, Senior Consultant at d-fine, lisa.loebling@d-fine.com

Christian Handschigl, Web Specialist & Consultant at abnorm media, christian@abnorm.de

Dr. Kai Hofmann, Scientific Desk Officer Law at the German Centre for Rail Traffic Research, hofmannk@dzsf.bund.de

Jan Schwedhelm, Consultant at d-fine, jan.schwedhelm@d-fine.com

1 David Reinsel, John Gantz and John Rydning, 'Data Age 2025: The Evolution of Data to Life-Critical' (International Data Corporation 2017) <https://www.seagate.com/files/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf> accessed 17.01.2024.

2 After the initial step of defining the business goal or research question and the identification of relevant data that aligns with the use case, the process of TDM unfolds as follows: TDM starts with obtaining and preparing the source material from various digital (or non-digital) sources, making it machine-readable, normalizing, structuring, categorizing, and converting it into suitable technical formats. The processed source data forms a corpus, which is then automatically analyzed using specialized software or scripts to uncover statistical frequencies or correlations within the datasets. The inclusion of annotations, which are metadata accompanying normalized and structured content, varies based on the corpus and research focus. Training machine learning algorithms to uncover hidden patterns and correlations is also considered part of TDM, requiring the preparation of training data for self-learning systems, while the quality of the processed source data significantly impacts the knowledge gained through TDM.[2]

3 In practice, TDM serves as a powerful approach to gain valuable insights from vast volumes of data across diverse fields. Today, the most prominent tool in this domain is ChatGPT, a sophisticated language model developed by OpenAI.[3] ChatGPT has garnered attention for its ability to generate human-like responses and engage in interactive conversations, making it a valuable asset for applications such as chatbots, virtual assistants, and customer support systems. The model has undergone extensive training with vast and diverse text data from various domains. The inclusion of this substantial amount of known content during training plays a crucial role in enabling the chatbot to deliver convincing and innovative responses. In addition to its attention-grabbing applications, TDM is also employed for fundamental tasks, such as extracting entities (e.g., organizations, people, places, and events) from text, identifying sentiment and emotions, and classifying texts into different categories or topics.[4]

4 TDM encompasses a range of techniques, from rule-based analysis (e.g., regular expressions) via feature-based machine learning (e.g., linear regression, support vector machines, or random forests) to representation learning (e.g., GPT-3, BERT, and variants). When selecting a model, various factors need consideration – in any case the quantity and quality of training data significantly impact the model's accuracy and effectiveness. Thus, collecting relevant data for training NLP models plays a central role in TDM projects.

5 To perform TDM, the source material is initially duplicated and organized into a corpus for subsequent analysis. This source material may be subject to copyright protection, such as literary works (Art. 2 lit. a Directive 2001/29/EC, Art. 2 Berne Convention, Section 2(1) no. 1 UrhG[5]), significant parts of databases (Art. 7 Directive 96/6/EC) or press publications (Art. 15 Directive [EU] 2019/790). The extent of protection is contingent on specific conditions, resulting in typically partial protection of the material. However, since prerequisites such as "intellectual creation"[6] (relating to Art. 2 lit. a Directive 2001/29/EC) or "substantial investment" (Art. 7 Directive 96/6/EC) cannot be checked automatically, in practice one must assume that the material is protected.

6 TDM, in principle, requires permission from the copyright holder to proceed lawfully. Some websites and platforms acknowledge this aspect and offer Application Programming Interfaces (APIs) that enable developers to programmatically access data.[7] These APIs often facilitate complex query commands for downloading targeted information in large quantities. Moreover, APIs can be utilized to manage access rights for data collection, as they permit data owners to restrict access to specific datasets and define the level of access granted to each user by distributing individual access tokens. APIs are purposefully designed for efficient, controlled, and structured information exchange, making them a preferable option from a copyright perspective. Nevertheless, setting up an API is not practically useful for many websites since it does not align with the goal and use cases that focus on providing information for human users rather than prioritizing structured data access.

7 Thus, other methods for TDM are more commonly used like web scraping, which enables the retrieval of information from websites and data collections. This technique involves utilizing software to extract data from the HTML code of a website and converting it into a structured format suitable for

2 Thomas Dreier, § 44b UrhG, in Thomas Dreier and Gernot Schulze, Urheberrechtsgesetz (7th edn, CH Beck 2022) no 5.

3 OpenAI, 'Introducing ChatGPT', <https://openai.com/blog/chatgpt> accessed 17.01.2024.

4 Daniel Jurafsky and James H Martin, *Speech and Language Processing: An Introduction to Natural Language Processing, Computational Linguistics, and Speech Recognition* (2008).

5 German Act on Copyright and Related Rights [Urheberrechtsgesetz]

6 ECJ, ECLI:EU:C:2018:899, no. 37 et seq., see also Section 2(2) UrhG.

7 For example, X/Twitter provides a developer API that allows for programmatic access to public X/Twitter data. See <https://developer.twitter.com/en/docs> accessed 17.01.2024.

analysis with NLP methods. Web scraping has gained popularity, as it enables users from various domains, including business and science, to efficiently gather data that would otherwise be time-consuming or impractical to collect manually. Unlike APIs, web scraping does not rely on access explicitly designed for TDM purposes. Instead, this method leverages the statutory exception from copyright protection provided by Art. 4 Directive (EU) 2019/790, making it particularly relevant for this type of mining.

B. Copyright exception for TDM

8 According to the general copyright exception for TDM in Art. 4 Directive (EU) 2019/790 – and its national transposition, for German law in Section 44b UrhG, it is permitted to reproduce lawfully accessible works and other subject matters in order to carry out TDM – regardless of the purpose of the TDM. Copies are to be deleted when they are no longer needed to carry out text and data mining, Art. 4(2) Directive (EU) 2019/790.

9 The TDM exception applies to all sorts of material protected by copyright or related rights. The only prerequisite is that the material is lawfully accessible. However, the TDM user does not have to check whether the works were made accessible with the consent of the rightsholder; instead, what matters is whether the TDM user has lawful access to the source where the material is found.[8]

10 Lawfully accessible means that the TDM user himself must be able to access the material, in the case of screen scraping by crawling the web (see Section C). This is why the TDM exception does not apply to user-generated content. If an end user of a TDM-based applications (e.g., ChatGPT or DeepL) enters third-party copyrighted material into this application, it is the responsibility of the end user to ensure that the usage of such material complies with relevant legal provisions. The application provider, on the other hand, is not allowed to use this material from this source for TDM – at least not by referring to the TDM in exception in Art. 4 Directive (EU) 2019/790. If the application provider wants to include user generated content in the training of its algorithms, he must establish mechanisms[9] to refrain from utilising content for TDM for which the rightsholders have not granted authorization. However, this issue does not fall within the scope of the TDM exception.

8 Thomas Dreier, § 44b UrhG, in Thomas Dreier and Gernot Schulze, *Urheberrechtsgesetz* (7th edn, CH Beck 2022) no 8.

9 The technical approach of C2PA (see Section E.I) is heading in this direction of law enforcement.

I. Opt-out

11 The most important limitation of the exception for TDM is set out in Section Art. 4(3) Directive (EU) 2019/790: The copyright holder may reserve the use of their copyrighted material for TDM purposes. Consequently, the general TDM exception does not apply when such a reservation has been made. Under these circumstances, utilization of the copyrighted material for TDM requires explicit permission from the copyright holder, who has the discretion to either prohibit TDM use entirely or make it subject to conditions such as remuneration.

12 This opt-out approach is at the core of the TDM regulation. The process of opting out entails distinct responsibilities for both the TDM user and the copyright holder:

- The TDM user bears the onus of proof, mandated by the phrasing of paragraph 3 ("are permitted only if they have not been reserved").[10] Thus, the user is required to substantiate that the copyright holder has not opted out, necessitating active searches for and documentation of relevant opt-outs.

- Conversely, the copyright holder is accountable for properly expressing their opt-out decision. While this stipulation derives from Article 4(3) of Directive (EU) 2019/790 ("on condition that the [...] has not been expressly reserved by their rightholders in an appropriate manner"). The copyright holder assumes the risk associated with the adequacy of their chosen method to communicate the opt-out.

13 In essence, the TDM user needs only to seek opt-outs that have been appropriately conveyed. The determination of appropriateness hinges on contextual factors, encompassing how the copyrighted material is made accessible and the degree of effort required for the TDM user to verify opt-outs. Consequently, a limited set of requirements can be generalized, such as ensuring opt-outs are articulated clearly and positioned where users are likely to encounter them. Furthermore, a reservation's impact is prospective[11]; if altered subsequently, reproductions already completed remain legal within the boundaries defined Art. 4(1) Directive (EU) 2019/790. Therefore, opt-outs need

10 Benjamin Raue, 'Die Freistellung von Datenanalysen Durch Die Neuen Text Und Data Mining-Schranken (§§ 44b, 60d UrhG)' [2021] Zeitschrift für Urheber- und Medienrecht 793, 797.

11 'Explanatory Memorandum of Section 44b UrhG' 89 <https://dserver.bundestag.de/btd/19/274/1927426.pdf> accessed 17.01.2024.

only be assessed when initiating new reproductions.

II. Machine-readable opt-out, i.e. machine-interpretable opt-out

14 If the content has been made publicly available *online*, the law sets out more specific requirements. In such instances, the copyright holder must express their opt-out through "machine-readable means" (Article 4[3] Directive [EU] 2019/790) or in a "machine-readable format" (Section 44b[3] UrhG), which essentially convey the same intent. If these conditions are not met, the opt-out is deemed ineffective.

15 Through the stipulation of machine-readability, the legislator clarifies the appropriate manner for conveying opt-outs in an online context. This distribution of risk between the copyright holder and the TDM user leads to the responsibility of the latter to identify potential opt-outs. If they are discovered to lack machine-readability, it disadvantages the copyright holder, rendering the opt-out ineffective.

16 Notably, the law does not furnish a precise definition of "machine-readable". Recital 18 of the directive (EU) 2019/790 only states "... it should only be considered appropriate to reserve those rights by the use of machine-readable means, *including* metadata and terms of a website or a service." This raises a seeming contradiction, as the machine-readability of a website's terms of use is uncertain. The explanatory memorandum to the German law tries to resolve this contradiction, as it mentions the terms of use of a website only in the context of *where* to express the opt-out, but not *how* to express it: "It can also be included in the imprint or in the terms [...], *provided that* it is machine-readable there, too."[12] Although still quite unclear, this explanation at least prioritizes machine-readability. If the copyright holder expresses the opt-out in the terms of use of the website, it is effective – if it is also machine-readable.

17 In the absence of a precise definition, the term "machine-readable" is to be understood functionally. As German explanatory memorandum to the law emphasises machine-readable means must be "suitable for automated processes of text and data mining [of online accessible sources]" because "[...] the purpose of the regulation is to ensure that automated processes, which are typical criteria of text and data mining, can actually be automated in the case of content accessible online".[13] Mere discoverability and automatic legibility of the opt-out are insufficient. Machines must also be capable of interpreting the opt-out in alignment with this perspective, rendering "machine-readable" tantamount to "machine-interpretable."[14] Therefore, an opt-out in only plain text (see C) or as a pictogram[15] is most likely not legally effective.

III. Which side is responsible for proposing a machine-readable standard?

18 The distribution of responsibility within the TDM exception presumes the feasibility for rights holders to reasonably express opt-outs. Within the online environment, it specifically assumes the availability of machine-readable formats accessible to TDM users. However, the opt-out approach encounters limitations when this assumption doesn't hold. The TDM exception does not address the question of who assumes the risk in situations where established standards are absent.

19 The opt-out approach of the TDM exception is very similar to the case law on thumbnails.[16] In this context, too, an opt-out solution was established: individuals who provide text or image content freely on the internet without technically feasible restrictions should anticipate customary usage

12 ibid.: „auch im Impressum oder in den [AGB] [...], sofern er auch dort maschinenlesbar ist."

13 ibid.: „in einer Weise erfolgen, die den automatisierten Abläufen beim Text und Data Mining angemessen ist"; „[...] bezweckt die Regelung, bei online zugänglichen Inhalten sicherzustellen, dass automatisierte Abläufe, die typisches Kriterium des Text und Data Mining sind, tatsächlich auch automatisiert durchgeführt werden können."

14 Winfried Bullinger in: Artur-Axel Wandtke and Winfried Bullinger (eds), *Praxiskommentar Urheberrecht* (6th edn, CH Beck 2022) § 44b UrhG no. 10. („detected and analyzed", german:„erkannt und ausgewertet"); Raue (n 10) 797; Marco Müller-ter Jung and Lewin Rexin, 'Rechtliche Anforderungen an Intelligentes Und Automatisiertes Technologiescouting Technische Umsetzung Unter Beachtung Urheberrechtlicher Und Datenschutzrechtlicher Hürden' Computer und Recht 174 (both only mention: "detected", german: "erkannt").

15 Björn Steinrötter and Lina Marie Schauer however consider plain text and pictograms (also) as maschine-readable, in: Marek Barudi (ed), *Das Neue Urheberrecht* (1st edn, Nomos 2021) § 44b UrhG no 14.

16 BGH 29.04.2010 - I ZR 69/08, openJur 2010, 528 (thumbnails I); 19.10.2011 - I ZR 140/10, openJur 2012, 659 (thumbnails II).

under prevailing circumstances. This may lead a search engine to interpret that the rights holder has consented to the use involving works' reproductions in thumbnails.[17]

20 The ('missing') opt-out within the TDM exception can be treated as an expression of consent. It adheres to the principles of the declaration of intent and is primarily interpreted from the recipient's standpoint. In situations of uncertainty, this recipient is the objective third party, i.e., a person possessing the knowledge expected in the relevant context. Their understanding is significantly shaped by customary practices in comparable scenarios. When customs are absent, no consent is inferred. The fundamental premise remains that TDM infringes copyright and thus constitutes an unlawful act. In situations lacking established norms, the TDM user faces a disadvantage. Nonetheless, the rightsholder must still communicate the opt-out, Article 4[3] Directive [EU] 2019/790 is clear on that. In such instances, any reasonable form of opt-out would be effective. The TDM user cannot contest that the rights holder did not use a machine-readable format.

21 This outcome aligns with the underlying notion in Section 31 (5) UrhG, which stipulates that, in cases of uncertainty, usage rights are granted only if they are essential to fulfilling contractual obligations. In scenarios where usage rights are likely to remain with the author[18], it is coherent that rights holders also tend to withhold consent.

22 Finally, the question arises at what level of dissemination machine-readable formats are to be considered common, prompting rights holders to use them to ensure an effective opt-out through compliance with a commonly accepted machine-interpretable format (see. B.II). A standardization body governing web crawling does not exist. The current "standards" (see D) have been shaped over time by Google's influence within the online sphere. The legislator's intention was to not wait for this normative influence to manifest, as this would render the TDM exception regulation redundant. Thus, it must suffice that practical machine-readable formats are extensively discussed, even if they have not yet become firmly established in practice.

C. Empirical analysis on possibilities to declare opt-outs

23 To comprehensively evaluate feasible procedures with reasonable effort for both copyright holders and TDM users to declare or to search for opt-outs, we perform an empirical test to analyze viable methods based on a current sample of websites. Our aim is to understand the practicability and exertion involved in identifying potential opt-outs. Ideally, copyright holders utilize established syntax, an aspect elaborated in the subsequent section addressing search engine standards (Section D). This segment focuses on the detectability of different standards and the evaluation of the machine-readability of the website's terms of use, aligning with Recital 18 of Directive (EU) 2019/790.

24 The process of searching for an opt-out within the terms of use page involves several steps:

- Identifying the webpage displaying the website's terms of use.
- Locating the pertinent section within the webpage.
- Interpreting the identified section as an opt-out for TDM

25 We conducted an analysis on a sample of 100 websites using a subset extracted from the latest crawl of the Common Crawl[19] archive (May/June 2023). The dataset holds petabytes of data accumulated since 2008, encompassing raw website data, extracted metadata, and textual content. Given the expansive nature of the Common Crawl dataset, which negates the requirement for individualized web crawlers, it emerges as a popular resource in TDM studies, offering both efficiency and comprehensive coverage. Prominent models such as OpenAI's GPT-3 have benefited from Common Crawl during their training, underscoring the dataset's significance in advancing the state-of-the-art in natural language processing.

26 Our sample comprised European domains that feature English versions, chosen to reflect the overall distribution of European web top-level domains within the Common Crawl dataset. For instance, out of the 100 websites sampled, 20 were German, 9 French, and 1 Portuguese, among others. However, of this number, only 85 were found to be valid for our study. The exclusions were due to different reasons: first and foremost, due to the fact that they had become inaccessible at the time of our analysis. For the valid sites, we proceeded with the steps as described.

17 BGH thumbnails I, no. 35 et seq.

18 Gernot Schulze, § 31 in Dreier and Schulze (n 8) n 110.

19 The Common Crawl Foundation, a Californian non-profit organization, was established with the mission of democratizing access to web information. Their vision embodies an "open" web that facilitates free access to information, laying the groundwork for innovation in research, business, and education.

27 1.) The terms of use page can be systematically identified by detecting distinct patterns or elements within the HTML code or URL. Standard HTML text elements within the terms of use segment, containing phrases such as "terms and conditions," "terms of use," or "terms of service," can serve as keywords for identifying matching content within HTML. This process, however, has inherent limitations, as some websites may utilize unconventional terminology or phrasing, leading to challenges in precisely identifying the desired section. For 12 websites, the page containing the terms of use was automatically identified utilizing the described methodology. However, limitations arose from the potential omission of specific pages of a website in individual monthly crawls by Common Crawl. Through manual investigation, a section containing the terms of use could be identified for 40 websites. This indicates that only about half of all websites are likely to contain such a section.

28 2.) To identify the pertinent section within the terms of use webpage, a keyword-based approach similar to step 1 was followed. Identifying particular sections of interest within a webpage, such as opt-outs in terms of use, poses considerable challenges when relying solely on keyword matching. This is because the phrasing and structure of such content can vary widely across websites, with synonyms, domain-specific terminologies, and varying language nuances.[20] For all the 12 websites where the terms of use were automatically detected in step 1, basic keyword searches either missed sections of interest or mistakenly highlighted unrelated content, showing that individual text content within the terms of use is a challenge for automated identification and interpretation of opt-outs. Therefore, to achieve a high degree of accuracy in this endeavor, specialized language models, which are trained to understand the text details and nuances of such documents, are required for both the identification and interpretation of relevant TDM sections.

29 The analysis highlights the difficulties of relying on specific subpages or sections, such as the terms of use, to communicate opt-outs. When accounting for this information across multiple domains and webpages, TDM users face significant challenges, as it necessitates the use of advanced, individually designed crawlers or a method to deal with possibly incomplete webpage coverage, when relying on pre-crawled websites. To ensure full webpage inclusion, e.g., through monthly crawls of Common Crawl, each crawl would need to be inspected, which raises feasibility concerns given the substantial storage and computational demands this approach entails. Moreover, automated interpretation of unique phrasings within the terms of use usually requires sophisticated language models. The vast diversity across websites complicates the automatic extraction of statements pertaining to usage restrictions.

30 The study shows that each of the three steps involves substantial effort and costs. Effective opt-out management would require advanced NLP methods, which might still carry high error rates. This could undermine the TDM exception's effectiveness. Opting out in a website's terms of use would not be appropriate to the automated processes of TDM. Therefore, it cannot be considered a legally effective opt-out by machine-readable means.[21] Consequently, Section D discusses the use of alternative standards established for analogous purposes such as search engines. Foremost among these is the robots.txt protocol (see D.I), a widely recognized standard used by websites to communicate with web crawlers and other automated agents. From our analysis, it is evident that this standard has gained widespread adoption: 75 of the 85 valid websites we inspected had a populated robots.txt file in their root directory. Given its prevalent use and standardized nature, there is a promising potential to further harness the robots.txt standard in streamlining the processes we are addressing.

D. TDM and search engines

31 The current challenge lies in the absence of a dedicated technological standard specifically tailored for TDM to meet the aforementioned legal requisites. The exemplary investigation has revealed the lack of a defined technological standard exclusively addressing legal demands for TDM. Consequently, consideration of alternative standards established for analogous purposes becomes pertinent, potentially offering utility or even sufficiency for TDM. In this context, the established standards utilized by search engine crawlers such as Google, Microsoft Bing, Yandex, among others, stand out. These standards encompass the definition of website authorship or ownership preferences for permitting or prohibiting website crawling and indexing – namely, robots.txt and meta-tags. Hence, adaption, expansion, and alignment of pre-existing standards with appropriate distribution should be considered for TDM, tailored

20 Müller-ter Jung and Rexin (n 14) no 30.

21 Tina Gausling, 'Wie Unternehmen Online Verfügbare Daten Nutzen Können' [2021] Computer und Recht 609, 611.; Bullinger no. 10 (n 14), Raue (n 10) 797 and Müller-ter Jung and Rexin (n 14) 174 emphasize that the crawler's algorithms must be able to recognize the opt-out automatically, but are not so consistent as to exclude the possibility of opting out in the terms of use for this reason. Steinrötter and Schauer (n 15) consider plain text to be adequate and therefore opting out in the terms of use to be legally effective.

to effectively fulfil its requirements. The following sections will delve into the mentioned standards and discuss how they can be expanded and utilized for declaring usage reservations for TDM.

I. Robots.txt

32 "If you don't want crawlers to access sections of your site, you can create a robots.txt file with appropriate rules. A robots.txt file is a simple text file containing rules about which crawlers may access which parts of a site."[22] The robots.txt standard defined by the Robots Exclusion Protocol[23] (RFC9309) serves as a widely adopted means of communicating instructions to web crawlers and other automated agents. Prominent search engine providers, like those mentioned above, as well as OpenAI and its ChatGPT plugin agents, designed to respond to real-time user queries, commit to following the relevant instructions provided by website owners.[24]

33 Setting up a robots.txt file in the root directory of a domain allows a website owner to define if certain URLs, directories, file patterns or even the entire website should not be indexed. Furthermore, it enables them to specify if certain crawlers, identified by their user agent name, are allowed or disallowed.[25]

34 Crawlers interpret the absence of a robots.txt file as a generally granted invitation to index the publicly contents of a website. Thus, setting up a robots.txt file can express an opt-out.

Example robots.txt:

```
user-agent: *
disallow: /

user-agent: googlebot-news
allow: /news
```

35 In the example, the initial rule prohibits all user agents from indexing by utilizing the asterisk (*) as a wildcard character in the user-agent field. The asterisk functions as a universal placeholder for all user-agents, signifying that the instructions pertain to all web crawlers and automated agents accessing the website. The subsequent rule permits the Google "googlebot-news" crawler to index the news directory.

36 The robots.txt standard possesses the capacity to both allow and disallow specific or all user agents for certain or all URLs of a website. However, it does not offer the capability to grant or deny access for specific purposes like TDM. The limitation of purpose can solely be achieved by excluding particular user agents. The proprietary scripts and software employed for extracting information from websites for TDM typically lack identifiable user agent names, making them ineligible for disallowance. The demonstrated method above, involving disallowing all agents except those recognized as not engaging in TDM-related crawling, would be the only viable approach using the robots.txt to express an opt-out for TDM without requiring an extension of the standard.

II. Meta tags

37 Another type of annotation used by search engine crawlers are the so-called meta tags. Meta tags are invisible HTML tags integrated in the head part of a HTML document defining a website. They contain meta data offering further information about the website they are integrated in. Meta tags are on a per page basis. Therefore, they can be different for every single page of a website.

38 While meta tags can contain different types of data for different purposes, there are special meta tags for indexing:

22 Google Search Central, 'How Google interprets the robots.txt specification' <https://developers.google.com/search/docs/crawling-indexing/robots/robots_txt> accessed 17.01.2024.

23 M.Koster, G. Illyes, H. Zeller and L. Sassman, 'RFC 9309 Robots Exclusion Protocol' <https://www.rfc-editor.org/rfc/rfc9309.html> accessed 17.01.2024.

24 OpenAI, 'ChatGPT-User' <https://platform.openai.com/docs/plugins/bot> accessed 17.01.2024.

25 Google Search Central, 'How Google interprets the robots.txt specification', <https://developers.google.com/search/docs/crawling-indexing/robots/robots_txt> accessed 17.01.2024.

Example meta tags:
<meta name="robots" content="noindex">
<meta name="googlebot-news"
content="index">

39 The example disallows all robots from indexing the current page, first. Then it allows the user agent called "googlebot-news", and only this user agent, indexing of the page. This way indexing can be allowed and disallowed on any page. By default, if there are no meta tags disallowing it, indexing is allowed. Again, an opt-out is necessary to avoid indexing.[26]

40 Like robots.txt, there is no option in meta tags to only allow crawlers for specific purposes.

III. TDM as part of the search engine standard

41 Considering the resemblance between TDM and search engine operations, adopting the existing tools utilized for search engines appears rational for TDM as well. Both the robots.txt and meta tags could serve as suitable machine-readable methods to accurately convey opt-outs for TDM.[27] Conversely, a pertinent question emerges: What is the implication if a website lacks a robots.txt or meta tag conforming to the outlined scheme? Can the user then assume that the rightholder has not expressed an effective opt-out?

42 For the general TDM exception, the term TDM – i.e., the applications that are covered by it – is deliberately defined broadly:

43 Art. 2(3) Directive (EU) 2019/790: "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."

44 Section 44b(2) UrhG: "the automated analysis of individual or several digital or digitised works for the purpose of *gathering* information, in particular regarding patterns, trends and correlations".

45 In the explanatory memorandum of Section 44b UrhG, a distinction between Text and Data Mining and search engines is presented: "An opt-out [...] for a website must not lead to it being treated unequally in the context of other uses without objective justification, for example when it is displayed as a search engine hit. This is because the reservation of use should not affect other use cases.[28] However, this statement can also be interpreted more as fairness requirements applied to search engines, particularly due to their significant market influence, rather than as a definitive differentiation from TDM.

46 From a technical standpoint, search engines can be regarded as an integral component of TDM. They autonomously analyze and crawl substantial volumes of text data accessible on the internet, subsequently indexing it and utilizing algorithms to retrieve pertinent information in response to user queries. Furthermore, they employ advanced natural language processing and information retrieval algorithms to comprehend the semantic context of user queries, categorize data into applicable classifications (such as news, images, or books), and extract salient topics from texts.

47 Considering these aspects, robots.txt and meta tags can indeed be utilized for opt-out purposes, albeit with certain constraints. As demonstrated earlier, disallowing all agents except those recognized as permissible could effectively serve as an opt-out method. A TDM user who has been explicitly granted permission could rely on this arrangement.

48 However, the converse approach does not yield the same results. The rightsholder cannot be directed to employ robots.txt or meta tags in the demonstrated manner. The limitations imposed by these standards present significant challenges. The rightsholder would be obligated to individually list all authorized user agents and maintain the list's accuracy over time. Failure to do so jeopardizes the visibility of the website in prominent search results. It's worth noting that the prohibition of devaluation by search engines due to a TDM opt-out is of limited value, as search engines periodically introduce new user agents that would need to be disregarded by the website. Consequently, a TDM user who is not disallowed through robots.txt or meta tags cannot reasonably argue the absence of an effective opt-out.

26 Google Search Central, 'Robots meta tag, data-nosnippet, and X-Robots-Tag specifications' <https://developers.google.com/search/docs/crawling-indexing/robots-meta-tag> accessed 17.01.2024.

27 Gausling (n 21) 611; Björn Steinrötter & Lina Marie Schauer, § 4, in; Barudi (n 15) no 14; Müller-ter Jung and Rexin (n 14) 174.

28 'Explanatory Memorandum of Section 44b UrhG' (n 11) 89.:„Ein Nutzungsvorbehalt nach § 44b Absatz 3 UrhG-E für eine Webseite darf nicht dazu führen, dass diese im Rahmen anderer Nutzungen ohne sachliche Rechtfertigung ungleich behandelt wird, beispielsweise bei der Anzeige als Suchmaschinentreffer. Denn der Nutzungsvorbehalt sollte andere Nutzungen nicht betreffen."

E. An own machine-readable standard for TDM

49 In order to establish a standardized framework facilitating the systematic formulation of usage restrictions pertaining to TDM of websites, various methods are under consideration. Through the suggested approaches, varying levels of precision in content exclusion can be accommodated. This permits meticulous regulation of website usage for TDM, ensuring both systematic and efficient incorporation of opt-out mechanisms.

I. Standards in development

50 Presently, multiple organizations are engaged in the development of potential standards concerning the allowance and disallowance of TDM. However, as of now, none of these standards has become established and found widespread acceptance.

51 W3C proposes the TDM Reservation Protocol (TDMRep) which foresees meta tags or a JSON-LD integration of the permissions in the page's code. This way it is possible to allow or disallow certain pages. The directive "tdm-reservation" accepts either 0 (=opt-out) or 1 (=opt-int) to specify if TDM rights are reserved or not reserved. The second directive, "tdm-policy," enables the specification of a URL where additional policy-related information can be accessed. It's important to note that 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, with W3C delineating their structure and admissible values.

52 Analogous to the robots.txt mechanism, TDM reservations may be defined in a file named tdmrep.json, which has to be placed in the domain's root folder. In this scenario, an additional directive is mandated to specify the paths to which the reservations apply.[29]

53 IPTC's RightsML standard, which was published in 2018 and is based on W3C's Open Digital Rights Language (ODRL), offers defining extensive machine-readable usage policies for any type of media. It's available as XML, RDF and JSON-LD. This standard was initially intended to facilitate the communication of intellectual property rights and usage permissions associated with media assets. Over time, RightsML has found application in conveying licensing information, copyright terms, and usage restrictions for digital content across diverse sectors. This existing standard and infrastructure could be extended to encompass opt-outs for TDM by incorporating attributes that explicitly denote TDM permissions and restrictions. By integrating TDM-specific information into the RightsML schema, a comprehensive and structured approach can be achieved for addressing opt-outs related to TDM activities.[30] Thus, RightsML has been proposed as a possible solution at the W3C Text and Data Mining Reservation Protocol Community Group.[31]

54 The Coalition for Content Provenance and Authenticity (C2PA) developed another approach. They also introduced a rights protocol that can be attached as metadata directly to content. Opt-out reservations are delineated through specific data mining entries, allowing differentiation between various forms of utilization. At the cost of being operationally more complex, it offers the advantage of cryptographic traceability for content modifications. This standard therefore goes beyond the opt-out declaration towards the enforcement through content provenance.

55 Observing the evolving landscape of AI and research applications, Google recognised the need for updated web publisher controls that accommodate these new use cases. They initiated a public discourse inviting stakeholders from the web and AI communities, including publishers, civil society, and academia, to contribute to the development of complementary protocols with robots.txt as a starting point that enhance web publisher choice and control for emerging TDM applications[32]. The discussion is still underway without preliminary results or draft implementation proposals being public yet.

II. REP – Proposal for the implementation

29 World Wide Web Consortium, 'TDM Reservation Protocol (TDMRep)' <https://www.w3.org/2022/tdmrep/> accessed 17.01.2024.

30 International Press Telecommunications Council, 'IPTC RightsML Standard 2.0' <https://iptc.org/std/RightsML/2.0/RightsML_2.0-specification.html> accessed 17.01.2024.

31 International Press Telecommunications Council, 'IPTC's RightsML at W3C Text and Data Mining Reservation Protocol CG' <https://www.iptc.org/news/iptc-rightsml-at-w3c-text-and-data-mining-reservation-protocol-wg/> accessed 17.01.2024.

32 Danielle Romain, 'A principled approach to evolving choice and control for web content' <https://blog.google/technology/ai/ai-web-publisher-controls-sign-up/> accessed 17.01.2024.

56 As described in the preceding section, a pragmatic approach involves leveraging well-established conventions of the robots.txt file (see Section D.I), which allows website owners to establish wide-ranging exceptions at both the directory and page levels. In the same way that robots.txt can be used to declare access and usage restrictions for web crawlers, it could also be extended to declare usage restrictions for AI model training and other TDM activities. This extension would involve augmenting the robots exclusion protocol (REP) to incorporate information about the approval or disapproval of content specifically for TDM purposes.

57 Technically, this proposed extension can be actualized through the introduction of an optional term "purpose" within the robots.txt file. This extension empowers website owners to precisely define access permissions and restrictions tailored to specific purposes. The "purpose" term accommodates the assignment of various values, including "search-engine," "tdm," and "other," thereby affording a finer-grained control over user-agent behaviour. To ensure comprehensive coverage, it should be mandatory for each user-agent to be assigned to at least one of the purpose groups. This condition guarantees the explicit coverage of all user-agents in terms of their intended applications.

58 In instances where the purpose term is absent from a rule specified in the robots.txt file, it defaults to encompassing all feasible values. This default behaviour contributes to inclusivity and mitigates inadvertent access or restrictions.

59 By adopting this approach, the example presented in Section D.I can be expanded to demonstrate the extension of the robots.txt file, incorporating TDM-specific usage restrictions:

Example robots.txt:
```
user-agent: *
disallow: /
purpose: tdm

user-agent: *
allow: /news
purpose: indexing
```

60 In this illustrative scenario, access for all users is denied for any TDM activities throughout the entire website. However, an exception is made for web crawlers designed to index the designated news directory. This strategic decision reflects a common consideration among website owners who aim to safeguard their content from automated gathering for NLP model training while simultaneously striving to enhance visibility in popular search engine query results, thereby increasing click rates.

61 By means of this proposed standard, website owners can effectively communicate their requirements regarding TDM and specify compliance with usage regulations for purposes beyond research.

62 The aforementioned approaches, namely the use of the robots.txt file and of HTML meta tags, focus on providing page-wide and per page opt-outs for TDM. However, in the pursuit of a comprehensive standard that allows for precise control of TDM access, we posit the necessity to introduce methods that permit the exclusion of specific sub-areas within individual web pages. There could also be instances where the need or obligation arises to permit or restrict TDM exclusively for specific segments of a single webpage, without these rules being applicable to other sections.

63 Structured data represents a potential solution that is currently employed by search engines. It encompasses machine-readable concealed supplementary content that is directly integrated into a website. It describes an element or a group of elements in a standardized form that can be interpreted by machines trained for it. While the suggested structured data format, JSON-LD, may not ideally cater to this objective due to its page-level embedding of structured data, alternatives in the form of microdata and RDFa standards are available. These extend the regular HTML code of a website creating new elements or assigning additional data to already existing elements.[33]

64 Structured data relies on standardized elements that are defined and described by schema.org. This poses challenges when attempting to introduce new elements for the purpose of excluding TDM from specific portions of a website.

65 An alternative and more straightforward approach involves the incorporation of a novel HTML data attribute, similar to the practice adopted by Google to exclude sections of a website from its featured snippets. Featured snippets are distinctive boxes that invert the format of a conventional search result, displaying the descriptive snippet before other content. These may also appear within a grouping of related questions, known as "People Also Ask."[34]

66 Referred to as "data-nosnippet," this attribute is to be applied to the HTML element whose content should

33 Google Search Central, 'Introduction to structured data markup in Google Search' <https://developers.google.com/search/docs/appearance/structured-data/intro-structured-data> accessed 17.01.2024.

34 Google Search Central, 'Featured snippets and your website' <https://developers.google.com/search/docs/appearance/featured-snippets#block-fs> accessed 17.01.2024.

not be displayed within the featured snippets.[35]

Example:

```
<body>
 <h1>Le Louvre</h1>
 <p>The Louvre in Paris is the national mu-
seum of France. It is situated within the 1st
arrondissement. ...</p>
 <div data-nosnippet>
 <h2>West wing closed</h2>
  <p>Because of the ongoing renovations in
the west wing, this part of the Louvre is not
accessible until the end of the year. We are
sorry for the inconvenience.</p>
 </div>
</body>
```

67 The provided example shows general information about the Louvre Museum in Paris. While the first part, the description, can be used by Google for the featured snippets, the second part, the information about the renovations, is excluded from being used for the snippets.

68 Introducing a new attribute "data-notdm" would enable webpage owners and content creators to exclude specific parts of a page from being used for TDM purposes. Crawlers would then have to look out for these annotations within the code and either include or exclude the corresponding HTML tag's contents when extracting information.

III. Machine-readability of the proposed standards

69 The proposed and described "data-notdm" HTML attribute, as well as, the REP approach, can be understood as machine-readable method to articulate an opt-out for TDM activities. The criteria for machine-readability (section B.II) emphasize functionality tailored to automated processes of TDM from online accessible sources. The fundamental requirement is that machines possess the capacity to comprehend and interpret the opt-out in accordance with the specified context. By adhering to this notion, both the "data-notdm" attribute and the REP framework satisfy the core prerequisites for machine-readability, as they enable precise, automated, and contextually aligned communication of TDM exclusion preferences.

F. Outlook

70 Ensuring compliance with copyright laws and adhering to legal boundaries for TDM is of paramount importance to provide website owners and content creators with continued confidence in content provisioning on websites. To achieve this, the development and widespread adoption of legally sound standards and their enforcement are desirable to maintain operational security. Current discussions about AI regulation and the European AI Act[36], primarily emphasize ensuring transparency in training data to proof that it is relevant, representative, complete and error-free. The AI Act rather establishes a form of product conformity framework for AI products to ensure their content quality depending on their risk class, rather than being a primary means of demonstrating adherence to copyright for training data usage. In the latest consolidated draft for the AI Act, however, the legislator also seeks to address this, by including an amendment that requires providers of generative AI systems to "document and make publicly available a sufficiently detailed summary of the use of training data protected under copyright law".[37]

71 Given the absence of established standards (in the meaning of customary practices) and in view of the dynamic discussion about new standards (see B.III and E), website owners are advised to adopt a pragmatic approach when expressing a machine-readable opt-out. Incorporating the proposed statement in the robots.txt – using the already accepted way to allow or disallow user-agents (see D.I) – and simultaneously integrating it with an HTML attribute within relevant webpage elements according to the now established methods, can serve as an interim solution. These can then easily be adapted for a purpose statement or changed to a "data-notdm" attribute when this way of declaring an opt-out becomes an accepted practice.

35 Google Search Central, 'Featured snippets and your website' <https://developers.google.com/search/docs/appearance/featured-snippets#block-fs> accessed 17.01.2024.

36 Tambiama Madiega, 'Artificial intelligence act' <https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-regulation-on-artificial-intelligence> accessed 17.01.2024.

37 Amendment 399 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, Article 28 b, <https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/CJ40/DV/2023/05-11/ConsolidatedCA_IMCOLIBE_AI_ACT_EN.pdf> accessed 17.01.2024.

Authors' rights vs. textual scholarship: a Portuguese overview

by **Elsa Pereira** *

Abstract: This article addresses the main restrictions that European textual and genetic scholars face when the literary works they study are not in the public domain. Using Portugal as an example, the essay illustrates the most relevant contours of copyright policy and licensing in countries with a legal tradition of *Droit d'Auteur*, which protects not only intellectual property but also the sensitive moral interests of authors. While considering a few limitations and exceptions for teaching and scientific research secured in the law, the paper refers to case studies that showcase legal shortcomings in balancing authors' rights with the academic freedom of textual scholars, especially when digital editorial methodologies are involved. We argue that the dominant protection currently afforded to copyright holders in Europe undermines the research ecosystem of this disciplinary field, rendering knowledge production and scientific publication practically unfeasible for anyone investigating textual variance in the works of 20th- and 21st-century writers. After drawing attention to the problem, we plead for policy-making adjustments to allow greater freedom in using copyrighted works for humanities research and scholarship.

Keywords: textual scholarship; digital scholarly editing; copyright; personal rights; cultural heritage; cross-border-access; licensing; freedom of research

Recommended citation: Elsa Pereira, Authors' rights vs. textual scholarship: a Portuguese overview 14 (2023) JIPITEC 510 para 1

A. Introduction

1 The primary goal of textual scholarship is to investigate how texts of the cultural heritage develop and change over time, whether due to authorial revision or corrupted transmission.[1] For that purpose, scholars must examine the extant source documents of a written work and compare their materialised textual versions. This "interpretive criticism of variant readings"[2] relies on a "range of discourses available to literary criticism",[3] such

* University of Lisbon, School of Arts and Humanities, CLUL, Lisbon, Portugal. Email: <elsa.pereira@campus.ul.pt>. ORCID: <https://orcid.org/0000-0001-5113-2060>. The research leading to this article was supported by Portuguese national funds through FCT – Fundação para a Ciência e a Tecnologia, I.P., within the scope of DL57/2016/CP1443/CT0033 and UIDB/00214/2020.

1 Barbara Bordalejo, 'What is textual scholarship?' (2007) <http://www.textualscholarship.org> accessed 2 November 2022.

2 Hans Walter Gabler, 'Textual Criticism' in M. Groden and M. Kreiswirth (eds), *The Johns Hopkins Guide to Literary Theory & Criticism* (1st ed, The Johns Hopkins University Press, Baltimore and London 1994) p. 709 <https://epub.ub.uni-muenchen.de/5812/1/5812.pdf> accessed 7 May 2023.

3 Hans Walter Gabler, *Text Genetics in Literary Modernism and*

as textual and genetic criticism, which "does not have to" but usually involves "a form of scholarly editing"[4] to display textual "variance in context", using "a multilevel system of apparatus" with "a key function for interpretative discourse".[5]

2 Like other fields handling products of the human mind, textual scholarship is thus hampered by legal uncertainty, which the digital turn in humanities research has further accentuated due to cross-border dissemination and other intrinsic matters of the online environment. As Walter Scholger has already observed, "most humanists (or scholars in general, regardless of their respective domains) are not familiar with the legal implications of their work", nor are they sufficiently conversant with the regulations that apply to their activity. "Unfortunately, there is also little to no support from universities' legal offices",[6] which exposes researchers to potentially troubling consequences.

3 This article reviews the legal contours specifically affecting European textual and genetic scholars when the studied literary works are not in the public domain. While copyright laws grant authors exclusive rights of exploitation, third parties may use protected works by seeking authorisations from rightsholders and contracts providing for transfer or assignment. The law also includes exceptions and limitations to authors' rights that allow specific unauthorised uses. As will be demonstrated, neither system (authorisations & assignments nor limitations & exceptions) functions properly with textual research and scholarship.

4 To illustrate the spectrum of complications arising in European jurisdictions, we will take the Portuguese legislation for reference and consider the main restrictions imposed on textual scholarship. The paper will refer to case studies in Portugal and other EU Member States, which showcase legal insufficiencies in balancing authors' rights with some exceptions for teaching and scientific research and conclude that, regardless of recent provisions introduced by EU Directive 2019/790 on copyright and related rights in the Digital Single Market, the dominant protection afforded to rightsholders undermines the research ecosystem of this disciplinary field. After drawing attention to the problem, we ask for policy-making adjustments to allow greater freedom in using copyrighted works for humanities research and scholarship.

B. Authors' rights in Portugal

5 Like other European countries, Portugal must abide by international treaties (such as the Berne Convention) and EU Directives for the harmonisation of copyright in the Member States, transposing those treaties and implementing these directives into national civil law.

6 Accordingly, the Code of Copyright and Related Rights[7] protects all "intellectual works in the literary, scientific, and artistic fields, whatever their type, form of expression, merits, mode of communication, or objective".[8] The Portuguese legislator opted for presenting a non-exhaustive enumeration of protected works, introduced by the adverb "namely",[9] which in practice means that any written text (including those dictated by practical purposes, such as correspondence) is covered by copyright, as long as it constitutes an original intellectual creation. We should note, however, that although the list ambiguously mentions "books, pamphlets, magazines, and newspapers" among the examples,[10] the object of legal protection should be the intangible content of the text, not its material record (either manuscript, print, or electronic):

"Copyright protects creations of the spirit, such as

Other Essays (Open Book Publishers, Cambridge 2018), p. 209.

4 Dirk Van Hulle and Peter Shillingsburg, 'Orientations to text, revisited' (2015) 59 Studies in Bibliography 37 < https://xtf.lib.virginia.edu/xtf/view?docId=StudiesInBiblio/uvaBook/tei/sibv059.xml;chunk.id=d25715e2576;toc.depth=1;toc.id=d25715e2576;brand=default> accessed 2 November 2022.

5 Gabler, 'Textual Criticism', p. 713.

6 Walter Scholger, 'Intellectual Property Rights vs. Freedom of Research: Tripping stones in international IPR law' (Abstracts of DH2014, Lausanne, 2014) <https://www.academia.edu/13198978/Intellectual_Property_Rights_vs_Freedom_of_Research_Tripping_stones_in_international_IPR_law_Abstract_of_DH2014_Long_Paper_?source=swp_share> accessed 2 November 2022.

7 Código do Direito de Autor e dos Direitos Conexos (CDADC). Law no. 45/85, of 17 September 1985, as amended up to Law-Decree no. 47/2023, of 19 June 2023 <https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=484&tabela=leis> accessed 2 September 2023. Throughout this article, all quotations are taken from the English translation provided by WIPO – World Intellectual Property Organization: Code of Copyright and Related Rights (as amended up to Law no. 45/85 of 17 September 1985) <https://www.wipo.int/wipolex/en/text/129418> accessed 2 November 2022. However, the numbering of the articles will be updated, according to Law-Decree no. 47/2023.

8 CDADC, art 2 (1).

9 CDADC, art 2 (1).

10 CDADC, art 2 (1) (a).

poems and paintings, which can be documented on a material record, such as books and canvases. However, any of these material records are distinct from the work. It is necessary to distinguish the work from the respective mechanical record or *corpus mechanicum*. [...] We should also note that ownership of the material record does not confer any rights over the work. Therefore, whoever acquires a book or canvas has no copyright over the works contained in these materials."[11]

7 In line with the French tradition of *Droit d'Auteur*,[12] such legal protection translates into two main types of provisions: "economic" as well as "personal rights", also "termed moral rights".[13] We will examine each separately from a textual scholarly perspective to assess their constraining implications for our research field (parts I and II) before considering some exceptions and limitations to authors' rights, which the law provides for allowing specific unauthorised uses of protected works (part III).

I. Economic rights

8 The Portuguese code generally defines economic rights as the "exclusive right" that authors have "to disclose, publish and exploit economically" their work "in any direct or indirect form".[14] According to the European Directive 2001/29/CE on the harmonisation of certain aspects of copyright in the information society, this should translate into three exclusive rights granted to authors and their representatives: the "exclusive right to authorise or prohibit direct or indirect, temporary or permanent reproduction by any means and in any form, in whole or in part" of the protected work;[15] "the exclusive right to authorise or prohibit any communication to the public of their works, by wire or wireless means";[16] and "the exclusive right to authorise or prohibit any form of distribution to the public by sale or otherwise".[17]

9 Although the Berne Convention states that "the enjoyment and the exercise" of economic rights are not "subject to any formality",[18] until 1918 the property of literary or artistic works in Portugal was traditionally dependent on formal registration,[19] and nowadays there is still an optional form managed by the General Inspection of Cultural Activities, which aims only to publicise the authorial property, upon requirement, but is not a pre-condition to holding copyright.

10 The duration of this protection has been changing throughout the years in Portugal. Since the 1990s, "in the absence of any special provision", the author's economic rights "lapse 70 years after the death of the creator of the work".[20] During that period, "the original owner of the copyright, as well as his successors [...] may: (a) authorise the use of the work by a third party; (b) transfer or assign all or part of the economic content of the work's copyright",[21] either in "temporary"[22] or "permanent" terms.[23] Rightsholders may, for instance, offer copyright as debt security[24] or sell the exclusive right to reproduce

11 Patricia Akester, *Direito de Autor em Portugal, nos PALOP, na União Europeia e nos Tratados Internacionais* (Almedina, Lisboa 2013), p. 68. Translated from the Portuguese by the author of this article.

12 Whereas countries adhering to the Common Law Copyright system (such as the UK and its former colonies) have been focusing protection on the commercial exploitation of literary works, countries with a Civil Law tradition of *Droit d'Auteur* (historically rooted in the French laws of 1791 and 1793) tend to see copyright as a "dualistic right" (Akester, *Direito de Autor em Portugal*, p. 28) or a monistic right with two components (Germany), protecting the economic value of intellectual property as well as the moral interests of authors.

13 CDADC, art 9 (1).

14 CDADC, art 67 (1).

15 Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (InfoSoc Directive, art 2). Current consolidated version of 06 June 2019 <http://data.europa.eu/eli/dir/2001/29/2019-06-06> accessed 2 November 2022.

16 InfoSoc Directive, art 3.

17 InfoSoc Directive, art 4.

18 Berne Convention for the Protection of Literary and Artistic Works (Paris Act of July 24, 1971, as amended on September 28, 1979), art 5 (2) <https://www.unido.org/sites/default/files/2014-04/Berne_Convention_for_the_Protection_of_Literary_and_Artistic_Works_28.09.1979_0.pdf> accessed 16 May 2023.

19 Instituto da Biblioteca Nacional e do Livro – Direcção Geral dos Espectáculos, *Direito de Autor em Portugal: Um Percurso Histórico* (Biblioteca Nacional: Lisboa 1994), pp. 46-47.

20 CDADC, art 31.

21 CDADC, art 40.

22 CDADC, art 43 (4).

23 CDADC, art 44.

24 CDADC, art 46.

an author's works to a particular publishing house.

11 While transfer and assignment "may only be effected by public deed"[25] and "contracts" "witnessed by a notary",[26] the Portuguese Code of Copyright holds that authorisations "to disclose, publish, use or exploit a work"[27] should consist of a more straightforward procedure. They must only "be granted in writing"[28] and "show specifically the authorised form of disclosure, publication and use, as well as the relevant conditions governing duration, place and remuneration".[29] Although the law states that authorisations and assignments are subject to remuneration, rightsholders may also waive any revenue in principle.[30]

12 The daughters of Portuguese writer José Cardoso Pires (1925-1998), for example, are willing to waive any compensation after their mother's death because they consider that "the best thing that can happen to an author's work is being accessible in order to avoid oblivion".[31] They also think that heirs should not interfere with what scholars do about a literary legacy because "an author's work does not belong to his descendants", and an heir should not be "a writer's zombie".[32] As we will see, this selfless attitude of Ana and Rita Cardoso Pires contrasts with some authors' successors, who might be inclined to "make money from the shoes of the deceased" and "carve some visibility for themselves",[33] making the authorisation process held by art 41 of the Portuguese Code of Copyright highly random and uncertain.

13 To illustrate the depth of the problem, we must briefly refer to a few recent cases involving individual rightsholders and the Portuguese Society of Authors (SPA) – a limited liability cooperative established in 1925, which currently manages the rights of more than 20,000 affiliated authors.[34]

14 In 2013, the author of this article obtained written authorisation from SPA to undertake a genetic-critical edition of poetry by Pedro Homem de Mello (1904-1984) within the scope of a post-doctoral project at the Center of Linguistics of the University of Lisbon. After approval by the Portuguese Foundation for Science and Technology, the scholar worked on this project in close collaboration with the author's heirs, who approved and encouraged the project, giving her unlimited access to the poet's manuscripts under their control. In 2019, however, after years of extensive research and project investment (both by funding institutions and by the researcher's private expenditure), the heirs, represented by SPA, informed the scholar that the oeuvre of Pedro Homem de Mello was no longer available for the intended use. It turned out that they had sold Assírio & Alvim a commercial edition of the author's complete works, led by a different editor chosen by the publishing house. Since the authorisation granted by SPA in 2013 did not mention the conditions of time and place for the authorised scholarly edition – as stipulated in art 41 (3) of the Portuguese Code of Copyright – or the term for paying the copyright fee, the heirs decided to act as if their personal commitment with the researcher never existed while SPA's legal office repeatedly ignored a lawyer engaged by the University of Lisbon in finding room for negotiation. As a result, the scholarly edition had to be abandoned and the publication of essays avoided from then on, since SPA also ignored subsequent authorisation requests for using transcriptions of poems in articles, leaving the whole project paralysed in "a kind of perverse

25 CDADC, art 44.

26 CDADC, art 43 (2).

27 CDADC, art 41 (1).

28 CDADC, art 41 (2).

29 CDADC, art 41 (3).

30 While the Portuguese Code of Copyright states that authorisations "shall be considered nonexclusive and subject to payment" (CDACD, art 41 [3]), it also says that transfer deeds must show the amount of the remuneration "where payment is involved" (CDADC, art 43 [3]), suggesting that acts covered by chapter V (authorisation and transfer & assignment) are not necessarily subject to remuneration. In this respect, the CDSM Directive, for instance, clarifies that "[n]othing in this Directive should be interpreted as preventing holders of exclusive rights under Union copyright law from authorising the use of their works or other subject matter for free, including through non-exclusive free licences for the benefit of any users" – Directive 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market (CDSM Directive, para 82) <https://eur-lex.europa.eu/legal-content/en/TXT/HTML/?uri=CELEX:32019L0790> accessed 16 May 2023.

31 Rui Couceiro, 'Herdeiros ou zombies dos escritores?' Visão (Lisboa, 10 January 2022) <https://visao.sapo.pt/opiniao/ponto-de-vista/2022-01-10-herdeiros-ou-zombies-dos-escritores/?fbclid=IwAR1GVNp1NJbdTIe1oIoNpTtKhQE-K9UFwPOhtcFyqnIdlT06R1NYpDvUH-I> accessed 31 May 2023. Translated from the Portuguese by the author of this article.

32 Ibid. Translated from the Portuguese by the author of this article.

33 Ibid. Translated from the Portuguese by the author of this article.

34 Information stated on the official webpage <https://www.spautores.pt/en/who-we-are/> accessed 16 May 2023.

self-denial – *perverse* because not warranted by the porous nature of copyrights".[35]

15 No less disturbing is the case exposed recently by Federico Bertolazzi in the newspaper *Nascer do Sol*.[36] For more than three years, this Italian researcher worked on a scholarly edition of the scattered non-fiction prose (essays, interviews, testimonies) of Portuguese poet Sophia de Mello Breyner Andresen (1919-2004). Supported by a sabbatical leave from the University of Rome Tor Vergata and a scholarship from Instituto Camões, he undertook extensive research to compile the texts that Sophia published in periodicals of the time. During that process, the author's heirs authorised the scholar to access Sophia's manuscripts at the Portuguese National Library, since these works, despite being deposited in an institution funded by public resources, can only be perused with "prior and personalised authorisations [from the heirs] depending on the researcher".[37] However, when the edition was finally concluded and proposed for publication, the heirs refused their authorisation, justifying the decision with the need to restrict publication to what they arguably consider the author's *best* works. Eventually, the scholar had to convert his publication into a mere inventory of bibliographic descriptions without the texts,[38] resorting to the same "art of designing around copyrights"[39] followed by other European scholars to avoid "fiercely vigilant and obstructive"[40] authors' descendants.[41]

16 Alarming as they are, reports of heirs and estates using copyright to hinder scholarship are not unique to Portugal, and the problem seems particularly accentuated in recent years with the digital turn in humanities research. James Joyce's Estate, for instance, is renowned for refusing permission and making "difficult or impossible, numerous scholarly and creative projects – notably, an electronic multimedia version of *Ulysses* that an academic had spent years developing".[42] As a result, digital humanities research on contemporary authors is strongly discouraged:

> "In the case of contemporary literary works, this inevitably means that the decision who to give the rights [...] remains in the hands of the authors and the executors of their estates, until the day those rights expire and the materials enter the public domain. Should these limitations stop us from building DSEs [Digital Scholarly Editions] around their works? For Robinson, the answer seems to be: yes. [...] Hans Walter Gabler's unsuccessful attempts to win the favour of the Joyce estate [...] rendered him unable to continue his work on a digital edition of Joyce's *Ulysses* [...]. 'Events like these decided us', Robinson explains, 'We would never work on materials where someone else could, by fiat, render all our work worthless just by refusing publication permission'."[43]

35 Robert Spoo, 'Copyrights and "Design-Around" Scholarship' (2007) 44-3 James Joyce Quarterly 567 <https://muse.jhu.edu/pub/80/article/232339/pdf> accessed 2 may 2023. Using full-text transcriptions or even excerpts in research articles is not covered by the exceptions specified in art 75 of the Portuguese Code of Copyright. See infra part 3 of this essay.

36 Teresa Carvalho, Interview with Federico Bertolazzi, 'Até que ponto os herdeiros de Sophia podem bloquear uma obra?' Nascer do Sol (Lisboa, 27 December 2022) <https://sol.sapo.pt/artigo/788704/ate-que-ponto-os-herdeiros-de-sophia-podem-bloquear-uma-obra-> accessed 2 January 2023. Federico Bertolazzi, 'Carta de resposta à Professora Maria Andresen' Nascer do Sol (Lisboa, 8 January 2023) <https://sol.sapo.pt/artigo/789562/carta-de-resposta-a-professora-maria-andresen> accessed 9 January 2023.

37 Fátima Lopes, 'Como se trabalha no Arquivo de Cultura Portuguesa Contemporânea' in Luiz Fagundes Duarte and António Braz de Oliveira (org), *As Mãos da Escrita* (Biblioteca Nacional de Portugal, Lisboa 2007), pp. 53-54 <https://purl.pt/13858/1/abertura/como-trabalha-acpc.html> accessed 9 January 2023. Translated from the Portuguese by the author of this article.

38 Federico Bertolazzi, *No Reino Terrível da Pureza: Bibliografia da Prosa Dispersa Não Ficcional de Sophia de Mello Breyner Andresen e Três Ensaios* (Documenta, Lisboa 2022).

39 Spoo, 'Copyrights and "Design-Around" Scholarship' 567.

40 Robert Spoo, 'Ezra Pound's Copyright Statute: Perpetual Rights and the Problem of Heirs' (2009) 56 UCLA Law Review 1825 <https://ssrn.com/abstract=1286233> accessed 2 may 2023.

41 After opposition from the Joyce Estate to most research projects in textual scholarship and scholarly editing, Michael Groden, "noted for his close textual study of the genetic development of *Ulysses*, has written several articles containing general descriptions and inventories of the recent manuscript discoveries but has scrupulously avoided offering extracts" (Spoo, 'Copyrights and "Design-Around" Scholarship' 567).

42 Spoo, 'Ezra Pound's Copyright Statute: Perpetual Rights and the Problem of Heirs' 1826. See also Spoo, 'Copyrights and "Design-Around" Scholarship' 563-585, for mention of other scholarly projects affected by decisions of the Joyce estate.

43 Wout Dillen and Vincent Neyt, 'Digital scholarly editing within the boundaries of copyright restrictions' (2016) 31-4 Digital Scholarship in the Humanities 787 <https://doi.org/10.1093/llc/fqw011> accessed 2 January 2017.

17 Although "[t]raditional critical editing, defined by the paper and print limitations of the codex format, is now considered by many to be inadequate for the expression and interpretation of complex, multi-layered or multi-text works of the human imagination" – to such an extent "that in future all [scholarly] editions should be produced in digital and/or online form"[44] – the truth is that digital editorial approaches are generally regarded with suspicion by heirs, legislators, and judges.[45] As Valentina Moscon pointed out, the InfoSoc Directive itself "is based on the general assumption that, particularly in the online environment, right holders need effective and rigorous control over widespread forms of mass usage"[46] due to the cross-border nature of the online environment, transcending the limits of national jurisdictions:

> "Article 7(8) of the Berne Convention states that 'the duration shall be governed by the law of the country in which protection is claimed'; however [...] [t]he digital world is global. Cyberspace is a concept that goes beyond national borders. According to the US Supreme Court, [...] cyberspace [...] does not have a precise geographic location and any Internet user, anywhere in the world, can access it.
>
> Since it is not easy to identify the territory from which the transmissions originate and where the contents are disseminated, the resolution of questions regarding the determination of the law applicable to the cross-border transmission of works in digital format, as well as the competent court, is compromised."[47]

18 This transnational inherent condition of the World Wide Web has been forcing digital scholarly projects to find ways of limiting access to online content in order to avoid liability for copyright infringement. The Association for Research and Access to Historical Texts and the Huygens Institute for the History of the Netherlands, for instance, opted to publish their 2021 scholarly edition of Anne Frank's manuscripts (1929-1945)[48] under geoblocking restrictions that allowed access only from IP addresses located in countries where Frank's diaries were in the public domain – even though the restrictive measure was not enough to prevent the author's heirs from taking legal action shortly after the online publication appeared:

> "Because the copyright to a number of Anne Frank's texts has not yet expired in the Netherlands, part of the research, such as the transcriptions of Anne Frank's diaries, took place in Belgium. The online scholarly edition is only accessible in those countries where the copyright law on Anne Frank's Texts so admits. In Belgium, Germany, the Netherlands Antilles and other countries, some 60 in all, this edition is available to everyone online at annefrankmanuscripten.org. Through geo blocking the availability is limited to those countries. In the Netherlands and a number of other countries the online scholarly edition is not accessible due to copyright regulations. An English translation of this edition will be made available later in those countries where copyright law so permits."[49]

19 More cautious was the approach of the Beckett Digital Manuscript Project, developed by the Centre for Manuscript Genetics at the University of Antwerp, the Beckett International Foundation at the University of Reading, the Oxford Centre for Textual Editing and Theory at the University of Oxford, and the Harry Ransom Humanities Research Center at the University of Texas at Austin, with the permission of the Estate of Samuel Beckett and the support of a grant from the European Research Council.[50] In this latter case, the research team was able to negotiate with the author's heirs successfully and found a compromise between the parties by limiting access

44 Marilyn Deegan and Kathryn Sutherland, 'Introduction' in Marilyn Deegan and Kathryn Sutherland (ed), *Text Editing: Print and the Digital World* (Ashgate, Farnham 2009), p. 1.

45 "Judges engaging in a fair use analysis more often than not expect scholarship to come packaged in print monographs written in academic language aimed at an audience of disciplinary specialists. When they encounter scholarly artefacts that depart from those formal expectations and draw from pre-existing work, judges are less likely to find the use of pre-existing work is fair and therefore non-infringing" – Robin Wharton, 'Digital Humanities, Copyright Law, and the Literary' (2013) 7-1 Digital Humanities Quarterly <http://www.digitalhumanities.org/dhq/vol/7/1/000147/000147.html#> accessed 11 February 2022.

46 Valentina Moscon, 'Academic Freedom, Copyright, and Access to Scholarly Works: A Comparative Perspective' in Roberto Caso and Federica Giovanella (ed.), *Balancing Copyright Law in the Digital Age: Comparative Perspectives* (Springer, Berlin-Heidelberg 2015), p. 102.

47 Akester, *Direito de Autor em Portugal,* pp. 103, 161. Translated from the Portuguese by the author of this article.

48 Peter de Bruijn, Elli Bleeker and Marielle Scherer (eds), *Anne Frank Manuscripten* (2021) <https://annefrankmanuscripten.org> accessed 7 February 2023.

49 Peter de Bruijn, Elli Bleeker and Marielle Scherer, 'For the first time all Anne Frank's manuscripts digitised' (28-09-2021) <https://www.huygens.knaw.nl/en/anne-franks-digitised-manuscripts-available-in-their-entirety-for-the-first-time> accessed 7 February 2023.

50 Dirk Van Hulle and Mark Nixon (ed), *Samuel Beckett Digital Manuscript Project* (2021) <https://www.beckettarchive.org> accessed 7 February 2023.

to the digital scholarly edition through a paywall, whose revenue reverts to the Beckett Estate:[51]

"Thankfully, in the case of the BDMP, all parties involved have realised that the future of scholarly editing is digital, and that the scholarly augmentation of Beckett's legacy will only increase the interest in his works – academic or otherwise. For this reason, the Beckett Estate agreed to give the directors of the BDMP the license to publish their genetic Editions of Beckett's manuscripts, as long as this happens behind a pay-wall. [...] each of the collaborating institutions are granted institutional access to the edition."[52]

20 Still, these national and international examples draw attention to the risks textual scholars face when working on 20th and 21st-century authors. Only through institutional protocols and formal contracts signed beforehand by all the parties involved (universities, holding libraries, authors' heirs, and publishers) may a project in this research field be viable, and even when that is the case, there is no guarantee that unexpected complications will not arise.

21 Although negotiated and contracted by public authorities at the highest level, the critical-genetic edition of the works by Fernando Pessoa (1888-1935), for instance, was confronted with unexpected copyright issues that could end up jeopardising the entire project.[53] As the Portuguese law at the time stipulated that copyright was in force for 50 years after an author's death, Pessoa's works entered the public domain for the first time in 1985. Therefore, in 1988, the Government entrusted a team of researchers led by Ivo Castro with creating a critical edition of this author's works to be published by the national printing house. Five years later, however, the European Council Directive 93/98/EEC, sketched under the internal market provisions of the Rome Treaty, required all the member countries "to enact legislation extending copyright terms retroactively to seventy years *post mortem auctoris*. This meant that works which had been enjoying public-domain status [...] were abruptly pulled back into copyright".[54] Thus armed with newly extended provisions, Pessoa's heirs decided to transfer the economic content of their copyright to publishers Assírio & Alvim, which did not take long to exercise their property rights, requesting the immediate suspension of the ongoing critical edition. Fortunately, in this case (unlike what happened with the project on Pedro Homem de Mello), Assírio & Alvim and the authors' heirs were open to negotiation.[55] The institutional nature of the project, developed under the auspices of the Government, made it possible to reach an understanding that mirrored some mitigation actions taken in other European countries at the time.[56] Despite the disruption and anxiety caused to everyone, the research team could thus proceed with their work, and the national printing house went on to publish eight volumes of the critical-genetic edition during Pessoa's copyright repristination, only by paying a reasonable fee to Assírio & Alvim.[57]

22 Even so, the cases above are illuminating evidence of the "distorting effects" that "extravagantly long monopolies" granted to author's heirs and transferees "are having on culture"[58] in general and textual scholarship in particular. In European jurisdictions, though, such dominant economic protection is further aggravated with additional personal rights granted to authors but exercised by heirs and estates alike. We will now focus on those moral rights described in the Portuguese law that have a major impact on textual scholarship.

II. Moral rights

51 Ibid <https://www.beckettarchive.org/getlogin.html> accessed 7 February 2023.

52 Dillen and Neyt, 'Digital scholarly editing within the boundaries of copyright restrictions' 789.

53 Simone Celani, *O Espólio Pessoa: Para Uma História das Edições e dos Critérios Adotados* (Imprensa Nacional, Lisboa 2020), pp. 40, 42-45.

54 Spoo, 'Copyrights and "Design-Around" Scholarship' 568.

55 A copy of the intimation, dated 16 May 1997, is kept among the project's documentation at the Library of the School of Arts and Humanities of the University of Lisbon. In the letter, addressed to the national printing house, Assírio & Alvim and Pessoa's heirs state that they were willing to discuss any commitment previously assumed, but would not fail to take legal action and protect their interests (xerocopy of a letter from Manuel Hermínio Monteiro and Manuela Nogueira to Imprensa Nacional-Casa da Moeda, ref. 210/DA. Universidade de Lisboa – Faculdade de Letras – Biblioteca, Espólio Equipa Pessoa. Uncatalogued documentation).

56 In the United Kingdom, for instance, a compulsory-license exception was issued to Danis Rose's revised edition of Joyce's *Ulysses* (Spoo, 'Copyrights and "Design-Around" Scholarship' 568-569).

57 Between 1997 and 2006, the Portuguese national printing house published the following volumes of the scholarly edition: *Poemas de Fernando Pessoa – Quadras* (1997); *Poemas Ingleses II: Poemas de Alexander Search* (1997); *Poemas Ingleses III: The Mad Fiddler* (1999); *Poemas de Fernando Pessoa: 1934-1935* (2000); *Poemas de Fernando Pessoa: 1921-1930* (2001); *Obras de António Mora* (2002); *Poemas de Fernando Pessoa: 1931-1933* (2004); *Poemas de Fernando Pessoa: 1915-1920* (2005).

58 Spoo, 'Copyrights and "Design-Around" Scholarship' 568.

23 Unlike authors' economic rights, "personal rights, termed moral rights",[59] are "perpetual, inalienable, and imprescriptible".[60]

24 While the guardianship of these moral rights cannot be transmitted,[61] the law holds that an author's successors may exercise them upon the writer's death until the work falls "within the public domain",[62] when the State takes over the responsibility.[63] In practice, this allows heirs and estates to use authors' moral rights to expand the sphere of power during and even beyond their period of economic exploitation and occasionally "suppress or control scholarship"[64] in what has already been labelled as "copyright misuse".[65] We shall therefore look into the practical implications for textual scholarship.

25 In broad terms, the Portuguese Code of Copyright defines moral rights as the author's "right to claim authorship of his work and to ensure its authenticity and integrity by opposing any mutilation, distortion or other modification thereof and, in general, opposing any action that might be prejudicial to his honour and reputation".[66] Simply put, this translates into two main provisions granted to rightsholders against the academic interest of textual scholarship: (a) the right to oppose any modifications to the authorial text; (b) the right to oppose the disclosure of unpublished or private writings that heirs may consider harmful to the author's reputation.

26 Regarding the first provision, we should note that heirs may oppose all modifications performed by anyone but the author.[67] Even where using a work "without [...] consent is lawful",[68] scholarly editors cannot introduce any correction or alteration to a text without formal consent of the author's successors, which "shall be requested by registered letter with acknowledgement of receipt".[69] The only exception is the "modernisation of spelling in accordance with the official rules in force", provided that it does not constitute an aesthetic option of the author.[70] This prescription runs against the principles of several schools of textual criticism – from the Italian *filologia d'autore* to the Anglo-American copytext editing approach – whose "editorial labor by controlled alterations" includes emendation to "critically recognisable" instances of the text, [71] such as authorial errors[72] and different types of corruptions introduced in the transmission process "when authors could not or did not read proof".[73] Although the spirit of the law behind art 56 (1) of the Code of Copyright is to protect the author against any harm caused to his intellectual creation, it also implies that authors and their heirs have the absolute power to block or derail the activity of a particular textual scholar in favour of another they trust. As often is the case, trusting personal acquaintances to exclusively make decisions on one's behalf and preventing other scholars from carrying out their critical practice does not necessarily safeguard the authorial best interest in the long run. This assertion is especially true for works covered by art 58 of the Portuguese Code of Copyright.

27 According to this, "[w]here the author has partially or wholly revised his work and has effected or authorised" an edition carrying the legal expression "ne varietur", not only is it forbidden to make alterations to that text, but no one, not even "his successors or third parties", may ever "reproduce any of the previous versions" again.[74] In this sense, a *ne varietur* edition, such as the one Maria Alzira Seixo and her team have been allowed to publish for António Lobo Antunes' complete works since 2003, will indefinitely prohibit any critical or genetic

59 CDADC, art 9 (1).

60 CDADC, art 56 (2).

61 CDADC, art 42.

62 CDADC, art 57 (1).

63 CDADC, art 57 (2).

64 Spoo, 'Ezra Pound's Copyright Statute: Perpetual Rights and the Problem of Heirs' 1822.

65 Spoo, 'Copyrights and "Design-Around" Scholarship' 575.

66 CDADC, art 56 (1).

67 CDADC, art 56 (1).

68 CDADC, art 59 (1).

69 CDADC, art 59 (3).

70 CDADC, art 93.

71 Gabler, 'Textual Criticism', p. 710.

72 Based on Roncaglia's and Cunha's previous considerations on this matter, João Dionísio identifies two main types of authorial errors: *errors by execution* and *conception errors* (João Dionísio, *Doença Bibliográfica* [Imprensa Nacional, Lisboa 2021], p. 118). The former result from momentary or mechanical distractions while writing, while the latter correspond to what Roncaglia called *errors of fact or language* – i.e. inaccuracies caused by memory lapses, cultural limitations, or the author's non-compliance with current linguistic norms. Only authorial errors by execution should deserve obvious correction by textual scholars (Ibid 107).

73 Gabler, 'Textual Criticism', p. 710.

74 CDADC, art 58.

editions of the author's works, even after they fall into the public domain. Such condition is all the more disturbing if we think that a list of errors has already been identified in the definitive volumes,[75] but "those typos in the *ne varietur* edition cannot be amended in reprintings", since "any alterations introduced in a *ne varietur*, even with the best of intentions and for correct purposes, are under the purview of the Law and imply judicial action against any of the entities involved: authors, writer, and editor".[76] And whereas the editorial team trusted by the Portuguese writer and his family openly admits that "the previous editions [...] constitute a valuable element for genetic studies", they also acknowledge that after the *ne varietur* is published, "the official use of the author's previous editions (in teaching, research, translations, citations, and other public purposes) is forbidden and subject to legal action".[77] Considering that Lobo Antunes was consulted but did not revise the *ne varietur* editions himself,[78] that he apparently delegated many decisions to his daughters,[79] and that new authorial – hence *authentic*[80] – manuscripts may resurface in the future – clarifying obscure passages in the corrupted printed text[81] or challenging the editorial decisions in the *ne varietur* printings – we can only agree that art 58 of the Portuguese Code of Copyright mainly protects "the commercial interests of the publishing house"[82] instead of the "authenticity and integrity"[83] of the literary work. Indeed, the absolute and definitive legal value of the moral protection granted to rightsholders does not take care of "the necessary elasticity" and "the desirable improvement of the established text"[84] to safeguard the integrity of the author's legacy, the ethics of cultural heritage for coming generations, and the independence of present and future scholarly research.

28 As for the second moral right with implications for textual scholarship, we will note that any person who "discloses or publishes a work not disclosed by its author or not destined to be disclosed or published, even where he presents it as the respective author's work and whether or not he seeks to obtain economic benefits" shall "be guilty of the offence of illegal exercise of rights".[85] According to the Portuguese code, rightsholders have the exclusive "right to decide upon the use of undisclosed and unpublished works",[86] and anyone willing to use those texts must follow the authorisation process held in art 41, with its challenging contours. Federico Bertolazzi, for instance, reveals that Sophia de Mello Breyner's daughter has been disclosing unpublished poems that the author left in manuscripts while prohibiting researchers from doing the same with the materials kept at the Portuguese National Library.[87] One of the author's grandsons was even allowed to continue a short story left unfinished by Sophia, which Porto Editora published with aplomb back in 2012.[88] Although such decisions of the heirs were legally protected by articles 57 (1) and 70 (1) of the Code of Copyright, we should probably ask about the ethical legitimacy of those granted moral rights that authors' successors have been executing.

29 To what extent should heirs and estates determine which unpublished works do or do not harm the reputation of the deceased? And to what extent should copyright protect literary drafts that the author did not even properly finish? In 2011, the Lisbon Court of Appeal, analysing a case that discussed whether a sculptor's model could be protected by copyright, determined that, similarly to a sketch, the artefact in question constituted a mere stage on the path to the final work that embodied the original idea and, therefore, did not deserve protection:[89]

75 Maria Alzira Seixo, Graça Abreu, Eunice Cabral, Agripina Carriço Vieira, *Memória Descritiva: Da Fixação do Texto para a Edição ne varietur da Obra de António Lobo Antunes* (D. Quixote, Lisboa 2010), pp. 145-149.

76 Ibid, p. 168. Translated from the Portuguese by the author of this article.

77 Ibid, p. 30. Translated from the Portuguese by the author of this article.

78 Ibid, p. 27.

79 Ibid, p. 25.

80 Dionísio, *Doença Bibliográfica*, p. 26.

81 Ibid, p. 43.

82 Ibid, p. 43. Translated from the Portuguese by the author of this article.

83 CDADC, art 56 (1).

84 Dionísio, *Doença Bibliográfica*, p. 43. Translated from the Portuguese by the author of this article.

85 CDADC, art 195 (2).

86 CDADC, art 70 (1).

87 Carvalho, Interview with Federico Bertolazzi, 'Até que ponto os herdeiros de Sophia podem bloquear uma obra?'. Bertolazzi, 'Carta de resposta à Professora Maria Andresen'.

88 'Conto inédito de Sophia terminado pelo seu neto' (02/10/2012) Diário de Notícias <https://www.dn.pt/artes/livros/conto-inedito-de-sophia-terminado-pelo-seu-neto-2804445.html> accessed 4 May 2023.

89 Judgment of the Court of Appeal of Lisbon [Acórdão do

"By dictating its incompleteness and classifying it as a 'common thing', the Court concluded [...] that the production in question was far from the concept of 'work' as a creation of the spirit or intellect, or that it lacked originality."[90]

30 For literary works, however, courts never applied the same interpretation, and, in general, authors' heirs have been especially protective of unpublished texts, claiming "family privacy"[91] or personal reputation to block the use of such writings as letters and diaries, but also poems, short stories, and novels in draft manuscripts. James Joyce's Estate is renownedly zealous in this regard, taking legal action against many researchers who publish the author's papers found in archives and libraries open to the community:

"Nearly all of the documents that the Estate has declared off-limits to publishing scholars — letters by James Joyce and Joyce family members, essays and memoirs by Lucia Joyce and Helen Kastor Fleischman Joyce — are either already published or held in archives and collections that are generally open to the public. So these documents are not 'private' in the sense that they are physically or legally inaccessible. We can learn any of their secrets; we just cannot quote our findings in articles and books or on the Internet. We can kiss but not tell. And how is our silence enforced? Through the climate of fear that many copyright holders have cultivated [...]. And when copyrights are used as scarecrows to obtain 'effective control over information,' [...] we are witnessing something that is increasingly being recognised by lawyers and judges as 'copyright misuse' — an attempt to extend copyright protection beyond its appropriate sphere."[92]

31 As such, and since obtaining authorisations from both custodians of the material and copyright owners[93] "may be difficult and sometimes hopeless",[94] it seems imprudent to develop any scholarly research on unpublished works before they fall into the public domain, which "[i]n the absence of any special provision" should be "70 years after the death of the creator of the work, even in the case of works disclosed or published posthumously".[95]

32 Still, copyright policy is "blessedly porous"[96] by incorporating several measures to permit unauthorised uses of protected works and limit copyright control exerted by rightsholders. The period legally in force for controlling works left unpublished by a writer is among those limitations to authors' rights.

III. Limitations and exceptions to authors' rights

33 While "the economic rationale for copyright is based on a public policy objective of encouraging creation for the benefit of society", and the moral rationale protects "the author's private right to control her expression",[97] many, if not all legislatures have fashioned ways to balance authors' rights with the "public access to creative works [...] in situations where the social costs of copyright restrictions outweigh the benefits":[98]

"Copyright protection must be broad enough to provide authors adequate incentives to produce and disseminate creative works, but not so broad that an author's ability to extract monopoly rents for access chills the production and dissemination

Tribunal da Relação de Lisboa], Process Nr. 323/07.8TVLSB. L1-2, 30-06-2011. Apud Akester, *Direito de Autor em Portugal,* pp. 64-65.

90 Akester, *Direito de Autor em Portugal,* p. 65. Translated from the Portuguese by the author of this article.

91 Spoo, 'Copyrights and "Design-Around" Scholarship' 573.

92 Ibid 574-575.

93 As warned by several holding libraries, "[t]he owner of copyright for material in the Manuscripts Collection is the writer or creator of the material, or the creator's legal heir(s). Note that the donor of the material is not always the copyright owner. In addition, many collections contain a variety of letters, diaries, documents owned by multiple copyright owners. [...] Should you wish to publish material from the Library's Manuscript Collection, you will need to declare your intention to the Library as custodian of the material. You will also need to obtain copyright clearance from the copyright holder(s)" (National Library of Australia, 'Rights and the Manuscripts Collection' <https://www.nla.gov.au/copyright-and-the-manuscripts-collection> accessed 15 November 2019).

94 Spoo, 'Copyrights and "Design-Around" Scholarship' 579.

95 CDADC, art 31.

96 Spoo, 'Copyrights and "Design-Around" Scholarship' 579.

97 Matt Jackson, 'Copyright' in Wolfgang Donsbach (ed), *The Concise Encyclopedia of Communication* (Wiley Backwell, Sussex 2015), p. 115.

98 Maureen Ryan, 'Fair Use and Academic Expression: Rhetoric, Reality, and Restriction on Academic Freedom' (1999) 8-3 Cornell Journal of Law and Public Policy 541-542 <https://scholarship.law.cornell.edu/cjlpp/vol8/iss3/3> accessed 8 January 2023.

of, and access to, creative works."[99]

34 As a country with a Civil Law system, Portugal avoids the monopolistic protection of rightsholders by legally providing some limitations to authorial rights (legal licenses and compulsory licenses, where authors and successors cannot prohibit specific uses but are still entitled to financial compensation) and exceptions covering specific unauthorised uses (not subject to compensation).

1. Limitations

35 Presently, the Portuguese Code of Copyright incorporates two types of legal (or statutory) licences that allow for specific unauthorised uses of copyrighted material, even though they are subject to fair compensation to authors or their successors. For legal licenses, it is the law itself permitting the use, whereas for compulsory licenses, the authorial consent is to be replaced by a court decision.[100]

36 Covered by legal licence situations are "the right to translate or transform the work in any way necessary for its use"[101] and also the right to disclose works left unpublished by a writer, "where the successors do not use the work within a period of 25 years from the date of the author's death".[102] However, the latter shall not apply "in the case of impossibility or delay in disclosure or publication for serious moral considerations that shall be decided upon by the courts".[103] In practice, this caveat leaves much latitude for litigation since, as we have seen, heirs often call on moral grounds, such as authorial reputation, to oppose the disclosure of unpublished works. Besides, significant discrepancies exist across jurisdictions and apply, depending on the country where publication takes place,[104] which makes it particularly unwise for scholars to rely on this legal license for working with unpublished writings:

"for unpublished works such as manuscripts, letters, diary entries, etc., the waters are particularly muddy. In Canada, for example, copyright of unpublished materials expires 50 years after the calendar year of the author's death [...]. In the USA, this period is extended to the author's life plus 70 years [...]. In the UK, on the other hand, '[w]orks that were unpublished at the author's death and remained so until 1 August 1989 [...] are protected by copyright [...]' until the year 2040. And in Australia, copyright can be enforced for 70 years after the unpublished work has been 'disclosed', meaning that it will differ from work to work, and on the purview of what it means to legally 'disclose' an unpublished work."[105]

37 Additionally, we may count as legal licence the possibility of including "short excerpts or parts of another author's work in works used for teaching".[106]Although the InfoSoc Directive allowed a similar optional provision for both teaching and scientific research[107], art 5 of the European CDSM Directive opted to exclude mention of research and scholarship.[108] Accordingly, the Portuguese legislator excluded research publications from art

99 Ibid 548-549.

100 Luís Manuel Teles de Menezes Leitão, *Direito de Autor* (2 ed, Almedina, Lisboa 2018), p. 172.

101 CDADC, art 71.

102 CDADC, art 70 (3).

103 CDADC, art 70 (3).

104 Authors' rights are protected by the law of the country where the use of a work occurs. Therefore, the law of the country where publication takes place should apply. In academic publications, however, a journal, based at the university of one country, is often published by an international editorial group from another country. Besides, digital publication is especially problematic due to the cross-border nature of the online environment transcending the limits of national jurisdictions.

105 Dillen and Neyt, 'Digital scholarly editing within the boundaries of copyright restrictions' 788-789.

106 CDADC, art 75 (2) (i).

107 InfoSoc Directive, art 5 (3) says that "Member States may provide for exceptions or limitations" in the following case: "(a) use for the sole purpose of illustration for teaching or scientific research, as long as the source, including the author's name, is indicated, unless this turns out to be impossible and to the extent justified by the non-commercial purpose to be achieved".

108 CDSM Directive, title II, art 5 (1) says that "Member States shall provide for an exception or limitation [...] in order to allow the digital use of works and other subject matter for the sole purpose of illustration for teaching, to the extent justified by the non-commercial purpose to be achieved, on the condition that such use (a) takes place under the responsibility of an educational establishment, on its premises or at other venues, or through a secure electronic environment accessible only by the educational establisment's pupils or students and teaching staff". This provision has just been implemented in art 75 (2) (g) and art 76 (7) of the Portuguese Code of Copyright. Art 5 of the CDSM Directive also establishes that "Member States may provide for fair compensation for rightholders for the use of their works", which the Portuguese CDADC has now incorporated into art 76 (1) (c), providing for "equitable remuneration to be paid to the author and publisher".

75 (2) (i) of the Code of Copyright, inhibiting textual scholars to use excerpts of copyrighted material without seeking permission and paying the required royalties – even though academics are generally not paid for their essays, since the incentive "to publish research results is mostly reputational rather than economic".[109]

38 As for compulsory licences, the Portuguese Code of Copyright holds that "[w]here the owner of the right to re-edit refuses to use his right or to authorise another edition after the work has become out of print, any interested party, including the State",[110] may obtain the authorisation through courts, "provided that re-edition of the work is in the public interest and that the refusal was not based on justified moral or material reasons, excluding financial reasons".[111] In practice, however, this extreme situation is hardly applicable in litigation with heirs because the *attainable moral reason* is an elastic notion, and, in general, Court disputes tend to be settled in favour of the author and his representatives.[112]

2. Exceptions

39 In addition to these legal and compulsory licences, art 75 of the Portuguese Code of Copyright lists a series of exceptions regarding the use of for copyrighted material, which are considered as fair and which are not subject to authorisation or payment to rightsholders. Among the free exceptions more directly implied in the activity of textual scholars, we shall highlight the possibility of libraries, archives, and educational establishments (including universities) digitising orphan works – that is "copyrighted works whose owners cannot be located"[113] – and making them available to the public, for preservation.[114] This provision has just been aligned with the recommendation held in art 6 of the European CDSM Directive for preserving cultural heritage in the Digital Single Market, but, nonetheless, falls far short of other measures implemented in North America to facilitate the use of orphan works to scholarly research.[115]

40 Also relevant for textual scholars is the new exception for text and data mining (TDM)[116] – recently transposed from the European CDSM Directive – since computational literary studies have been considering the publication of derived data or extracted features as a possible solution to navigate copyright restrictions. Besides metadata and ancillary data,[117] researchers refer to information extracted through TDM, such as classification and clustering of texts (e.g. for authorship attribution and stylometry), extraction of distinctive features, semantic analysis with topic modelling, analysis of polarity with sentiment analysis, character relationships with network analysis, and analysis of relationships between texts (e.g. in text reuse).[118] However, we should note that only those materials to which scholars have lawful access can be mined, and experiences in countries where TDM exceptions have been in force show that copyright issues will subsist:

109 Moscon, 'Academic Freedom, Copyright, and Access to Scholarly Works' 101.

110 CDADC, art 52 (1).

111 CDADC, art 52 (2).

112 As Valentina Moscon notes, the judicial power and the legislature currently seem "to care more about right holders' than users' interests" (Moscon, 'Academic Freedom, Copyright, and Access to Scholarly Works', p. 117).

113 David R. Hansen, 'Orphan Works: Mapping the Possible Solution Spaces' (2012) Berkeley Digital Library Copyright Project White Paper 2 <https://ssrn.com/abstract=2019121> accessed 4 June 2023.

114 CDADC, art 75 (2) (u).

115 See David R. Hansen's essay for a range of proposed orphan works solutions: "[r]emedy-limitation approaches, such as the one advocated in the 2006 U.S. Copyright office proposal, that are predicated on a user's good-faith, reasonable search for rights holders; administrative systems, such as the one adopted in Canada, that allow users to petition a centralized copyright board to license specific reuses of orphan works; access and reuse solutions that are tailored to rely upon the existing doctrine of fair use; and extended collective licensing schemes, which permit collective management organizations ('CMOs') to license the use of works that are not necessarily owned by CMO members, but that are representative of the CMO members' works" (Hansen, 'Orphan Works: Mapping the Possible Solution Spaces').

116 CDADC, art 75 (2) (v) (w); art 75 (6); art 76 (4) (5) (6).

117 Dillen and Neyt, 'Digital scholarly editing within the boundaries of copyright restrictions' 790-791.

118 Christof Schöch, Frédéric Döhl, Achim Rettinger, Evelyn Gius, Peer Trilcke, Peter Leinen, Fotis Jannidis, Maria Hinzmann, Jörg Röpke, 'Abgeleitete Textformate: Text und Data Mining mit urheberrechtlich geschützten Textbeständen' (2020) Zeitschrift für Digitale Geisteswissenschaften <https://doi.org/10.17175/2020_006> accessed 25 August 2023; José Calvo Tello and Nanette Rißler-Pipka, '¿Qué hacer con textos que no se pueden publicar? Datos derivados, criterios FAIR y TEI' (2023) 16 Journal of the Text Encoding Initiative <http://journals.openedition.org/jtei/4720> accessed 25 August 2023.

"Despite the TDM exception in German copyright law, Text and Data Mining (TDM) with copyrighted texts is still subject to restrictions, including those concerning the storage, publication and follow-up use of the resulting corpora, leaving the full potential of TDM in the Digital Humanities untapped".[119]

41 Finally, we shall point out that art 75 of the Portuguese Code of Copyright also allows for the "inclusion of quotations or summaries from another author's work, whatever their type or nature, in support of one's own opinions or for purposes of criticism, discussion or teaching".[120] However, citations of protected texts must be fully integrated into a critical argument and their length "shall not be so extensive that they prejudice interest"[121] or purchase of the original literary work. The Portuguese code does not state the precise extent or the proportion of a work that can be used for citation, but an amendment of the Berne Convention by the Brussels Act (1948) explicitly required that quotations be "short",[122] and while a few lines of a novel would be a small percentage of the work overall, the same amount of text may be considered rather substantial in shorter works such as poems. For that reason, some international publishing groups have been requiring in their regulations that any scholarly article quoting poems or song lyrics protected by copyright should be submitted with formal authorisation from rightsholders, regardless of the fair use clause found in most European and Anglo-American copyright laws:

42 As a warranty in the Journal Author Publishing Agreement you make with us, you must obtain the necessary written permission to include material in your article that is owned and held in copyright by a third party, including – but not limited to – any proprietary text, illustration, table, or other material, including data, audio, video, film stills, screenshots, musical notation, and any supplemental material. It is the custom and practice in academic publishing that the reproduction of short extracts of text and some other types of material may be permitted on a limited basis for the purposes of criticism and review without securing formal permission, on the basis that: the purpose of quotation or use is objective and evidenced scholarly criticism or review (not merely illustration); a quotation is reproduced accurately, either within quotation marks or as displayed text; full attribution is given. However, a quotation from a song lyric or a poem, whether used as an epigraph or within the text, will always require written permission from a copyright holder. Our publishing agreement with you requires that you must obtain written permission to reproduce any content, especially image content, in your article, when that content is owned and held in copyright by a third party.[123]

"Do I need permission to use poems and songs? Yes, permission should always be obtained. Please be aware that some poets will not allow changes to the layout of the poem or allow you to use a small number of lines. Poem fees are normally charged per line. With song lyrics you should be aware that even if you only use one line you may be charged the same price as you would for the complete song. Rightsholders for song lyrics require people intending to reproduce lyrics to apply for permission for each reuse, and a fee may be charged."[124]

43 Moreover, art 5 (3) (d) of the European InfoSoc Directive recommends that "quotations for purposes such as criticism or review" should only be legal "provided that they relate to a work [...] which has already been lawfully made available to the public".[125] Such a requirement opens the door for litigation by heirs and estates,[126] forcing literary critics into

119 Schöch et al., 'Abgeleitete Textformate: Text und Data Mining mit urheberrechtlich geschützten Textbeständen'.

120 CDADC, art 75 (2) (h).

121 CDADC, art 76 (2).

122 Meanwhile, the Stockholm revision replaced this adjective by the expression "compatible with fair practice" (Berne Convention for the Protection of Literary and Artistic Works. Stockholm Act, 1967, art 10 [1] <https://wipolex-res.wipo.int/edocs/lexdocs/treaties/en/berne/trt_berne_003en.pdf> accessed 4 May 2023).

123 Taylor & Francis, 'Author Services' <https://authorservices.taylorandfrancis.com/using-third-party-material-in-your-article/> accessed 15 November 2019.

124 Taylor & Francis, 'Author Publishing Agreement' <https://authorservices.taylorandfrancis.com/publishing-your-research/writing-your-paper/using-third-party-material> accessed 15 November 2019.

125 Unlike art 5 of the new CDSM Directive, this art 5 of the InfoSoc Directive was a non-compulsory exception, stating that "Member States *may* provide for limitations" to allow "quotations for purposes such as criticism or review". In the UK (where many scholarly publishing groups are based), quotations for criticism or review are also only allowed when "the work has been made available to the public" (Copyright, Designs and Patents Act 1988, Section 30 <https://www.legislation.gov.uk/ukpga/1988/48/contents> accessed 4 May 2023).

126 There are several such cases abroad, involving the Joyce Estate. According to Robert Spoo, "Professor Carol Loeb Shloss of Stanford University's English Department [...] had spent years researching a biography of Joyce's talented and troubled daughter, Lucia, and at last published it in 2003 [...], but not before she and her publisher deleted many

"carefully designing around any impulse to quote from" unpublished material[127] or "paraphrasing it nearly out of existence".[128] But while this kind of "design-around scholarship"[129] may be attempted in some literary studies, it is usually not viable in textual and genetic criticism because assessing the "macrogenesis (the genesis of the work in its entirety across multiple versions)" requires collation of "large textual units along the syntagmatic axis with the development along the paradigmatic axis on a macrolevel".[130]

44 For all that, the narrow scope of the exceptions currently provided in national and communitarian laws, in accordance with the so-called *three-step test*,[131] results in ineffective counterbalancing of "the monopolistic protection that copyright affords to authors [...] against the limitation on public access to creative works".[132]

C. Conclusion and outlook

45 The case studies analysed in this article showcase several shortcomings in balancing authors' rights with the academic freedom of textual scholars, especially when digital editorial methodologies are involved.

46 As others have noted before, literary "copyrights are coming to resemble closely guarded patents", whose usage restrictions constitute "a deadweight loss to society".[133] Extremely long economic and moral provisions "premised on a neoclassical theory of copyright"[134] have been placing "monopoly control in the hands of heirs and transferees who [...] become privileged and sometimes arbitrary custodians of culture".[135] Such dominant protection afforded to European rightsholders undermines the production of new knowledge in the humanities and the textual scholarship research ecosystem, rendering scientific publication practically unfeasible or reduced to few derived data at best.[136]

47 This circumstance compromises "the free exchange and criticism of ideas [...] at the core of academic freedom",[137] which is "recognised as a

quotations from unpublished material after receiving multiple threats from Mr. Joyce. When Shloss informed the estate that she intended to create a website that would contain the deleted quotations placed within a scholarly context, the Estate forbade the project as unauthorized and infringing. Having engaged legal counsel [...], Shloss filed an action against the estate in a California federal court, seeking a declaration that her proposed website made fair use of the copyrighted materials and that the estate's actions with respect to her and other scholars over the years constituted copyright misuse. [...] After losing its motion to dismiss, [...] the Joyce estate agreed to a settlement whereby Shloss was able to place on her website all of the quoted material she had planned to include, and to make additional uses of the material that she had not sought in her complaint" (Spoo, 'Ezra Pound's Copyright Statute: Perpetual Rights and the Problem of Heirs' 1826).

127 Spoo, 'Copyrights and "Design-Around" Scholarship' 576.

128 Ibid 566.

129 Ibid 564.

130 Dirk Van Hulle, 'Modelling a Digital Scholarly Edition for Genetic Criticism: A Rapprochement' (2016) 12-13 Variants 34-56 <https://doi.org/10.4000/variants.293> accessed 10 July 2023.

131 "In international copyright law, the 'three-step test' restricts the ability of states to introduce, and maintain, exceptions to the exclusive rights of authors and other right-holders. Under its well-known terms, exceptions are only permitted (1) in certain special cases; (2) which do not result in a conflict with the normal exploitation of a work and (3) which do not unreasonably prejudice the legitimate interests of the author (or other right-holder). Originating in the 1967 Stockholm Conference revision of the Berne Convention, this formula now forms an integral part of several international agreements concerning copyright and related rights and has been applied as a constraint on the availability of exceptions to the exercise of other forms of intellectual property right at international level. The 'test' has also recently come to play a significant role in domestic copyright laws" – Jonathan Griffiths, 'The "Three-Step Test" in European Copyright Law: Problems and Solutions' (2009) 4 Intellectual Property Quarterly 428-457 <https://ssrn.com/abstract=1476968> accessed 27 August 2023.

132 Ryan, 'Fair Use and Academic Expression' 541.

133 Spoo, 'Copyrights and "Design-Around" Scholarship' 564.

134 Ryan, 'Fair Use and Academic Expression' 590.

135 Spoo, 'Ezra Pound's Copyright Statute: Perpetual Rights and the Problem of Heirs' 1827.

136 It goes without saying that the suppression of the words contained in the document or other scholarly use of "ultra-safe substitutions for literary art [...] does not inject a functional equivalent into the intellectual" activity of our disciplinary field (Spoo, 'Copyrights and Design-Around Scholarship' 578).

137 Spoo, 'Copyrights and Design-Around Scholarship' 590. Although "there is little consensus as to what academic freedom means" (Moscon, 'Academic Freedom, Copyright, and Access to Scholarly Works' 103), according to Michael W. McConnell "[t]he term refers both to the freedom

fundamental right by several national constitutions and international treaties".[138] The examples and scenarios presented above demonstrate that the academic freedom of literary and textual scholars has often been challenged by interferences and obstructions that perversely amount to submitting scholarly research to the agendas of copyright owners. Therefore, in the interest of research and study, we shall join in pleading for policy-making adjustments to ensure more effective limitations to the lengthy copyrights executed by heirs and successors.

48 Firstly, the provisions in art 59 (3) and art 58 of the Portuguese Code of Copyright need to be revised to adequately safeguard the author's literary legacy and the community's cultural heritage. Secondly, we need to extend the scope of the available exceptions in art 75 of the Code of Copyright to allow for scholarly publication in the digital age – or otherwise, a legal license designed with scholarship in mind so that academic researchers may work with published texts and holographic materials in public archive librarie, disclosing research results (in person, on paper, and online) without interference from heirs or successors. Moreover, we also need national or European management systems led by independent copyright boards to facilitate the clearance of orphan works for different uses and reduce the randomness of our current authorisation system.[139] Until these and further measures are implemented to solve the problem, academic research will remain perilous and risky for anyone investigating textual variance in the works of 20th- and 21st-century writers.

of the individual scholar to teach and research without interference (except for the requirement of adherence to professional norms, which is judged by fellow scholars in the discipline) and to the freedom of the academic institution from outside control" – Michael W. McConnell, 'Academic Freedom in Religious Colleges and Universities (1990) 53 Law and Contemporary Problems 305 <https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=4058&context=lcp> accessed 26 August 2023. For an introduction to the theory of academic freedom, see also Ryan, 'Fair Use and Academic Expression' 573-576.

138 Moscon, 'Academic Freedom, Copyright, and Access to Scholarly Works' 103. Moscon notes that art 13 of the Charter of Fundamental Rights of the European Union, for instance, establishes that "[t]he arts and scientific research shall be free of constraint" (Ibid 104), and "[a]t the European national level, academic freedom [...] is usually afforded separate protection in the Constitution" (Ibid 105), as happens in Portugal (Constitution of the Portuguese Republic, 7th Revision [2005], pt I, title III, ch III, art 73 [4] <https://www.parlamento.pt/sites/EN/Parliament/Documents/Constitution7th.pdf> accessed 25 August 2023).

139 See the essays by Robert Spoo – 'Ezra Pound's Copyright Statute: Perpetual Rights and the Problem of Heirs' 1828-1831 – and David Hansen – 'Orphan Works: Mapping the Possible Solution Spaces' – for more specific proposals on balancing long copyrights with the needs of the public.

Digital Exhaustion: A Decade After the UsedSoft Case

by **Petr Kalenský** *

Abstract: Digital exhaustion has been a recurring theme in EU copyright law. While some may argue that the ruling of the Court of Justice of the European Union (CJEU) in the Tom Kabinet case definitively solved the surrounding questions, this paper takes the opposite stance. It offers a critical analysis of the CJEU's major decisions in a decade-long legal saga and examines the current status quo from the perspective of copyright exhaustion in the context of copyright law. The paper pleads for a balanced approach to digital exhaustion in the modern age as the current ruling of the CJEU has resulted in a clear shift of balance in favor of the rightsholders at the expense of users and other stakeholders in the market with copyright-protected works.

Keywords: Copyright Exhaustion, Digital Exhaustion, UsedSoft, Tom Kabinet

Recommended citation: Petr Kalenský, Different Digital Exhaustion: A Decade After the UsedSoft Case 14 (2023) JIPITEC 525 para 1.

A. Introduction

1 The story of digital exhaustion under EU copyright law begins more than ten years ago, on the 3rd of July 2012. On this day, the Court of Justice of the European Union ("**CJEU** ") delivered its highly anticipated ruling in the case C-128/11 *UsedSoft GmbH v Oracle International Corp.* ("***UsedSoft* case**"). In its ruling, the CJEU concludes that the distribution right and its exhaustion may apply to digital (intangible) copies of computer programs. At the time, it could seem as if the metaphorical nail had been hammered into the coffin of the traditional understanding of the distribution right and its exhaustion, as being exclusively bound to the realm of tangible objects.[1] In hindsight, it is obvious that while the

* The author is a Ph.D. candidate in the IP Law program of the Masaryk University Law School and a law firm associate focused on IP law. The author would like to thank Matěj Myška for his kind support and valuable feedback in the process of writing this paper. This article is the result of the project of the Grant Agency of the Czech Republic [Copyrighted Works and the Requirement of Sufficient Precision and Objectivity (GA22-22517S)].

1 Emma Linklater, 'UsedSoft and the Big Bang Theory: Is the e-Exhaustion Meteor about to Strike' (2014) 5 (1) Journal of Intellectual Property, Information Technology and

UsedSoft case and subsequently the decision in the case C-263/18 *Nederlands Uitgeversverbond and Groep Algemene Uitgevers* ("***Tom Kabinet* case**") certainly left a strong impression, their actual impact in accommodating the EU copyright law framework to the new, digital age and in balancing the rights of various stakeholders active in the digital markets with copyright-protected works, is limited.

2 To set the stage for further analysis, this paper begins by outlining and critically assessing the individual chapters of the digital exhaustion saga, as created by the CJEU in its decisions over the years. Through a critical assessment of the CJEU's jurisprudence, it is evident that the story of digital exhaustion is everything but straightforward; the story contains inconsistencies and flaws, and importantly, remains without a satisfying resolution even after over a decade since its beginning. Thereby, the initial parts of this paper outline the current regulatory status quo surrounding digital exhaustion under EU law. This analysis shows that the rationales driving copyright exhaustion in the traditional markets with copyright-protected works are no longer emphasized in the digital age. In its following parts, the paper asserts that while the technological environment has changed *significantly* since the inception of copyright exhaustion, a substantial part of the rationale underlying the principle of exhaustion may be viewed as highly relevant in the modern day and in some cases in fact, it may be as relevant as ever.

B. The Genesis of Digital Exhaustion in the Case Law of the CJEU

I. UsedSoft case as the Big Bang

3 The *UsedSoft* case has brought about the big bang setting off the more than a decade-long saga of discussions in the EU. The case concerned Oracle, a software development company, which supplied a databank software in 85% of cases by download through the internet.[2] Oracle granted the license through a licensing agreement and included the right to store a copy of the program permanently on a server and to allow a certain number of users to access it by downloading the software to their computers. The licensing fee entailed a lump sum payment and the license was granted as perpetual, non-exclusive, and non-transferable.[3] UsedSoft GmbH, a company focusing on the resale of "used" software licenses, has purchased such licenses from the customers of Oracle. The essential question referred for a preliminary ruling subsisted in assessing whether the supply by a download of a computer program, for an unlimited period, subject to the payment of a lump-sum fee, may be considered as an exercise of the distribution right and if so, whether the abovementioned supply exhausts the distribution right. To the surprise of many, the answer of the CJEU to both questions has been affirmative. The decision in the *UsedSoft* case may be considered revolutionary due to the striking attempt of the CJEU to assimilate the "traditional" and digital markets with computer programs and generally, its innovative, technologically neutral approach aimed at helping to create a more flexible copyright framework or, more precisely, adapting it to the rapid technological shift of the preceding decades. That said, the means by which the decision in the *UsedSoft* case paves the way for such flexibility is unfortunate and contains too many flaws and inconsistencies to provide a solid foundation for the adaptation of the distribution right and the exhaustion doctrine to the digital age.

1. Scope of the Relevant Rights

4 In the decision, the CJEU pays little attention to the assessment of which exclusive rights are actually involved in the supply of a computer program for permanent use by download. The CJEU skips this analysis and instead, begins its reasoning with where the distribution right ends, rather than where the applicable right begins. This is striking in hindsight, as the CJEU later demonstrated in the *Tom Kabinet* case that answering the latter question is no straightforward task. Rognstad notes that this failure to consider whether the distribution right even applies to the facts of the case might be, among other, caused by the formulation of questions posed to the CJEU by the German Court.[4] However, in the subsequent decision in the *Tom Kabinet* case, the reformulation of the questions posed by the Dutch court in order to first discuss the applicable right did not seem to form an issue for the CJEU.[5]

Electronic Commerce Law < https://www.jipitec.eu/issues/jipitec-5-1-2014/3903/jipitec_5_1_linklater.pdf>

2 Case C-128/11, *UsedSoft GmbH v Oracle International Corp.* (CJEU, 3 July 2012), para 21.

3 Ibid.

4 Ole-Andreas Rognstad, 'Legally Flawed but Politically Sound: Digital Exhaustion of Copyright in Europe after UsedSoft' (2014) 1 Oslo Law Review 1.

5 In the *Tom Kabinet* case, the questions of the Dutch court focused solely on considerations regarding the distribution right. The answers of the CJEU, however, focused on the communication to the public right.

5 From the wording of the applicable law, there are solid arguments for the conclusion that the distribution right and its exhaustion, irrespective of whether relating to computer programs or other protected works, are limited exclusively to tangible copies incorporating such works. The link between distribution right and requirement of tangibility of copies is rooted in the relevant provisions of the WIPO Copyright Treaty ("**WCT**") and the Agreed Statements concerning the WIPO Copyright Treaty ("**Agreed Statements**"). The WCT does not distinguish between the different types of protected works in the questions surrounding the distribution right. The Agreed Statements are further unambiguous in stating that the key term "copies" refers *"exclusively to fixed copies that can be put into circulation as tangible objects".*[6] The conclusion of the CJEU that the tangibility requirement does not apply to the distribution of computer programs helps the equal treatment of offline and online secondary dispositions with copies of computer programs and thereby balancing the rights and interests of various stakeholders in the market with protected works. However, rather than explicitly stating that the CJEU opted for a teleological, technologically neutral approach rather than the strict adherence to the wording of the applicable law, the CJEU based its argumentation, to a large extent, on the construction of the *lex specialis* statutory mosaic. The *lex specialis* argument is unfortunate for at least two reasons. Firstly, it is inconsistent with the applicable law, as the WCT and the Agreed Statements equally apply to computer programs, since no distinction is made with regard to the distribution of copies of a computer programs and other works protected by copyright. Secondly, as shown in later cases, this line of argumentation may form a significant hurdle for the balanced application of the exhaustion doctrine in the digital age.

2. The Lex Specialis Argument: A Clunky Tool for Assimilation of Intangible Copies

6 In the *UsedSoft* case, the CJEU draws a divide between the *lex generalis*, the Directive 2001/29/EC, on the harmonisation of certain aspects of copyright and related rights in the information society ("**InfoSoc Directive**") and the *lex specialis,* the directive 2009/24/EC on the legal protection of computer programs ("**Software Directive**"). It is precisely this divide that, according to the CJEU, enables interpreting the term "copy" under the Software Directive as including computer programs not incorporated into a tangible object. The CJEU argues under paras 55 through 59 of the *UsedSoft* case that it does not appear from Article 4 (2) of the Software Directive that the distribution right under the Software Directive is limited to tangible copies and that Article 4 remains silent on this issue. The CJEU further emphasizes that the Software Directive aims to protect computer programs in any form, including those incorporated into hardware.[7] The CJEU's conclusion is that the European legislator clearly intends to assimilate both tangible and intangible copies into that provision of the Software Directive. However, it is precisely the silence of the Software Directive, which, from the literal reading of the relevant law speaks against the assimilation of intangible copies under the Software Directive, rather than for it. The Software Directive simply sets forth no provisions to override the conditions for the application of the distribution right and its exhaustion under the InfoSoc Directive and the WCT. The provisions of the Software Directive invoked by the CJEU, interpreted by the CJEU as superseding the relevant provisions of the WCT and the InfoSoc Directive, such as the mentioned Article 1(2) of the Software Directive do no such thing. Article 1(2) of the Software Directive states that "*Protection in accordance with this Directive shall apply to the expression in any form of a computer program*" (emphasis added) and should be interpreted as merely stating that any form of expression of a computer program, as a specific literary work, which may be represented through various means, such as the source code or the machine code of the computer program, is protected. This provision alone says close to nothing about the scope of the distribution right and its exhaustion. The CJEU's conclusion to the contrary strikes as inconsistent with other landmark cases dealing with the distribution right and the exhaustion thereof, such as the decisions in cases C-456/06 *Peek & Cloppenburg KG v Cassina SpA* or the case C-419/13 *Art & Allposters International BV v. Stichting Pictoright*. In these cases, the CJEU emphasizes the importance of the interpretation of EU law provisions in line with the obligations of the EU arising from international treaties, such as the WCT (and the Agreed Statements). Apart from that, the foundation for the application of the distribution right in the digital world based on the *lex specialis* divide is, as shown by the later development, a very shaky foundation indeed for a balanced application of the exhaustion doctrine in the digital age.

3. The UsedSoft Conditions

7 CJEU set forth the following conditions that need to be fulfilled for the distribution right to a copy

6 Agreed Statements concerning the WIPO Copyright Treaty adopted by the Diplomatic Conference on December 20, 1996, Agreed Statement concerning Articles 6 and 7.

7 *UsedSoft* case (n 2), para 57.

of a computer program to be exhausted under the Software Directive:

- a copy (tangible or intangible) of a computer program must be placed on the market in the European Union by the copyright holder or with its consent; through a
- sale (also including a perpetual license paid for by a lump-sum fee, by which the licensor gains a remuneration corresponding to the economic value of the copy); provided that
- the original acquirer makes his own copy unusable at the time of its resale.

8 Apart from the conditions stated above, the CJEU also supported its arguments by invoking the functional equivalence of online supply to the supply on a tangible medium in the present case.[8] While the concept of functional equivalence is a theme echoing in the subsequent case law of the CJEU, the theme is applied inconsistently in the subsequent case law of the CJEU, as shown below.

4. The "Sale" Criterion

9 One of the conditions allowing exhaustion to occur with respect to the distribution of computer programs is one of "sale" of the copy of the computer program. In simple terms, the underlying transaction must result in a transfer of ownership in that copy.[9] Oracle, quite understandably, argued that no actual sale took place, as Oracle made a copy of the program available for download free of charge, along with the conclusion of a license agreement, granting the user with non-exclusive and non-transferable user right for an unlimited period for that program. The CJEU disagreed. According to the CJEU, both of these steps in the context of the case render the transaction a sale.[10] The CJEU further refers to the argumentation that the term "sale" must be interpreted broadly, as "*encompassing all forms of product marketing characterised by the grant of a right to use a copy of a computer program, for an unlimited period, in return for payment of a fee designed to enable the copyright holder to obtain a remuneration corresponding to the economic value of the copy of the work of which he is the proprietor*"[11] otherwise, the effectiveness of copyright exhaustion could be undermined.[12] According to the CJEU, it is precisely the existence of a transfer of ownership, which, according to the CJEU, converts an act of communication to the public under Article 3 of the InfoSoc Directive into an act of distribution under Article 4.[13]

5. The Obligation of the Original Acquirer to Make its Copy Unusable

10 In order for exhaustion to occur, the original acquirer must make its own copy unusable at the time of its resale, in order to avoid infringing the exclusive right of reproduction of a computer program belonging to its author, laid down in Article 4(1)(a) of the Software Directive.[14] While the purpose of this condition is clear and the condition itself is necessary in order to be able to treat digital and tangible copies equally, a counterargument presents itself in that making a copy unusable, after a new copy has been made is not decisive in the assessment of whether reproduction right has been infringed upon, as at one point in time, a new reproduction has been made and the other one had been created. The CJEU case law seems not to consider the reproduction right a vital part of the applicable rights equation, as most considerations revolve around the distribution and communication to the public rights. This approach varies significantly from the practice in the United States, *e.g.*, in the equally famous *ReDigi* case[15] and in the related appellate decision of the US Court of Appeals for the Second Circuit.[16]

6. Living in the Post-UsedSoft Universe

11 Although many saw the *UsedSoft* case as an open door to the adoption of digital exhaustion regarding protected works outside the scope of the Software Directive, the decision had quite the opposite effect. While the decision employs a teleological, technologically neutral approach, which could indeed be helpful in accommodating copyright law to the new age, it created a deep legislative divide

8 *UsedSoft* case (n 2), para 61.

9 ibid., para 42.

10 ibid., para 84.

11 ibid., para 49.

12 ibid.

13 ibid, para 52.

14 *UsedSoft* case (n 2), para 70.

15 Decision of United States District Court for the Southern District of New York of 30 March 2013, *Capitol Records, LLC v. ReDigi Inc*.

16 Decision of United States Court of Appeals for the Second Circuit of 12 December 2018, *Capitol Records, LLC v. ReDigi Inc*.

between the regimes of the distribution right under the Software Directive and under the InfoSoc Directive, effectively excluding digital exhaustion for works outside of the scope of protection of the Software Directive.

12 In the end, the application of the conclusions of the *UsedSoft* case in the following cases dealing with computer programs was not without issues. By way of example, in the subsequent proceedings before national courts in Germany. One can quite easily imagine the excitement among UsedSoft's legal counsels on the summer day the CJEU promulgated its decision in the case. One can also imagine the disappointment when after receiving the decision in the *UsedSoft* case, the case is not won in the proceedings back before the national courts. Revolutionary as it may be, the *UsedSoft* case laid down a set of conditions, the fulfilment of which proved to be rather difficult to support with sufficient evidence. In the national proceedings, the German courts held that to claim exhaustion as a limitation of the distribution right, UsedSoft bore the burden of proof regarding the fulfilment of conditions set forth by the *UsedSoft* case. In particular, UsedSoft failed to prove that Oracle had given consent to the download of a copy of the computer program against payment of a license fee, that Oracle had granted a right to a permanent use to the particular copies of programs, that the original acquirer made its own copies unusable at the moment of resale; and finally, that the new acquirer only uses the software within the boundaries of the terms of the original licensing terms. Consequently, UsedSoft agreed to a cease-and-desist undertaking, thus bringing the long-standing German UsedSoft saga to an end.[17]

13 The *UsedSoft* case seems to have raised more questions than answers by strengthening the split of the relevant legislation into two realms – the realm of "traditional" copyright works, embodied in the InfoSoc Directive and one of the computer programs, under the Software Directive. The CJEU pursued a commendable goal in adapting copyright law to the new technological reality, however, it chose unfortunate means for this undertaking. Ole-Andreas Rognstad describes the *UsedSoft* case as legally flawed but politically sound.[18] Sven Schonhofen notes, in an equally fitting manner, that "*facts plus policy = results = doctrine.*"[19] Interestingly enough, the CJEU did not get to tackle digital exhaustion directly on many more occasions after the *UsedSoft* case. However, there are several subsequent decisions of the CJEU, at least partially completing the fragmented picture of digital exhaustion under EU law.

II. Meeting of the Lex Specialis and the Lex Generalis

14 Case C-355/12 *Nintendo v. PC Box* ("***Nintendo* case**") is not, on its face, a digital exhaustion case, but a case concerning technological measures.[20] However, along with DRMs, the CJEU examined the nature of videogames as works protected by copyright. That is, whether videogames, as copyright-protected works, fall within the scope of the InfoSoc Directive only, or whether they belong under the umbrella of the Software Directive. According to the CJEU, video games constitute complex matter comprising not only a computer program but also graphic and sound elements, which, although encrypted in a computer language, have a unique creative value that cannot be reduced to such encryption.[21]

15 Insofar as the parts of a videogame (in this case, the graphic and sound elements) are part of its originality, they are protected by copyright together with the entire work, in the context of the system established by the InfoSoc Directive.[22] Containing creative elements, the value of which cannot be reduced to their encryption in a computer language, is not a robust distinguishing characteristic of video games when compared to computer programs in their pure form. Undoubtedly, video games usually contain a higher quality of these elements than "regular" computer programs. However, the bar for copyright protection under EU copyright law, as set, *i.e.*, by case C-5/08, *Infopaq International A/S v Danske Dagblades Forening*[23], is much lower. Furthermore, the CJEU expressly states in the case C-393/09 *Bezpečnostní softwarová asociace – Svaz softwarové ochrany v. Ministerstvo kultury* that a graphical interface can be protected by copyright as a work under the InfoSoc

17 'The End of the UsedSoft Case and Its Implications for "Used" Software Licences' (*Osborne Clarke*) <https://www.osborneclarke.com/insights/the-end-of-the-usedsoft-case-and-its-implications-for-used-software-licences> accessed 8 January 2023.

18 Rognstad (n 4).

19 Sven Schonhofen, 'Usedsoft and Its Aftermath: The Resale of Digital Content in the European Union' (2015) 16 Wake Forest Journal of Business and Intellectual Property Law 262, 277.

20 Case C-355/12, *Nintendo Co. Ltd, Nintendo of America Inc., Nintendo of Europe GmbH v. PC Box Srl, 9Net Srl* (CJEU, 23 January 2014).

21 *Nintendo* case (n 20), para 23.

22 *Nintendo* case (n 20), para 23.

23 Case C-5/08, *Infopaq International A/S v Danske Dagblades Forening* (CJEU, 16 July 2009).

Directive, if it is an own intellectual creation of an author.[24] At the time, at least two points could be distilled from the decision in the *Nintendo* case with regard to digital exhaustion.

16 The first point is that the CJEU insists on expanding the *lex specialis* argument elaborated in the *UsedSoft* case. The divide discussed above is strengthened, as according to the *Nintendo* case, the protection under the Software Directive is only available for "pure" computer programs (which will not be commonplace in practice). The opinion of AG Sharpston further supports this line of argumentation. In her view, the Software Directive takes precedence over the provisions of the InfoSoc Directive only where the protected material falls entirely within the scope of the former.[25] She further adds that: "*If Nintendo and Nintendo-licensed games were computer programs and no more, Directive 2009/24 would therefore apply, displacing Directive 2001/29. Indeed, if Nintendo applied separate technological measures to protect the computer programs and the other material, Directive 2009/24 could apply to the former, and Directive 2001/29 to the latter.*"[26]

17 What the above means in connection to the application of the distribution right and the exhaustion thereof to complex matters is still not settled.[27] Two approaches come to mind in the light of the *Nintendo* case, and neither is without flaws. One approach, which treats videogames as a subject matter wholly regulated by the InfoSoc Directive, granting exhaustion to distribution of tangible copies of videogames only. The second approach, treating different parts of the videogame differently, meaning that parts of the videogame falling under the protection of the InfoSoc Directive are assessed according to this directive and the parts of the videogame subsisting in "pure" computer programs would be assessed according to the Software Directive. But the latter granular approach becomes even more complicated after the brief assessment of complex matters as a concept in the *Tom Kabinet* case, where the CJEU took the position that for the subsumption of the subject-matter under the umbrella of the correct directive, it must be assessed whether the computer program plays merely an incidental role in the complex matter.[28] Therefore, if a computer program forms only an incidental element of the complex matter-work at hand, the application of the Software Directive is excluded. *A contrario*, it indicates that in case the computer program element of the complex matter at hand is not merely incidental, the Software Directive applies. Regardless of the result of the above application dilemma, one thing remains rather clear. The granular approach, which would assess each of the elements of complex matter with regard to exhaustion of the distribution right separately, *i.e.*, under the rules of different directives, is close to inconceivable from the view of practical reliance on copyright exhaustion and legal certainty, which forms one of the fundamental foundations of the exhaustion principle as a legal concept. If only certain parts (computer programs) of a highly complex, digital, copyright-protected matter, such as a modern-day videogame, would be deemed exhausted and other traditional protected works would not, it would make any reliance on exhaustion highly complicated, if not impossible. Such an approach would, therefore, go starkly against the purpose of exhaustion discussed in the latter parts of this paper.

III. VOB: A Confusing, yet Technologically Neutral Glimpse of Hope?

18 Although one could very well argue that the landscape surrounding digital exhaustion is complex already in the light of the case law discussed above, case C-174/15 *Vereniging Openbare Bibliotheken v Stichting Leenrecht* ("***VOB* case**") adds to this complexity.

19 In summary, the Dutch court sought the answers to the following two questions:

- whether e-book lending falls under the umbrella of the lending right under the directive 2006/115 on rental right and lending right and on certain rights related to copyright in the field of intellectual property; and
- whether it is in accordance with the EU law, if the laws of a member state introduce a condition on the application of the restriction on the lending right, subsisting in the fact that the copy of the work made available by the establishment must have been brought into circulation by an initial

24 Case C-393/09, *Bezpečnostní softwarová asociace – Svaz softwarové ochrany v Ministerstvo kultury* (CJEU, 22 December 2010), para 51.

25 *Nintendo* case (n 20), para 34.

26 ibid.

27 See, *e.g.*, Alina Trapova and Emanuele Fava, 'Aren't We All Exhausted Already? EU Copyright Exhaustion and Video Game Resales in the Games-as-a-Service Era' (2020) 3 Interactive Entertainment Law Review 77.

28 Case C-263/18, *Nederlands Uitgeversverbond, Groep Algemene Uitgevers v Tom Kabinet Internet BV, Tom Kabinet Holding BV, Tom Kabinet Uitgeverij BV*, (CJEU, 19 December 2019), para 59.

> sale or other transfer of ownership of that copy within the European Union by the rightsholder or with his consent within the meaning of Article 4(2) of Directive 2001/29.[29]

20 To the first of the questions, the CJEU held that there are no grounds for excluding e-books from the scope of the lending right. The CJEU avoids the issue of the link between tangibility and the term "copies" within the WCT by diligently distinguishing between the rental and lending rights. This allowed the CJEU to hold that neither the WCT nor the Agreed Statements proscribe the concept of "lending" from being interpreted as also including e-book lending.[30] While the answer to the first question is not particularly controversial, the same cannot be said about the answer to the second question posed to the CJEU, which may have surprised many inhabitants of the post-*UsedSoft* universe.

21 The CJEU had answered that nothing in the EU law precludes the introduction of the above condition, subsisting in nothing less than digital exhaustion, under the national law of Member States.[31] This conclusion may, at first glance, be seen as good news for digital exhaustion under the InfoSoc Directive, since the CJEU essentially concludes that the Member States may legislate for digital exhaustion regarding e-books – otherwise, the existence of a condition in question would be nonsensical. While the decision itself and the opinion of the AG contains many arguments oriented at technological neutrality, which were subsequently not considered in the following *Tom Kabinet* case, the decision in the *VOB* case should not be seen as a "pro-digital exhaustion" decision for the reasons discussed below.

22 The critical part of the reasoning behind the *Tom Kabinet* case may be seen in para 85 of the opinion of AG Szpunar, in which the AG states that in case that lending or rental rights are acquired with the consent of the author, it may be assumed that the author's interests are sufficiently protected and on the contrary, where there is a reliance on the derogation from an exclusive right, such interests of the rightsholder may be in jeopardy.[32] The CJEU holds that such a condition for the applicability of the derogation from an exclusive right is capable of reducing those risks.[33] Therefore, the CJEU's analysis revolves not around the usual purposes ascribed to copyright exhaustion, such as the limitation of control of the rightsholder over secondary transactions (after having the opportunity to receive adequate remuneration). The decision further does not at all assess whether digital exhaustion is even conceivable under the explicitly referred to InfoSoc Directive. The reasoning of the *VOB* case revolves almost exclusively around the question of whether introducing the condition provides the rightsholders with more protection. In simpler terms, the CJEU concludes that adding a step to the application of a limitation (and therefore, to a use of a protected work without the authorization of the relevant rightsholder) strengthens the position of the rightsholder.

23 For this reason, the *VOB case* should not primarily be read as a pro-digital exhaustion decision, but a pro-rightsholder decision. The equation, as the CJEU presents it, seems to be merely:

> *more complicated access to a limitation = more rightsholder protection = in accordance with the EU law.*

24 Considering the amount of controversy surrounding digital exhaustion, the fact that not a single word of the argumentation in the *VOB* case was devoted to considerations concerning the relationship between digital exhaustion and Article 4 (2) of the InfoSoc Directive, is puzzling. With the knowledge of the following decision in the *Tom Kabinet* case, Sganga calls the co-existence of the *VOB* case and the *Tom Kabinet* case a systematic mystery.[34] It is easy to agree with this assessment.

IV. Tom Kabinet: A Door Closed Shut (?)

25 If the wait for the outcome of the *UsedSoft* case was full of suspense, the wait for the *Tom Kabinet* case was a cliffhanger for all of those hoping for, at the very least, an interim ending of the EU digital exhaustion saga. By the *Tom Kabinet* case, the existing judicial and legislative patchwork could be made whole in one way or another. Instead, the CJEU presented yet another set of steps in what Mezei calls an "*an exhausting dance exercise, in which the court takes a few*

29 Case C-174/15, *Vereniging Openbare Bibliotheken v Stichting Leenrecht* (CJEU, 10 November 2016), para 65.

30 ibid., para 39.

31 ibid., para 65.

32 *VOB* case (n 29), opinion of AG Szpunar para 85.

33 *VOB* case (n 29), para 64.

34 Caterina Sganga, 'Is the Digital Exhaustion Debate Really Exhausted? Some Afterthoughts on the Grand Chamber Decision in Tom Kabinet (C-263/18)' (*Kluwer Copyright Blog*, 19 May 2020) <http://copyrightblog.kluweriplaw.com/2020/05/19/is-the-digital-exhaustion-debate-really-exhausted-some-afterthoughts-on-the-grand-chamber-decision-in-tom-kabinet-c-263-18/> accessed 7 January 2023.

steps right and a few steps left".[35] The facts of the case, along with the submitted preliminary questions seemed to form a perfect storm for the resolution of lingering questions surrounding digital exhaustion in the regime of the InfoSoc Directive. Likely, the Dutch Court shared this view, judging from the wording of preliminary questions posed, focusing on the distribution right and its exhaustion in the digital environment under the InfoSoc Directive.

26 The Dutch court asked, among other, whether, in the opinion of CJEU:

- the supply of an e-book by download for use for an unlimited period of time at a price constitutes an act of distribution within the meaning of article 4 (1) of the InfoSoc Directive; and
- whether such an act can trigger the exhaustion of the distribution right.

27 Possibly spoiling suspense for the reader, this paper begins the analysis with the outcome of the case. The CJEU concluded that the supply of an e-book by download for use for a period of time at a price constitutes an exercise of the right of communication to the public rather than the exercise of the distribution right. Although the CJEU mentions the *UsedSoft* case explicitly, the CJEU does not, in fact, follow the same line of interpretation of the relevant directive provisions, as shown below.

1. The Wording of the Law and the Historical Intent

28 One of the stark contrasts between the interpretative approach of the CJEU in the *UsedSoft* case and the *Tom Kabinet* case is that the latter decision does not pose the question of whether the assessed transaction involves a transfer of ownership within the meaning of the *UsedSoft* case. This is surprising, as it was precisely the deemed existence of a transfer of ownership, in a case including a licensing agreement, which changed, in the view of the CJEU, an act of communication to the public into an act of distribution.[36] Instead, the CJEU focuses on the aim of the InfoSoc Directive stated, in the recital (15) thereof, subsisting in the implementation of WCT obligations. As described above, the minimum "floor" of substantive protection set by the WCT and the Agreed Statements is unambiguous in creating a link between the exclusive right of distribution, its exhaustion and the tangibility requirement. The Court follows this newly found emphasis with the analysis of the explanatory memorandum to the InfoSoc Directive, which, according to the CJEU, makes it clear that "*any communication to the public of a work, other than the distribution of physical copies of the work, should be covered not by the concept of distribution to the public.*"[37] CJEU invokes the recitals of the InfoSoc Directive and identifies two objectives of the InfoSoc Directive contained therein. Firstly, creating a general and flexible framework at the EU level to foster the development of the information society and for the copyright to respond to technological development brought novel ways of exploiting protected works.

29 Nevertheless, one must not forget other goals, such as the goal contained in the recital (31) of the InfoSoc Directive, which aims to safeguard a fair balance of rights interests between the different categories of rightsholders, as well as between the different categories of rightsholders and users. How the CJEU reconciles these two competing objectives paints the stark contrast between the *UsedSoft* case and the *Tom Kabinet* case. These goals and their reconciliation are in no way specific to EU copyright law, as the provisions of the recitals reflect the purposes of copyright law and the underlying balancing aspect of copyright law as such.

30 In the *UsedSoft* case, while keeping in mind the latter objective in the form of balancing and the rightsholders being able to obtain adequate remuneration, the CJEU takes a very flexible, functionally oriented approach, going over and possibly even against the wording of the applicable law in order to achieve a technologically neutral solution - assessing that the transaction at hand constituted a transfer of ownership when formally, the transaction in question was a grant of a license, rather than a sale. Accordingly, the CJEU holds that the right of distribution and its exhaustion applies.

31 Conversely, in the *Tom Kabinet* case, the CJEU sticks to the literal interpretation of the law along with arguments subsisting in the legislator's historical intent, emphasizing almost exclusively the objective of the high level of protection of the rightsholder. In order to achieve this goal, the CJEU states that the right of communication to the public must be understood broadly as encompassing all communication to the public not present at the place

35 Péter Mezei, 'The Doctrine of Exhaustion in Limbo - Critical Remarks on the CJEU's Tom Kabinet Ruling' (2020) 148 ZESZYTY NAUKOWE UNIWERSYTETU JAGIELLONSKIEGO PRACE Z PRAWA WLASNOSCI INTELEKTUALNEJ, 130. "plainCitation":"Péter Mezei, 'The Doctrine of Exhaustion in Limbo - Critical Remarks on the CJEU's Tom Kabinet Ruling' (Social Science Research Network 2020

36 *Tom Kabinet* case (n 28), para 52.

37 ibid., para 45.

where the communication originates.[38] While the concerns regarding the compliance of the *UsedSoft* case with the wording of the law were shared above, the adoption of a polar opposite interpretative approach in the form of the conclusions of the *Tom Kabinet* case creates even more uncertainty in an area of law that is far from clear. Firstly, the strong (and after the decisions in the *UsedSoft* and *VOB* cases, rather surprising) insistence on the historical intent does not exactly facilitate the mentioned goal of adapting the copyright law framework to the current digital reality and striking a balance between the various groups of stakeholders in the market with protected works. Each of the documents invoked by the CJEU far predates a point in time, where the business model of *Tom Kabinet* or a similar business models would even be conceivable, and the digital market was a concept still in its beginnings. As such, it formed a more or less niche alternative to the distribution of tangible carriers to watch out for in the future.

32 Secondly, while it is clear that the high level of protection of rightsholders is one of the leading objectives of copyright law within the EU, it is not the only objective shaping the outline of EU copyright law and it must be balanced with the rights and interests of other stakeholders in the market with protected works.

2. Scope of the Directives

33 Aware of the existing ambiguity surrounding the scope of the InfoSoc Directive and the Software Directive, the CJEU reiterates the *lex specialis* argument contained in the *UsedSoft* case in stating that the regime of the Software Directive cannot be applied to a case concerning e-books. Dealing with considering e-books as a complex matter, the CJEU mentions the incidental role of computer programs in e-books. Let us recall the CJEU invoking the Article 1 of the Software Directive in the *UsedSoft* case and its broad definition of the protected subject-matter under the directive. The Software Directive states that computer programs, including the preparatory materials, are to be protected as literary works, whereas the protection includes the expression of a computer program in any form. The only criterion for protection in Article 1 (3) of the Software Directive being that the work is original, in the sense that it is an own intellectual creation of the author. Paragraph 3 then states expressly that no other criteria shall be applied to determine eligibility for protection. According to the Software Directive, the incidental or non-incidental role of a computer program makes no difference in whether or not the computer program is eligible for protection under that directive. Furthermore, if the argumentation of AG Sharpston in the *Nintendo* case was to be followed in the *Tom Kabinet* case, the CJEU would have to deal with two parts of the equation – the elements falling under the InfoSoc Directive and the computer program elements falling under the Software Directive.

3. Equivalence and equal treatment

34 CJEU further analyses the transaction at hand through the prism of functional and economic equivalence. These two concepts form a leading argument in the CJEU case law for the introduction of digital exhaustion regarding computer programs under the Software Directive, but also a leading argument against it concerning works protected under the InfoSoc Directive. The approach of the AG and the CJEU in the *Tom Kabinet* case differs fundamentally. The CJEU and the AG mention functional equivalence, however, the reasoning of the case revolves around economic equivalence. While seemingly taking into consideration the *UsedSoft* case line of reasoning, the approach of the CJEU is different. Should the functional equivalent approach (*UsedSoft* case) be applied in the *Tom Kabinet* case, the CJEU would first, as it did in the *UsedSoft* case, consider, prior to the application of the right of communication to the public pursuant to Article 3 of the InfoSoc Directive, whether the transaction at hand constitutes or is equivalent to a sale.[39] The question is whether it should have done so in the light of its own decision in the *UsedSoft* case, as in that case, the CJEU held that it was exactly that circumstance that triggered the conversion of an act of communication to the public to the one of distribution[40], implying, that were no sale or other transfer of ownership involved, the transaction could be seen as communication to the public. If there is truly the option of such a conversion occurring under the applicable laws, the analysis of whether it had, in fact, occurred should immediately follow the conclusion that there is an act of communication to the public. While in the *UsedSoft* case, the CJEU omits the first part of the applicable rights analysis, *i.e.*, whether distribution or communication to the public right applies, merely stating the occurrence of the conversion described above, in the *Tom Kabinet* case, the CJEU omits the step lying in assessing the nature of the transaction at hand and whether it includes a transfer of ownership or its equivalent. If the transaction was equal to a sale by the standards set forth by the CJEU in the *UsedSoft* case, then the

38 *Tom Kabinet* case (n 28), para 49.

39 *UsedSoft* case (n 2), para 52.

40 ibid.

objectives of the principle of exhaustion were to be examined along with whether the exhaustion is able to fulfill its purpose in the digital transaction at hand. The difference is further even starker in comparison to the *VOB* case, which, although not explicitly mentioning functional equivalence, sets forth functional equivalence in all but name.

35 CJEU distinguishes the facts in the *Tom Kabinet* case from the facts in the *UsedSoft* case through the prism of equivalence between the supply by a download for permanent use and the supply through the distribution of a tangible carrier. In the first place, the CJEU agrees with the argument of the AG, that dematerialised digital copies do not deteriorate with use and therefore, form perfect substitutes to new copies. Further, according to the CJEU, this characteristic of second-hand e-books is further strengthened by the fact that exchanging such copies requires neither additional effort nor additional cost, and therefore the impact of the secondary markets on the interests of the rightsholders would be stronger. As further discussed below, these aspects are merely simplified fragments of the mosaic forming the assessment of functional and economic equivalence.

4. An "Exhaustion-like" Foot in the Door?

36 The last point regarding the *Tom Kabinet* case I would like to draw the reader's attention to is the following. Above, the decision has been described in the title as "*a door closed shut*". However, is it possible that the CJEU left a crack open in this door leading to digital exhaustion in the regime of the InfoSoc Directive? After concluding that the supply of an e-book by a download constitutes an act of communication to the public, the CJEU states in point 69, that: *(...) having regard to the fact, noted in paragraph 65 of the present judgment, that any interested person can become a member of the reading club, and to the fact that there is no technical measure on that club's platform ensuring that (i) 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 and (ii) after that period has expired, the downloaded copy can no longer be used by that user (see (...) Vereniging Openbare Bibliotheken (...)), it must be concluded that the number of persons who may have access, at the same time or in succession, to the same work via that platform is substantial.(emphasis added)*"[41]

37 The paragraph above comprises two aspects – a reproduction right aspect and a "new public" aspect. In the first part, the CJEU reaffirms its position promulgated in the *UsedSoft* case, that to not breach the reproduction right, only one copy must exist and be "usable" so that the copy is transferred rather than multiplied. Therefore, the mere fact that at least in the time of copying, two reproductions exist, does not itself form a breach of the reproduction right in such cases. The second part of the paragraph leaves more room for interpretation. As ironic as the above reference to the *VOB* case might be in the light of the mutual inconsistency of the decisions in the *VOB* case and the *Tom Kabinet* case, it suggests that were the abovementioned requirements fulfilled, there would have been no new public within the meaning of the *Svensson*[42] case and others. If that is the case, there could be room for an exhaustion-like rule present in the CJEU's understanding of the right of communication to the public and its limits, taking a deviationist stance to the application of rules regarding digital exhaustion. Such a solution could form more of a middle-ground solution in the balancing of rights of various stakeholders when compared to the solution lying in abolishing exhaustion of rights as a principle with regard to copyright works outside of the scope of the Software Directive without any particular policy considerations supporting such a step. Nevertheless, such a solution would not come without its own set of problems. From a systemic perspective, this solution blurs the already blurry lines between individual exclusive rights in the digital world. Furthermore, the room for this solution seems to be significantly limited by the subsequent case law of the CJEU, expanding the scope of the "new public" in the CJEU case law such as *Renckhoff*[43] or the *VG Bild-Kunst*[44] case. This case law further sheds light on the newly found non-willingness shown in the *Tom Kabinet* case, as opposed to the *UsedSoft* case, to interpret certain acts in the digital domain as an exercise of the distribution right and instead, to subsume all such acts under the wide umbrella of the ever-so-expanding right of communication to the public. As aptly noted by Oprysk, the Article 3 (3) of the InfoSoc Directive has continually been used by the CJEU as an argument to subsume a certain act under the communication to the public, as a failure to do so would lead to the exhaustion of the right and even in cases, in which the dissemination was of an independent, not of a secondary nature.[45] This

41 *Tom Kabinet* case (n 28), para 69.

42 Case C-466/12, *Nils Svensson, Sten Sjögren, Madelaine Sahlman, Pia Gadd v Retriever Sverige AB* (CJEU, 13 February 2014).

43 Case C-161/17, *Land Nordrhein-Westfalen v Dirk Renckhoff* (CJEU, 7 August 2018).

44 Case C-392/19, *VG Bild-Kunst v Stiftung Preußischer Kulturbesitz* (CJEU, 9 March 2021).

45 Liliia Oprysk, 'How Much "New" Public Is Too Much? The CJEU's VG Bild-Kunst Judgment and Non-Exhaustive Control Over a Work's Consumption' (2022) 53 IIC - International Review of Intellectual Property and Competition Law 1323,

itself is misleading, as only in the case of transactions of secondary nature, exhaustion should even come into question.[46]

V. A Dream of Balanced Copyright Exhaustion in the Digital Age

1. Relevance of Copyright Exhaustion Foundations in the Digital Age

38 In light of the above analysis, a solid foundation for copyright exhaustion in the digital age under EU copyright law may seem like nothing more than a dream. The following part of this paper asserts that copyright exhaustion, albeit in form balanced to suit the needs of the digital age better, is not only helpful to attain the balance among various stakeholders in copyright law – it is necessary. There are fundamental reasons why the rationale behind exhaustion preserves its relevance in the digital age and in some cases, its relevance may be even more vital. These reasons, lying in the very purpose of copyright exhaustion, do not distinguish between tangible and digital modes of distribution and apply indiscriminately. These fundamental reasons include, among others, the balancing effect of exhaustion (including reward theory arguments)[47], the competition and innovation-enhancing effects of exhaustion, and the function of exhaustion as a safeguard of the interests of the public at large. Furthermore, policy goals such as applying copyright law in a technologically neutral manner further favour preserving the exhaustion doctrine in one way or another.

2. Balance as the Foundation of Copyright Exhaustion

39 While the balance among different groups of stakeholders may be the ideal for which copyright law strives, achieving it is no simple task. What the term "balance" means is further subject to policy considerations, and it is therefore hard to pinpoint any objective measures or benchmarks. Balancing the rights of stakeholders in the market with copyright-protected works forms one of the inherent rationales behind the very introduction of exhaustion into copyright law, as it delimits the scope of control provided by the exclusive distribution right and reconciles it with the ownership rights of the lawful acquirer of a copy of a protected work.[48] However, it seems that the balancing aspect continuously disappears from the considerations revolving around digital exhaustion and the general secondary dissemination of protected works.[49]

40 Targosz presents four traditional explanations of the purpose of exhaustion, which are mutually non-exclusive.[50]

41 These are the:

- reconciliation of property rights in the "copy", as a specific object and the rights to the copyright-protected work itself;
- safeguarding that the rightsholder has the opportunity to recover adequate remuneration when putting the copy on the market for the first time;
- legal certainty; and
- facilitation of circulation of goods on the market (e.g. by creating secondary markets).

42 In the reasoning of the *Tom Kabinet* case, the CJEU only explicitly considers the function of exhaustion as a safeguard for the rightsholder to recover adequate remuneration. However, as seen from the explanations set forth by Targosz, this is not the only perspective through which copyright exhaustion can and should be viewed. There are doubts that this explanation alone is sufficient for concluding preserving or excluding exhaustion[51] in the digital domain, as it is more of a defence of exhaustion, rather than its sole justification in copyright law.[52]

43 Secondly, the CJEU makes no sophisticated economic

1328.

46 Ibid.

47 Péter Mezei and Caterina Sganga, 'The Need for a More Balanced Policy Approach for Digital Exhaustion – A Critical Review of the Tom Kabinet and ReDigi Judgments' (15 June 2023) <https://papers.ssrn.com/abstract=4480825> accessed 27 June 2023.

48 Péter Mezei, *Copyright Exhaustion: Law and Policy in the United States and the European Union* (Second edition, Cambridge University Press 2022) 7.

49 Oprysk (n 45) 1339.

50 Tomasz Targosz, 'Exhaustion in Digital Products and the "Accidental" Impact on the Balance of Interests in Copyright Law'in Bently L, Sutherhansen U and Torremans P (eds.) *Global Copyright: Three Hundred Years since the Statute of Anne, from 1709 to Cyberspace* (Edward Elgar 2010) 341.

51 ibid, 344.

52 ibid.

analysis regarding the factors that would enable the rightsholder to obtain adequate remuneration, but only briefly references the rather apparent concerns of the rightsholders.[53] The CJEU does not deeply inquire into the impact of the existence of secondary markets with protected works on the rightsholder or other subjects in the markets with protected works. The existence of secondary markets does not only influence these groups of stakeholders, it further influences the amount of innovation in the market. There are almost countless questions that could be asked in this regard, such as, whether one resold copy of an e-book truly means one less sale for the distributor, rather than a user who would otherwise not purchase the e-book at all for the (higher) price set on the primary market, or, in the worse scenario, would opt for obtaining a digital copy illegally. Whether the existence of a secondary market may motivate the user to acquire "new" copies due to the fact that with the option of resale, the investment into such copies no longer necessarily presents sunk costs, and in case the customer no longer desires to possess such a copy, it may recover part of the costs by its resale.[54] The CJEU does not deal with any of these analyses, and with so many different variables, the CJEU reaches its conclusion with striking efficacy.[55] The argumentation provided by the CJEU in the *Tom Kabinet* case heavily focuses the protection of the rightsholder, with no real emphasis on the existence and the activities of other stakeholders in the market. To be clear, this should by no means be understood as stating that the extension of copyright exhaustion into the digital domain is not able, to an extent, negatively affect the interests of the rightsholder in obtaining remuneration or is able to deal with all of the concerns above. However, it is a mistake to deem exhaustion an obsolete doctrine with no place in copyright law of the current day. The question of how the rightsholder is affected (and whether it is proportionate) by the introduction of digital exhaustion should clearly be asked and examined. However, the answer to this question cannot be provided merely on the basis of a simplifying statements such as that digital copies do not deteriorate with use and that exchanging such copies requires no additional effort nor additional costs, as the considerations are *much* more complex.

44 While the *leitmotif* in providing strong protection to rightsholders in the *Tom Kabinet* case seems to be to facilitate innovation[56], the effect may be precisely the opposite. Lawrence Lessig describes the inherent war between copyright and technology, lying in the fact that new technological means restrict the amount of control the rightsholder may exercise over the relevant copyright works.[57] According to Elkin-Koren and Salzberger, following up on Lessig's theory, the copyright setting must be differentiated from the setting of ownership rights, as "*...in real property the legal protection is necessary in order to create incentives to produce and protect the right of possession. In intellectual property law, in contrast, there is a need only to generate sufficient incentives to create. Thus, with regards to intellectual property there is a need only for less than perfect control, while in real property the law must provide perfect control to the owner.*"[58] This consideration should be key in assessing whether the rightsholder is able to obtain *adequate* remuneration. In the light of the *Tom Kabinet* case and case law expanding the term "*new public*", it seems that the focus of the CJEU lies in granting control to the rightsholder and the rightsholder being able to recover as high remuneration as possible, rather than considering whether such remuneration is just enough to provide a sufficient incentive to create further and to spur innovation while preserving the balance with the interests of the public-at-large. There are also other considerations to be made in assessing whether the remuneration granted is adequate and whether in the specific case, the rightsholder interest lying in remuneration is not outweighed by the negative externalities of granting the rightsholder a wide scope of control, which may encompass the stifling of competition and innovation and thereby, the grant of extensive control disproportionately harms the public-at-large.

45 In the end, if the goal of copyright law is to maximize

53 According to the decision in the *Tom Kabinet* case, electronic books form perfect substitutes to their traditional - tangible counterparts, and exchanging digital copies requires neither additional effort nor costs, therefore a secondary market therewith would likely affect the (monetary) interests of the rightsholder much more than in the case of secondary markets with traditional books.

54 Targosz (n 50) 338.

55 Liliia Oprysk, 'Secondary Communication under the EU Copyright Acquis after Tom Kabinet: Between Exhaustion and Securing Work's Exploitation' (2020) 11 JIPITEC <https://www.jipitec.eu/issues/jipitec-11-2-2020/5095> accessed on 5 June 2023.

56 The CJEU invokes the recital (4) of the InfoSoc Directive, setting forth that „*A harmonised legal framework on copyright and related rights, through increased legal certainty and while providing for a high level of protection of intellectual property, will foster substantial investment in creativity and innovation, including network infrastructure, and lead in turn to growth and increased competitiveness*", while focusing merely on the high level of protection element, however, that is not the only variable in the equation.

57 Lawrence Lessig, '*Code:Version 2.0*' (BasicBooks 2006) 172.

58 Elkin-Koren N and Salzberger EM, 'The Law and Economics of Intellectual Property in the Digital Age: The Limits of Analysis' (Routledge Taylor & Francis Group 2015) 93.

the welfare of the public-at-large and not only to maximize the control and profit generating capabilities of the rightsholders, balancing is necessary. Such balancing does not only take the form of limitations on the exclusive rights in scope and time, but it also comes in the form of the introduction of principles such as copyright exhaustion. While the grant of property-like control to the rightsholders may give an incentive to create, it, at the same time, hinders the creation process, as new creations rely on the previous ones.[59] In the mentioned balancing, one must not forget that not only were the costs of (legal or illegal) copying significantly diminished in the digital age[60], the means and extent to which the rightsholders may exercise control increased significantly, through the introduction of elements such as DRMs or private ordering into the equation. These means are not to be overlooked, as these allow the rightsholders not only to control the distribution of the protected works, but also the very consumption of their contents by their users, even after their authorized placement on the market.

3. The Competition and Innovation Enhancing Side of Exhaustion

46 It would be an error to consider copyright exhaustion solely in the vacuum of copyright law, especially within the EU legislative framework. Copyright exhaustion allows for the very existence of secondary markets and facilitates the circulation of goods.[61] After all, the exhaustion principle, as introduced into EU law by the *Deutsche Grammophon case*[62], played an essential role in the functioning of the EU single market and helps to achieve the first of the four fundamental freedoms in the single market, the free movement of goods. Targosz notes that the functions of exhaustion may not be determined only by using copyright law concepts and further observes that driven by the *effet utile* reasoning, the CJEU has shaped exhaustion in an autonomous way, as a tool ensuring the effective circulation of goods and when needed, acknowledging the exhaustion of other rights other than purely material right of distribution.[63] After all, applying a rule strikingly similar to exhaustion may be observed in applying the "new public" requirement, which by no means arises from the wording of article 3 of the InfoSoc Directive.

47 Some of the positive effects of secondary markets lying in mitigating certain types of anti-competitive behaviour have been well described. Firstly, secondary markets help prevent or mitigate the vendor lock-in effect. By creating a secondary source of acquiring relevant copyright works, the public no longer has to rely only on the primary channels. A secondary market may further spur innovation through the rightsholders having to compete with secondary markets on top of the competition in the primary market. Even if this increase in competition results in lower profit, the level of innovation may be higher, as some producers may try to entice customers to continue paying premium prices by innovating and releasing new or upgraded products.[64] A policy facilitating innovation should further not only include producer-level innovation, but the innovation on other levels as well, in order to promote the welfare of the public-at-large.[65] Finally, secondary markets considerably influence price discrimination strategies. The existence of secondary markets has the potential to limit the negative effects of excessive price discrimination, as it offers new means of acquisition of the relevant work, presumably for a more favorable price. On the other hand, it does not make price discrimination impossible and in some aspects, might even help the rightsholders in the setting of their commercial strategy. For example, it will allow the customers to "sort themselves out"[66] and it might be rational to presume, that the customers willing to pay premium prices will, most likely, be concentrated in the most part on the primary market.

4. Exhaustion as a Safeguard of Public Interest in Copyright law

48 Exhaustion may also be seen as one of the inherent checks and balances of copyright, ensuring that copyright law strikes a balance between the interests of the rightsholders and the interests of the public-

59 ibid., 49.

60 This circumstance is often stressed as a significant detriment to the rightsholders, as the digital means of distribution facilitate illegal copying as well. However, it is vital to keep in mind that the costs of legal distribution by the rightsholders were significantly diminished as well.

61 Targosz (n 50) 342.

62 Case 78-70, *Deutsche Grammophon Gesellschaft GmbH v Metro-SB-Großmärkte GmbH & Co. KG* (ECJ, 8 June 1971).

63 Targosz (n 50) 342.

64 Ariel Katz, 'The Economic Rationale for Exhaustion: Distribution and Post-Sale Restraints' in Caliboli I and Lee E (eds.) *Research Handbook on Intellectual Property Exhaustion and Parallel Imports* (Edward Elgar Publishing 2016) 26.

65 ibid., 28.

66 ibid., 26.

at-large.[67] By effectively deleting exhaustion off the map in the digital domain under the InfoSoc Directive, the CJEU shifts this balance substantially in favour of the rightsholders, as the amount of control they may exercise over the subsequent fate of protected works in the digital domain starkly increases in comparison to the amount of control granted to tangible copies of protected works. While the CJEU argues with historical intent for the purposes of keeping exhaustion out of the digital domain for protected works in the regime of the InfoSoc Directive, the question is whether such a shift in balance was indeed intended to be brought about by the "mere" change of the technological means of distribution and dissemination of protected works. A more nuanced approach is necessary and as many issues the decision in the *UsedSoft* case had from the point of the wording of the relevant law, it seems to do a better job in providing for such a nuanced approach, taking into considerations the circumstances of the new technological reality.

49 The role of exhaustion with regard to the public-at-large may further be observed in the context of regulation such as the directive 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services ("**Digital Content Directive**"). The Digital Content Directive explicitly states that it is without prejudice to copyright laws, including the InfoSoc Directive. Despite this relatively unambiguous statement, there seems to be a number of friction points between the Digital Content Directive and EU copyright laws. Spindler, Oprysk and Sein primarily point to the possible friction with the objective conformity test contain in Article 8 (1) of the Digital Content Directive, lying in the requirement of reasonable expectations of the consumer.[68] For example, as Oprysk and Sein note, when faced with a "*Buy now*" button with regard to an e-book, a reasonable expectation of consumers may exist to acquire (buy) content, which they can also dispose of and permanently transfer their access to another person.[69] Further in the case of videogames, the digital copies are often of the same or higher price as their counterparts on tangible carriers. Digital copies are not sold and what more, are usually bound to a user-account, which may not be transferred to another person by virtue of the EULA or an alike private ordering instrument. The absence of exhaustion or an exhaustion-like rule clearly puts the users "buying" the digital versions of videogames in a disadvantageous position and strengthens the position of the rightsholder, on the basis of nothing more than the technology the customer decided to use. Last but not least, the existence of secondary markets, brought about by the exhaustion principle, further serves the public-at-large by helping prevent the disappearance of certain works due to the discontinuation of their distribution on the primary market.[70]

5. Functional and economic equivalence

50 The CJEU invokes the concepts of functional and economic equivalence, along with the reference to the primary law principle of equal treatment in both of the landmark digital exhaustion cases discussed above. In the present author's view, neither of these forms an *en bloc* normative barrier for introducing copyright exhaustion in the digital environment for the works protected under the InfoSoc Directive. The obvious difference between the *UsedSoft* case and the *Tom Kabinet* case is that while the CJEU found the sale of a computer program on a tangible carrier and the sale of a program by downloading from the internet are similar, whereas, in the case of distribution of tangible books and e-books, the court reached the opposite conclusion But what are the criteria for such equivalence? In the *UsedSoft* case, the CJEU considers the functional equivalence of the online transmission method and the supply on a material medium.[71] In the *VOB* case, the CJEU is not as explicit, but also invokes the functional equivalence of digital lending and the lending of printed works, in line with the principle of equal treatment.[72] Finally, in the *Tom Kabinet* case, CJEU mentions equivalence from an economic and functional point of view.[73]

51 One of the most frequent arguments against digital exhaustion lies in the assertion that an electronic copy is a perfect substitute for a new copy, as it does not deteriorate with use and thereby a parallel second-hand market would be likely to affect the interests of the copyright holders in obtaining an appropriate reward for their works much more than the market for second-hand tangible object. This is a gross oversimplification. As Geiregat notes, the argument arises from the erroneous premise that the rightsholders have an exclusive right to

67 Targosz (n 50) 343.

68 Gerald Spindler, 'Digital Content Directive And Copyright-Related Aspects' (2021) 12 JIPITEC 111.

69 Liliia Oprysk and Karin Sein, 'Limitations in End-User Licensing Agreements: Is There a Lack of Conformity Under the New Digital Content Directive?' (2020) 51 IIC - International Review of Intellectual Property and Competition Law 594, 619 .

70 Katz (n 64) 27.

71 *UsedSoft* case (n 2), para 61.

72 *VOB* case (n 29), para 53.

73 *Tom Kabinet* case (n 28), para 58.

market new or unused copies.[74] Consequently, it is also erroneous to consider secondary markets as involving only transactions with used or to some extent barely functional copies of protected works. Secondary markets frequently also contain new and unused copies of protected works.[75] It further seems fair to assert that a book that has been read ten times does not necessarily grant its user a lower amount of enjoyment of the protected subject matter than a new book. And from the perspective of copyright law, after all, it is the subject matter that copyright protects, not the deteriorating physical condition of pages in a book. It is further misleading to say that digital copies do not deteriorate. They do, just differently. Whether the digital copy in question is stored on a server or a device, it may be destroyed or corrupted. Furthermore, due to the fast-paced development of the technological landscape, file formats become obsolete, and it therefore seems entirely possible that a tangible book outlasts an e-book in the amount of time its user may enjoy the protected subject matter. Digital copies are further often bound to a platform or device of a specific provider. Not to mention that used audio or audiovisual content carriers, such as DVDs and blu-rays, including usual wear and tear, can provide exactly the same experience as new ones. Books or other tangible copies of protected works may, and often do, gain value by becoming a collector's item due to being a part of a certain edition or may even be valued for other features, which could, under different circumstances, be considered defects. The resale price of such books is usually a multiple of the original price set by the rightsholder on the primary market. Digital assets, safe for, *e.g.* the phenomenon of NFTs, do not generally share this feature.

52 The economic aspect of equivalence lies in considerations revolving around the question whether copyright exhaustion is able to bring about equivalent economic effects in the digital world, especially whether it is able to ensure that the rightsholder obtains adequate remuneration. The focal point of the argument asserting the economic inequivalence of transmission of digital and tangible copies of protected works relates to copyright piracy concerns and the asserted ease with which digital copies may be exchanged. In simpler terms, this argument asserts that defying the "one (legal) copy, one user" principle is easier in the digital domain. On the other hand, so is equipping the digital content with protective measures. This argument is once again a question of technology, not a normative basis for the refusal of the rationale of exhaustion as such. While it is undeniable that no technical solution is perfect, and that every conceivable solution, however ingenious and inventive, may most likely be bypassed, whether now or in the future, this is not a feature characteristic only to digital content. It is clear that the internet facilitates the ease with which reproductions, legal and illegal alike, can be made and distributed. However, the very same can be said about the invention of a printing press. For this argument to become a solid obstacle for the relevance of the rationale of exhaustion, one would have to conclude that under no circumstances is it possible for digital copies to be protected in a comparable manner as tangible ones. But this is hardly the case in the age of technologies such as blockchain, delete-and-forward technologies and many others, which make the transactions with digital copies more transparent and allow to observe the mentioned "one copy – one user" rule in the digital domain.

53 The CJEU mentions that it is obvious that exchanging digital copies requires neither additional effort nor additional cost, so a parallel second-hand market would be likely to affect the interests of the copyright holders in obtaining an appropriate reward for their works much more than the market for second-hand tangible objects.[76] By this, the CJEU presumes a lot about the behaviour of the user, as it presumes that merely because the users have the option to resell, the users will change their behavior in such a significant way that it substantially endangers the primary market. Of course, this would benefit the user, as mentioned above, as any investment into the digital copy would no longer present sunk costs. But there seems to be no convincing evidence to support this presumption[77] and if there is any, it is not presented in the *Tom Kabinet* case. Geiregat raises another interesting point, this point being that maybe the residual value of e-books, among other, lying in the acquirers being willing to transfer them, is exactly the reason why they should be able to do so, rather than a reason to exclude transferability.[78] All of these arguments are valid, however, the considerations around them are not binary. Balancing must be carried out in order to count with the nuances of various situations which may occur. It seems inadequate to treat the above rightsholder concerns as self-evident truths forever barring exhaustion from the digital domain. And it further seems inadequate to deem these concerns applicable in any case under the InfoSoc Directive, however not in the case of the cases related to computer programs under Software Directive.

74 Simon Geiregat, *Supplying and Reselling Digital Content: Digital Exhaustion in EU Copyright and Neighbouring Rights Law* (Edward Elgar Publishing 2022) 159.

75 ibid.

76 Tom Kabinet case (n 28), para 58.

77 Geiregat (n 74) 164.

78 ibid.

54 Many of the arguments regarding functional and economical (in)equivalence present in the *Tom Kabinet* case reject digital exhaustion and the rationale behind it, rather than genuinely assessing whether the application of copyright exhaustion in the digital domain may be functionally and economically equivalent.

C. Conclusion

55 More than a decade after the landmark *UsedSoft* case, the landscape surrounding digital exhaustion remains unclear. Even after all this time, the path to digital exhaustion in the current legislative landscape of the EU seems to be all but simple. But as shown above, the fundamental rationales of copyright exhaustion remain and apply indiscriminately on the selected mode of distribution. From a policy perspective, normatively excluding copyright exhaustion causes a significant shift of balance in favour of the rightsholders, with little rational policy arguments supporting this shift.

56 The inconsistency in the answers to the questions surrounding digital exhaustion may be a symptom of a more general inconsistency within the case law of the CJEU concerning the secondary dissemination of protected works in the digital domain. On the one hand, the exclusive right of communication to the public is not subject to exhaustion, yet this has by no means prevented the CJEU from developing extensive case law effectively exempting certain acts of communication from the scope of this right in an exhaustion-like manner. [79] On the other hand, the CJEU makes further steps in the other direction by expanding the term "new public" scope. In the case of exhaustion, in the *UsedSoft* case, the CJEU strongly prioritizes a flexible teleological approach over the wording of the relevant law and examines digital exhaustion without even considering whether distribution right even applies, but in the *Tom Kabinet* case, the CJEU sticks to a literal interpretation of the wording of the InfoSoc Directive. Another culprit may be found in the rigidity of the copyright law framework. But one can hardly blame the authors of copyright treaties coming from the age of VHS tapes for being unable to predict the fast-paced technological development of the years to come.

57 It has not been persuasively shown that the balance intended by the introduction of copyright exhaustion became obsolete in the digital age.[80] Therefore, there is cause for concern when the shift in the balance brought about by the development of technology so one-sidedly favours the rightsholders. The issues underlying exhaustion in the digital domain call for nuanced solutions, carefully considering the impact on the rights and interests of various stakeholders in the market with protected works. Of course, it is a different question completely what the practical relevance of each right from the existing framework of exclusive rights is going to be in the not-so-distant future.

58 On the one shore stand means of dissemination of protected works such as streaming, software-as-a-service and others, the relevance of which is constantly on the rise within the recent years and which could, effectively make the distribution right obsolete and any further considerations would concern the "right to access", rather than secondary transactions with protected works. On the other shore, there is the momentum-gaining concept of Web 3.0, which, through the means of blockchain-based technologies, such as NFTs embraces individual ownership of immaterial goods and the individual freedom to dispose of them freely, as part of digital self-determination. Furthermore, both of these streams are not mutually exclusive and will most likely grow along each other. In the absence of a crystal ball, any predictions are necessarily precarious. However, irrespective of further development in one way or another, one thing remains certain – a balanced approach to legal concepts such as copyright exhaustion in the digital domain is necessary and the underlying issues are, after more than a decade, far from solved.

79 Oprysk (n 45) 1329.

80 Targosz (n 50) 346.

Taming NFTS with Trademark Law Tools: Future Challenges for Sri Lanka

by **Wathsala Ravihari Samaranayake ***

Abstract: When NFTs were first introduced, it was generally believed that they would foreclose avenues for trademark counterfeiting owing to their innate characteristics. Despite all the optimism, NFTs have given rise to a number of unprecedented trademark issues. Thus, the question arises whether the traditional trademark law regime is sufficiently equipped to tackle NFTs-related trademark issues. Although it ostensibly involves a mere extension of the existing trademark law principles to a new phenomenon, in effect, it entails an arduous exercise infused with intricate legal issues. To be more explicit, the complexity of the legal issues posed by NFTs has baffled many sophisticated legal regimes in the world including the USA and EU. The legal issues that surfaced in *Hermès Int'l v.Rothschild, 590 F. Supp. 3d 647 (S.D.N.Y. 2022), Nike Inc. v. StockX LLC. 1:22-cv-. 00983 (S.D.N.Y. February 3, 2022)* and *Juventus F.C. v Blockeras s.r.l*, (*Docket No. 32072/2022, Court of Rome IP Chamber, 20/07/2022)* bear testimony to this fact. As far as Sri Lanka is concerned, however, to the best of the author's knowledge, the courts have not encountered any NFTs-related trademark disputes so far. But this does not mean that it will be immune from such issues in the future. The concept of NFTs has become so pervasive that it is no longer limited to sophisticated jurisdictions. Therefore, in this paper, an attempt is made to critically evaluate the adequacy of the existing legal regime on trademarks in Sri Lanka to grapple with the legal dilemma created by the proliferation of NFTs in the virtual realm. This paper will also look at the developments in comparative jurisdictions, specifically, the USA and EU with a view to shedding light on how the international experiences and best practices can be used to ameliorate the Sri Lankan trademark landscape, in view of the growing menace of NFTs.

Keywords: NFTs, Trademarks, Nice Classification, Misleading Similarity, Exhaustion, Nominative Fair Use, Immutability

Recommended citation: Wathsala Ravihari Samaranayake, Taming NFTS with Trademark Law Tools: Future Challenges for Sri Lanka, 14 (2023) JIPITEC 541 para 1

A. Introduction

1 The exponential growth in disruptive technologies is reshaping modern society and its business models. Perhaps, the best example is the metaverse phenomenon which is a revolutionary breakthrough in human-technology interaction. The metaverse is a sophisticated, shared and immersive three-dimensional virtual universe[1] which mimics the physical world. The following excerpt is a lucid explanation of what it constitutes:

"The [m]etaverse is an integrated network or social sphere that operates in the digital space. It is a continuum of several immersive virtual experiences in the digital spaces. All the synchronous experiences enhance the sensation of interactions (....). Users of the [m]etaverse or augmented reality world would meet and socialize with other participants using personalized avatars in real-time. The different range of activities is accessible using specialized devices like virtual reality headsets, smartphones, digital glasses, goggles, and more. In short, the [m] etaverse is an embodied internet that provides a scaled-up world in the virtual space. Just like the world where we are in, it is a place where we connect

* Lecturer, Faculty of Law, University of Colombo, Attorney-at-Law.

1 'Metaverse" is a virtual space parallel to and independent of the real world, an online virtual world that mirrors the real one, and it is increasingly real': Zhao Guodong, Yi Huanhuan and Xu Yuanzhong, *Metaverse* (Kindle Edition 2021).

with our families, friends, work colleagues, clients, and other significant people." [2]

2 The metaverse, which is often accoladed as the next iteration of the internet is 'a concept for a cyberspace realm that [is] built on the existing infrastructure of the internet using the emerging technologies of blockchains, cryptocurrency, and [Non-Fungible Tokens (NFTs)].'[3] Although NFTs can be conveniently dissociated from the metaverse owing to their mutually independent existence, the fact that the metaverse ascribes singular and significant importance to NFTs cannot be thrust into oblivion.[4] It has been observed that 'NFTs are currently used in the metaverse as collectibles, access keys, investments, deeds of ownership, voting and governance tokens for decentralized autonomous organizations (DAOs), and facilitators of services or experiences'.[5] NFTs have thus become extremely popular today, with the Metaverse gaining momentum in the past few years.

3 Notably, the history of NFTs is traced back to two sources. While some believe that Kevin McCoy's "Quantum" NFT minted on the Namecoin blockchain in 2014 is the first ever NFT, others are of the view that Colored Coins designed on the Bitcoin network in 2012 are in fact the very first NFTs to exist. [6] Nonetheless, 'the genesis of the spread of NFTs can be traced back to 2017, and it is linked to the funny phenomenon of "Cryptokitties"'.[7] Since then, thousands of NFT projects including Beeple's $69 million NFT auction piece[8] have been launched.

4 The most intriguing question which defies a precise answer is what an NFT constitutes. Although the contours of an NFT remain largely undefined, its meaning can be gleaned to some extent from its basic characteristics. The primary characteristic of an NFT is that it is non-fungible. In contrast to fungible objects which are equivalent in value, NFTs are unique one-offs. The upshot of this is that whilst fungible objects like money or bitcoins are mutually interchangeable, non-fungible tokens cannot be exchanged with one another. For this reason, NFTs have been likened to 'items of artistic or historical significance, or rare trading cards'.[9] An equally important characteristic of an NFT is that it functions as a token[10] capable of attributing an immutable proof of ownership to an underlying artwork or a virtual or physical asset. However, the "Token" in an NFT is "truly a digital item designed to track the asset by its 'TokenID' and attribute ownership to the current owner".[11] These dual characteristics are portrayed by the very term 'Non-Fungible Tokens'.

5 Another vexing issue that is linked to the previous issue is the lack of a uniform definition for NFTs. Interestingly, however, a survey of existing literature on NFTs reveals that there are primarily two types of defintions of NFTs, one that alludes to a digital certificate and the other that characterizes an NFT as a digital asset. The EUIPO defines NFTs as "unique digital certificates registered in a

2 Vitali Lazar, *Cryptocurrency Investing Guide and Metaverse Explained: Absolute Beginner Guide to Start Trading and Understand Blockchain Technology, Bitcoin, NFT and Altcoins* (Kindle Edition 2022)

3 Michael D. Murray, 'Trademarks, NFTs, and the Law of the Metaverse' (2023) 6 Arizona Law Journal of Emerging Technologies (forthcoming) (footnotes omitted). See also, Darell Freeman, *Metaverse for Beginners: An Ideal Guide for Beginners to Understanding and Invest in the Metaverse: NFT Non-Fungible Token, Virtual Land, Real Estate, Defi, Blockchain Gaming and Web 3.0* (Cryptosphere Accademy 2022) 58: 'A metaverse is 'a persistent online world where users can experience a richer immersive experience than existing online services through virtual and augmented reality interfaces'; Fouad Sabry, *Immersion Into Virtual Reality: The perception of being physically present in a non-physical world* (One Billion Knowledgeable 2022): 'A combination of the words "meta" and "universe", the phrase "metaverse" was first used in the science fiction book Snow Crash, which was published in 1992'.

4 See Georgia Weston, 'NFTs and their Role in the "Metaverse"' (*101 blockchains*, 24 December 2021) <https://101blockchains.com/nfts-and-metaverse/> accessed 2 December 2022 (noting that 'The metaverse is a massive concept, and NFTs can serve as a key concept in the broad ecosystem').

5 Murray (n 3).

6 See Benjamin Hor et al, *How to NFT* (CoinGecko 2022) 10

7 Andrea Sestino, Gianluigi Guido and Alessandro M. Peluso, *Non-Fungible Tokens (NFTs): Examining the Impact on Consumers and Marketing Strategies* (Springer Nature 2022) 13.

8 'Beeple, a digital artifact, was the first digital artist to make history by selling NFT- backed artwork at an auction house. The sale brought in $69 Million dollars': Josh Caine, *NFT for Beginners: Ultimate Guide for Creating, Buying, Selling, and Trading Non-fungible Tokens (Make Profit with Digital Crypto Art and Collectables)* (Kindle Edition 2022).

9 Lennart Ante, 'The Non-Fungible Token (NFT) Market and Its Relationship with Bitcoin and Ethereum' [2022] FinTech 216.

10 For a definition of the term 'token' see Sestino, Guido and Peluso, (n 7) 12. ('In IT, a token is a set of digital information able to identify a specific purchasable object.')

11 Madison Yoder, 'An "OpenSea" of Infringement: The Intellectual Property Implications of NFTs' (2022) 6 The University of Cincinnati Intellectual Property and Computer Law Journal, art 4, 4.

blockchain, which authenticate digital items but as distinct from those digital items".[12] A similar idea has been expressed by Lennart Ante who remarked that 'NFTs are unique certificates of authenticity on blockchains that are usually issued by the creators of the underlying assets'. [13] In fact, the Collins English Dictionary which announced 'NFT' as the buzzword of year 2021, defined an NFT as a unique digital certificate, registered in a blockchain, that is used to record ownership of an asset such as an artwork or a collectible.'[14] All these definitions treat NFTs as digital certificates. By contrast, Vicky V. Choudhary defines an NFT as 'a cryptographic asset on the blockchain that consists of unique identification codes and metadata that allows them to be distinguished from one another'.[15] In a similar vein, Clark Griffin asserts that NFTs are '[c]ryptocurrency assets that act as a rare and unique project, whether virtual or physical, for example[,] digital art or real estate'.[16] Both Choudhary and Griffin hold the view that NFTs are cryptographic assets. The important point to be noted is that characteristics possessed by a digital certificate are necessarily different from those of digital assets. It is obvious therefore that the definition of NFTs is full of controversies that, as we would see later in this article, mirror the legal dichotomies underlying NFTs.

6 The key attributes of NFTs include 'unicity', 'scarcity', 'authenticity', 'transparency', 'transferability' and 'indivisibility'. The unicity of NFTs stems from their quality of being unique. Each NFT is unique, like for example, a custom-made silver necklace. There is no replica of an NFT owing to the fact that 'each NFT has a specific digital identifier (...), such that the pair "contract address-token ID" is unique within the reference ecosystem (i.e., the blockchain)'.[17] Guadamuz expounds on this so-called 'pair' in the following statement:

> "The first core element of an NFT is a number known as the tokenID, which is generated upon the creation of the token; the second is the contract address, a blockchain address that can be viewed everywhere in the world using a blockchain scanner. The combination of elements contained in the token make it unique; only one token in the world exists with that combination of tokenID and contract address."[18]

7 Indeed, it is the uniqueness that NFTs are imbued with, which makes them rare and not mutually interchangeable. The view has been expressed that 'by leveraging their unicity, NFTs may be used to simulate and create the concept of "scarcity"'.[19] It appears therefore that 'scarcity' is a direct consequence of uniqueness; as NFTs are associated with one digital or physical object they provide scarcity in the market.[20] Importantly, the element of scarcity has an intriguing effect on NFTs embodying digital art. It has been observed that 'Digital art has mostly failed to generate value for creators because it is not seen as rare; it can be copied or manipulated

12 'Virtual Goods, Non-Fungible Tokens and the Metaverse' (*EUIPO European Union Intellectual Property Office*, 23rd June 2022) < https://euipo.europa.eu/ohimportal/en/news-newsflash/-/asset_publisher/JLOyNNwVxGDF/content/pt-virtual-goods-non-fungible-tokens-and-the-metaverse> accessed 2nd January 2023. However, this definition has sometimes been criticized. For example, see Katfriend Paolo Maria Gangi, What is an NFT? A comment to the EUIPO Guidance on NFTs (*The IPKat*, 14 July 2022) <https://ipkitten.blogspot.com/2022/07/guest-post-what-is-nft-comment-to-euipo.html> accessed 28th December 2022 ('First, the EUIPO describes NFTs as "certificates registered in a blockchain" but this sounds a bit like a devaluation of what an NFT is, since it is primarily a "token", meaning a digital asset created using some specific technological standards, the most common being ERC-721 and ERC-1155, and which can be traded or transferred within a blockchain (or a market place) eco-system according to specific rules written in the smart contract (like the automatic payment of royalties to the NFT creator)').

13 Ante (n 9). See also Sestino, Guido and Peluso (n 7) 1: ('NFTs-that is, the cryptographic ownership certificates of digital objects').

14 However, certain authors have also defined NFTs as tokens or proofs of ownership. For example, see Freeman (n 3) 61: 'NFTs are tokens that exist on the blockchain and can be used to prove ownership of connected digital assets'. See also Hor et al. (n 6) 6: '(...) an NFT is a token that possesses a unique identifier and has additional parameters that allow you to store certain information on it'.

15 Vicky V. Choudhary, *Non Fungible Token (NFT): Non Fungible Token (NFT): Delve Into The World of NFTs Crypto Collectibles And How It Might Change Everything?* (Vicky Virendralal Choudhary 2022) 11.

16 Clark Griffin, *Mastering NFT: Create, Sell and Invest in Non-Fungible Tokens and Digital Art* (Top Notch International 2022). See also John Potts, *The Near-Death of the Author: Creativity in the Internet Age* (University of Toronto Press 2022): 'An NFT -or non-fungible token-is a digital asset that is not fungible, that is exchangeable; rather, it is held to be unique object.'

17 Sestino, Guido and Peluso (n 7) 14.

18 Andres Guadamuz, 'Non-fungible tokens (NFTs) and copyright' [2021] WIPO Magazine 1, 34.

19 Sestino, Guido and Peluso (n 7) 14

20 See World Intellectual Property Organization, *Blockchain technologies and IP ecosystems: A WIPO White Paper* (WIPO 2022) 23.

in ways that undermine the principles of scarcity and originality that drive art markets'.[21] But this loophole has been remedied by the advent of NFTs which are unique and irreplicable. Here, the point one must remember is that 'while it is true that anyone can take a screenshot of an art NFT, this screenshot will not have any of the identifying information or the creator's digital signature that comes with the purchase of the NFT, nor will it have the record of past transactions going back to its creation'.[22] A mere screenshot of the digital art embodied in the NFT is distinct from the NFT. It is the NFT that cannot be easily duplicated and which thereby retains its scarcity.[23] This also explains why sometimes the decision to buy an NFT would be fueled by purely a desire to seize the so-called 'bragging rights'. People buy NFTs not so much to claim legal ownership rights but for the clout associated with the ownership of a unique and one-off item.

8 Authenticity is an equally important characteristic of an NFT. An NFT contains built-in authentication, which serves as proof of ownership.[24] The digital infrastructure of NFTs is composed of blockchain technology and smart contracts. 'NFTs take advantage of smart contract technology to store and record unique information on the blockchain'.[25] 'The integrity of the blockchain[26] network on which NFTs [reside], ensures their authenticity by preventing them from being altered, removed, or replaced'.[27] 'Blockchains make it nearly impossible to hack into the system or change the transaction records in any way, so before buying a (...) NFT, a user is able to look at its records to see who originally created it, as well as all of its previous owners'.[28] Evidently, therefore, '[b]lockchain-enabled NFTs facilitate asset provenance or tracking, and verify asset ownership or authenticity'.[29]

9 The next attribute of NFTs, transparency, is linked to their immutability. The immutable records of ownership create transparency in the transaction in three ways: to know whom you are dealing with, to know your rights and to know the previous owner of the asset, if any.[30] It has in fact been observed that '[t]ransparency is an inherent part of the architecture of blockchains, and NFTs are built on top of them. This suggests that, in a sense, NFTs were designed to be shown'.[31] Be that as it may, the transparency in NFTs helps to create trust between buyers and sellers. Apart from transparency, NFTs are also infused with 'transferability'. NFTs can be transferred within the blockchain ecosystem subject to the rules specified in the smart contract.[32] Accordingly, NFTs can be bought and sold multiple times through digital platforms.[33] Due to the reason that NFTs can be identified with a unique ID number, NFTs possess a higher level of transferability than many other assets living in the blockchain. [34] Another striking feature

21 Greg Hearn, *The Future of Creative Work: Creativity and Digital Disruption* (Edward Elgar Publishing 2020) 88

22 Yoder (n 11) 4.

23 See Daniel Plumley and Rob Wilson, *The Economics and Finance of Professional Team Sports* (Routledge 2023) 157: ('This stands in stark contrast to most digital creations, which are almost always infinite in supply.')

24 See ibid.

25 Hor et al (n 6) 8

26 By definition, a blockchain is a distributed, decentralized, immutable ledger used to store encrypted data.

27 Farhan Khan et al, 'Advancements in Blockchain Technology with the Use of Quantum Blockchain and Non-Fungible Tokens' in Mahendra Kumar Shrivas et al (eds.), *Advancements in Quantum Blockchain with Real-Time Applications* (IGI Global 2022) 216. See also Harsh Vardhan Singh Rawat et al, 'Rise of Blockchain-Based Non-Fungible Tokens (NFTs): Overview, Trends, and Future Prospects' in Vaclav Skala (eds.), *Machine Intelligence and Data Science Applications: Proceedings of MIDAS 2021* (Springer Nature 2022) 7: 'NFTs records of ownership cannot be modified as the information is maintained at all times in the blockchain ledger.'

28 Yoder (n 11) 2. See also Hor et al (n 6) 8 ('NFTs mitigate issues such as fraud and plagiarism, which is a common problem all non-fungible goods face. Rather than hiring an expert, we can verify the authenticity of an NFT using the blockchain')

29 Hearn (n 21) 88

30 See Ramakrishnan Ramanan and Benson Edwin Raj, 'The World of NFTs (Non-Fungible Tokens): The Future of Blockchain and Asset Ownership' in Adel Ben Mnaouer and, Lamia Chaari Fourati (eds.) *Enabling Blockchain Technology for Secure Networking and Communications* (IGI Global 2021) 99. See also Yoder (n 11) 3 ('In addition to being able to view an NFT's previous owners, one is also able to view the original creator of the NFT, or whoever first minted it.').

31 Milkyway Media, *Summary of Matt Fortnow & QuHarrison Terry's The NFT Handbook* (Milkyway Media 2022).

32 See Singh Rawat et al (n 27) 7 ('NFTs are quite easy to transfer from one owner to another with the help of smart contracts that are executed in the background'.)

33 See Sestino, Guido and Peluso (n 7) 14 ('Due to their peculiar characteristics, NFTs can be proposed, traded, sold, or transferred through digital platforms').

34 See Yvonne Landry, *Nft: All You Need to Know About Investing in Nft (Application and How to Make Money With Non-fungible*

of NFTs is that they are indivisible.[35] The ensuing position is that an NFT 'can only stay in existence as an individual token, unlike the cryptocurrencies which act as [fungible tokens] and are divisible. This means that the NFTs cannot be used for transaction at parity and are independent of the cryptocurrency market, unlike fungible tokens'.[36]

10 NFTs, which are sometimes called 'digital diamonds' have undoubtedly become a digital trend in the current era due to these characteristics. It has been pointed out that:

> "(....) There is a growing interest in using NFTs to stimulate a new paradigm around business value propositions and intellectual work. The *momentum* is driven mainly by three factors: the opportunity for creators to exercise and transmit the rights associated with such items; the possibility for users to boast about owning such objects; and the facilitation of marketing and advertising strategies that can leverage such items."[37]

B. The Kinship between NFTs and Trademark Law

11 It has been observed that '[i]n a space where nearly anything can be minted and sold as an NFT,[38] from a tweet to a digital luxury good, the potential legal implications [of NFTs] are endless for both buyers and sellers, as well as NFT trading platforms'.[39] While it is true that NFTs can tokenize any form of valuable data capable of being stored digitally, what needs to be appreciated from a legal perspective is that the NFT is distinct from the virtual or the physical asset or the digital artwork which underlies the NFT.[40] Most importantly, when 'an NFT represents a virtual good or is linked to a physical good, each NFT is only a marker (or pointer) to the virtual good or the physical good, but it is not the "the good" itself'.[41] It follows that NFTs often contain a web link to the original work 'because the non-fungible token is not the work itself, rather a unique digital signature that is linked in some way to an original work'.[42] At this point, one may wonder why people sometimes pay astronomical prices to purchase a mere web link that points to a virtual or a physical asset or some digital artwork,[43] if the concomitant transfer of ownership or possession of the underlying asset is not envisaged by an NFT sale. The answer is simply that: '[t]his is not ownership in a traditional sense, and yet the money flows into the NFT marketplace where the bragging rights and "ownership" value of being recorded on the blockchain as the registered owner of a digital or physical item exceeds the value of the uninhibited right to possession and use of the item'.[44] Thus, digital bragging rights are valued more than the asset itself.[45]

12 Evidently, therefore, ownership of an NFT does not necessarily guarantee the ownership of the underlying asset nor the intellectual property rights pertaining to such asset. A corollary of this

Tokens) (Kindle Edition 2022).

35 See Sestino, Guido and Peluso (n 7) 13: ('Whereas [fungible tokens] are divisible into fractions, NFTs are not mutually interchangeable and thus totally indivisible.'). (citations omitted)

36 Singh Rawat et al (n 27)

37 Sestino, Guido and Peluso (n 7) 13.

38 See Guadamuz (n 18) 33. ('Any digital work, including physical goods, which can be represented in digital form, such as a photo, video or a scan can be turned into a non-fungible token').

39 Yoder (n 11) 1.

40 See Murray (n 3) (noting that 'NFTs are separate from the items that are "tokenized" by the NFT (i.e., linked to the NFT by the process of minting the NFT))'.

41 MLL Meyerlustenberger Lachenal Froriep Ltd, 'NFTs and Trademarks – What You Need to Know' (*MLL News Portal,* 8th April 2022) < https://www.mll-news.com/nfts-and-trademarks-what-you-need-to-know/?lang=en> accessed 27th December 2022.

42 Guadamuz (n 18) 34.

43 See Liew Voon Kiong, *Web3 Made Easy: A Comprehensive Guide to Web3: Everything you need to know about Web3, Blockchain, DeFi, Metaverse, NFT and GameFi* (Liew Voon Kiong 2022) 127 ('In fact, the NFT purchaser owns nothing more than a unique hash on the blockchain with a transactional record and a hyperlink to the file of the original creation.') (citations omitted)

44 Murray (n 3).

45 See Robert Barbera, *Retire and Refire: Financial Strategies for People of All Ages to Navigate Their Golden Years with Ease* (Kindle edition 2022): 'People are paying money, tens and hundreds and sometimes millions of dollars, for the bragging rights of owning a digital piece of art.' See also Peter Cramer and Brendan O'Rourke, 'As NFTs Blur the Line between "Receipt" and "Product", Trademarks Owners Fight over New Virtual Markets' (2022) 42 The Licensing Journal, art 5, 5: 'Often, it is ownership of the NFT itself—and the associated benefits, such as entry into specific communities, self-branding on social media, or participation in business ventures, not to mention potential for return on investment—that the purchaser desires'.

is that an NFT does not eliminate the possibility that someone other than the owner of the NFT holds property rights over or intellectual property rights in the underlying good itself.[46] Axiomatically, therefore, NFTs can impinge upon the rights of a trademark owner where the NFT displays or otherwise incorporates a trademark that belongs to a person other than the one who minted the NFT.[47] This is in fact ironic because there was a lot of anticipation that the NFTs would inhibit misuse and exploitation of intellectual property owing to their unique authentication system.[48] Whilst it is true that the immutability of ownership records in NFTs means that the avenues for the misappropriation of a trademark will be limited if not foreclosed where the NFT is minted by the trademark owner himself or by any other person with his permission[49]; the converse happens when the creator of the NFT incorporates a third party's trademark without permission.[50] In effect, this may not only be prejudicial to the interests of the trademark owner but can even be detrimental to consumers as such NFT can cause consumer deception. Kathryn Park points out that:

"In the wild-west environment, trademark risks abound. First, sales that rely on the goodwill of a brand may accrue to someone other than the brand owner (...). Second, customers who purchase a fraudulent NFT may end up disgruntled that an expensive item is not an authorized branded one, as the value they have invested in the NFT disappears."[51]

13 Additionally, trademark owners' rights can also be affected due to the proliferation of bad faith trademark filings in respect of Metaverse or NFTs. It has been pinpointed that, 'bad actors are trying to usurp valuable trademark rights in the metaverse with preemptive filings. Bad faith applications for metaverse trademarks abound.'[52] In fact, well-known brand owners, having now realized their vulnerability in the crypto world, are accordingly taking steps to remedy the situation by filing applications to register their marks for NFT-associated goods or services, notwithstanding the classification turmoil[53] that exists. Taco Bell, Coca-Cola, and Nike are just a handful of the big-name brands that are making their initial forays into the NFT world.[54]

14 However, the fundamental question remains whether the conventional trademark law regime is sufficiently equipped to grapple with the legal conundrums which NFTs have unveiled. Whilst some legal experts believe that trademark issues connected with NFTs can be addressed by the existing trademark law[55], others offer dissenting views. It has been cautioned that '[t]he enormous price tags [NFTs] carry will undoubtedly spawn hotly

46 See K. S Divyashree and Achyutananda Mishra, 'Blockchain Technology in Financial Sector and its Legal Implications' in Mousmi Ajay Chaurasia and Chia-Feng Juang, *Emerging IT/ICT and AI Technologies Affecting Society* (Springer Nature 2022) 225 ('Buying an NFT does not mean that one is buying the underlying [intellectual property] rights in a given content'.)

47 Yoder (n 11) 5: 'Some brands are claiming that NFTs have infringed upon or diluted their trademarks, whether that be in a piece of digital art or fake store locations in virtual cities'

48 See Julia Bishop et al, 'NFTs, Brands, and the Metaverse' (*INTA*, 16th February 2022) <https://www.inta.org/perspectives/features/nfts-brands-and-the-metaverse/> accessed 3rd January 2023. ('Brand owners see anticounterfeiting applications as one of the strongest cases for using blockchains, as NFTs can be used to authenticate physical products and provide a product's transaction history').

49 As duplication of the NFT is difficult if not impossible.

50 See Yoder (n 11) 14: 'Even corporate trademarks are not safe in the Metaverse, with other opportunists quick to profit from associating their NFTs with famous brands in their quest to become the next Beeple. The number of IP infringement issues continues to grow with the NFT industry's popularity, leading to new precedents being set both in the physical world and in the Metaverse'.

51 Kathryn Park, 'Trademarks in the metaverse' [2022] WIPO Magazine 1, 30.

52 ibid 31. The author further notes that: 'In the United States, for example, bad faith applications for metaverse marks have been spotted recently for fashion brands like Prada and Gucci. These bad filings are a major challenge for trademark owners because combatting such bad faith applicants has a price; potentially huge legal fees and a drain on corporate resources'.

53 This point will receive further discussion below.

54 Mansi Jain, 'Trademark Protection in NFT's' (*Law Daily*, 15th July 2022) <https://www.lawdaily.cslr.in/2022/07/trademark-protection-in-nfts.html?m=1> accessed 6th December 2022.

55 See for example Mary Kate Brennan, 'Nike's Trademark Fight Against StockX Moves Offline' (*IPWatchdog*, 18th May 2022) <https://ipwatchdog.com/2022/05/18/nikes-trademark-fight-stockx-moves-offline/id=149098/> accessed 28th December 2022: 'Navigating the legal world of NFTs can seem confusing because many consumers and brands are not well-versed in the technology, legal regulations are sparse, and no case has yet made it to a decision on the merits. That said, basic legal principles – especially trademark and other intellectual property laws – should apply'.

contested legal challenges if something goes awry'.[56] Therefore, and also for the purpose of establishing legal certainty, it is important that the adequacy of a country's trademark law regime to tackle NFTs-related issues is periodically assessed.

15 Notably, NFTs-related trademark issues have surfaced prominently in the USA and the controversial legal issues that cropped up in the cases of *Hermès Int'l v. Rothschild*[57] and *Nike Inc. v. StockX LLC*[58] have seemingly baffled the USA courts. In *Hermès Int'l v. Rothschild*, the defendant minted a collection of NFTs depicting digital images of handbags titled "MetaBirkins," which Hermès claimed, did infringe its famous BIRKIN trademark used for luxury handbags. By contrast, Nike case concerned NFTs which were linked to physical goods. The dispute arose when StockX launched its Vault NFT collection, with each NFT tied to a physical item that StockX sold, including well-known Nike sneakers.[59] Nike specifically alleged that:

"Without Nike's authorization or approval, StockX is 'minting' NFTs that prominently use Nike's trademarks, marketing those NFTs using Nike's goodwill, and selling those NFTs at heavily inflated prices to unsuspecting consumers who believe or are likely to believe that those 'investible digital assets' (as StockX calls them) are, in fact, authorized by Nike when they are not."[60]

16 Similarly, in *Juventus F.C. v Blockeras s.r.l*[61] where a European court for the first time looked at trademark infringement issues in the context of NFTs, the allegation of Juventus F.C. was that the NFTs sold by Blockeras featuring an Italian football player wearing a Juventus jersey 'infringed its word marks for 'JUVE' and 'JUVENTUS' and figurative mark consisting of the black and white striped jersey with two stars on the chest,' [62] The unprecedented legal issues that came to light in these cases, unmistakably bear testimony to the fact that technology has outstripped the traditional legal structures. Against that backdrop, the quintessential question that this article delves into is whether the law governing trademarks in Sri Lanka can withstand the issues posed by NFTs. The law relating to trademarks in Sri Lanka is encapsulated primarily within the Intellectual Property Act No. 36 of 2003.[63] Apart from the statutory legal regime, the common law action of passing off is also invoked in the context of trademark disputes in Sri Lanka. However, close and careful scrutiny of Sri Lanka's traditional legal regime on trademarks reveals certain gaps where NFTs are considered. The complexity of these issues is exacerbated by the extremely sophisticated nature of the technology deployed by NFTs, the enigmatic characterization of NFTs as well as the relative newness of the concept of NFTs in Sri Lanka. The popularity of the concept of NFTs has just begun to rise in Sri Lanka. Several projects involving NFTs have been launched during the year 2022 and Dialog Axiata PLC, one of Sri Lanka's largest telecommunications service providers and the country's largest mobile network operator recently introduced Sri Lanka's first fully immersive Metaverse which also incorporates NFTs.[64] However, unlike the crypto community, the legal experts and the judiciary of Sri Lanka do not seem to have still had the time or opportunity to acquaint themselves with these concepts.

17 The issue of whether Sri Lanka's existing legal regime on trademarks can tackle the challenges posed by NFTs is addressed below under four specific headings (i) Registration and classification issues (ii) establishing misleading /confusing similarity between virtual and physical goods in cases involving unauthorized registrations/ uses (iii) application of the exhaustion and nominative fair use defenses (iv)

56 Park (n 51) 33

57 *Hermès Int'l v.Rothschild,* 590 F. Supp. 3d 647 (S.D.N.Y. 2022)

58 *Nike Inc. v. StockX LLC*, 1:22-cv-. 00983 (S.D.N.Y. February 3, 2022).

59 See Andrew Rossow, 'The Nike v. StockX Lawsuit Could Determine What Type of NFTs Can Be Created' (*Nftnow* 26th May 2022) < https://nftnow.com/features/the-nike-v-stockx-lawsuit-could-determine-what-type-of-nfts-can-be-created/> accessed 12th January 2023.

60 Brooks Kushman, 'Nike v. StockX Case Highlights Many Unanswered Questions About IP and NFTs' (*JDSupra* 7th September 2022) < https://www.jdsupra.com/legalnews/nike-v-stockx-case-highlights-many-9205701/> accessed 15th January 2023. See also: 'Nike files trademark infringement lawsuit against StockX NFTs' (*Retail Insight Network* 7th February 2022) <https://www.retail-insight-network.com/news/nike-stockx-lawsuit/> accessed 8th December 2022.

61 *Juventus F.C. v Blockeras s.r.l*, Docket No. 32072/2022, Court of Rome IP Chamber, 20/07/2022

62 'Are trade marks protected in the metaverse?' (EUIPO European Union Intellectual Property Office, 23rd June 2022) <https://euipo.europa.eu/ohimportal/en/web/guest/key-user-newsflash/-/asset_publisher/dIGJZDH66W8B/content/id/14049958?> accessed 10th June 2023.

63 Intellectual Property Act No. 36 of 2003 of Sri Lanka (Hereinafter 'IP Act').

64 'Dialog Launches 'Futureverse' - Sri Lanka's First Fully Immersive Metaverse' (*Dialog*, 1st January 2023) <https://dlg.dialog.lk/news/dialog-launches-futureverse-srilanka-first-fully-immersive-metaverse> accessed 5th January 2023.

application of certain statutory remedies to NFTs. In exploring these issues, examples shall be drawn from comparative jurisdictions, particularly, the USA.

I. Registration and classification issues

18 It is undisputed that '[f]iling (or re-filing) trademark registrations embracing goods and services related [to] the metaverse, online world, digital art, and NFT to protect your trademarks in the online world may result in better protection'.[65] Importantly, however, the registration of trademarks is carried out in Sri Lanka based on the international classification of goods and services. In terms of Section 106 (1) (d) of the IP Act, an application for registration of a mark shall *inter alia* contain 'a clear and complete list of the particular goods or services in respect of which registration of the mark is requested, with an indication of the corresponding class or classes in the international classification, as may be prescribed.' Notably, however, Sri Lanka is not a party to the Nice Agreement Concerning the International Classification of Goods and Services for the Purposes of the Registration of Marks.[66] Yet, Sri Lanka 'follows in substance the classification recognized therein'.[67] In fact, Regulation 16 of Intellectual Property Regulations No. 01 of 2006[68] incorporated the international classification of goods and services embedded in the Nice Agreement.[69] Although the Regulation in essence incorporated the 2006 version of the Nice Agreement, the National Intellectual Property Office (NIPO) of Sri Lanka as a practice follows the latest version of the so-called Nice Classification, albeit the legitimacy of such adoption could be in question. As such issues fall outside the remit of this paper, it is apposite only to consider how the NFTs-related goods or services can be designated in a trademark application in Sri Lanka.

19 Until the 12th edition of the Nice classification was adopted in 2023, it suffered from not having NFTs-related goods or services specifically listed in the classification.[70] The problem of not having a particular item specifically listed in Nice Classification is that on the one hand, it gives broad leeway to the national offices to adopt divergent approaches in accommodating or refusing to accommodate applications designating such goods or services; and on the other, it creates legal uncertainty in trademark registration disputes, especially where the similarity of goods or services of the marks in question is challenged.[71] However, even before the 12th edition of the Nice Classification was introduced, taking cognizance of the sudden upsurge in the number of trademark applications seeking registrations for Metaverse and NFTs associated goods and services; 'the European Intellectual Property Office (EUIPO), which has responsibility for EU trademark registrations, issued guidance on its approach to classifying virtual goods and NFTs'.[72] The EUIPO stated that NFTs fall under

65 Jain (n 54).

66 Nice Agreement Concerning the International Classification of Goods and Services for the Purposes of the Registration of Marks (as amended on September 28, 1979) <https://www.wipo.int/wipolex/en/treaties/textdetails/12617>. (Hereinafter 'Nice Agreement'). See also Wipo-Administered Treaties (*WIPO IP Portal)* https://www.wipo.int/wipolex/en/treaties/ShowResults?search_what=C&treaty_id=12 accessed 4th January 2023. See further Jessie N. Roberts, *International Trademark Classification: A Guide to the Nice Agreement* (Oxford University Press 2012) 13 (Introduction) ('Its purpose was to create a classification system for goods and services that would be used by as many countries as possible to promote consistency in trademark classification within national trademark offices.')

67 D M Karunaratna, *Elements of the Law of Intellectual Property in Sri Lanka* (Sarasavi Publishers 2010) 25.

68 Intellectual Property Regulations No. 01 of 2006 published in the Extraordinary Gazette No.1445/10 dated May 17, 2006.

69 Regulation 16 states that 'The application for registration of a mark may relate to goods or services of any one class of the international Classification set out in the fourth Schedule hereto'.

70 It is noteworthy that in *Juventus F.C. v Blockeras s.r.l*,(n 61) the court found that defendant's NFTs infringed the plaintiff's trademark registration (in particular for class 9) covering goods not included in the Nice Classification and that are inherent to downloadable electronic publications. See further 'Are trade marks protected in the metaverse?' (EUIPO European Union Intellectual Property Office, 23rd June 2022) <https://euipo.europa.eu/ohimportal/en/web/guest/key-user-newsflash/ /asset_publisher/dIGJZDH66W8B/content/id/14049958?> accessed 10th June 2023

71 In the absence of NFTs specific registrations it has been commented that: 'As a consequence, a rigorous interpretation of trademark law would infer that there is no trademark infringement because the goods and services are unique. At the time, there is no case law in this area, therefore courts may take a different approach': Jain (n 54).

72 Roisin Culligan and Jane Gallagher, 'Brand Protection in the Metaverse: EUIPO Updates Guidance on Trade Mark Applications for NFTs and Virtual Goods' (*William Fry* 14th July 2022) < https://www.williamfry.com/newsandinsights/news-article/2022/07/14/brand-protection-in-the-

Class 9 of the Nice Classification list. It further stated that: '[f]or the Office, the term *non fungible tokens* on its own is not acceptable. The type of digital item authenticated by the NFT must be specified. Services relating to (…) NFTs will be classified in line with the established principles of classification for services'.[73] Thus, examples of acceptable specifications include: '"*downloadable music authenticated by NFTs*" in class 9 [and] "*providing an online virtual environment for trading virtual art and virtual art tokens*" in class 35'.[74] It appears however that in issuing this guideline, EUIPO took inspiration from the proposed revision to the Nice Classification.

20 The 12th edition of the Nice Classification which became effective on the 1st of January 2023, for the first time, referred to the term NFTs. It includes the specific item- 'downloadable digital files authenticated by non-fungible tokens [NFTs]' in class 9. This is undeniably a much-needed extension of the Nice classification in the digital age. Notably, however, the wording of the new item is premised on the cardinal principle that the NFTs are distinct from their underlying assets.[75] It has been remarked that:

21 Only the content linked to the NFT is included in the classification, not the NFT itself. So the code sequence itself cannot be registered, as it is neither a good nor a service. Protection as a computer program is also rightly to be denied to the individual token. In this respect, it is consistent to tie in the content linked to the NFT when expanding the classification.[76]

22 This could be the reason why the classification is silent about NFTs linked to physical assets. The idea is perhaps that when an NFT is authenticating a physical asset as opposed to a digital asset or digital artwork, it can be protected by the existing categories of goods to which the particular physical asset belong for the reason that it is not the NFT that is deemed relevant for trademark registration purpose but the underlying asset. But this posits the question of whether the existing classification of physical goods can adequately ensure protection for the phenomenon of 'phygital NFTs'.[77] It could be argued that the Nice Classification should be further expanded to incorporate 'phygital NFTs' as owners of trademarks used in relation to phygital NFTs will find themselves in the vexing situation of not having a definite class in which they can file the relevant trademark applications.[78]

23 Although no mention has been made of the NFTs-related services, it has been observed that 'they will be classified in line with the established principles of classification'.[79] Needless to say, this is controversial. In fact, the Court of Justice remarked in IP Translator[80], the purpose of the registration system, part of which is the Nice Classification, is that "economic operators must be able to acquaint themselves, with clarity and precision with registrations or applications for registrations made

metaverse-euipo-updates-guidance-on-trade-mark-applications-for-nfts-and-virtual-goods> accessed 10th January 2023.

73 Virtual Goods, Non-Fungible Tokens and the Metaverse (n 12).

74 'EUIPO guidance on classifying virtual goods and NFTs' (*Walker Morris,* 1st December 2022) <https://www.walkermorris.co.uk/in-brief/euipo-guidance-on-classifying-virtual-goods-and-nfts/> accessed 23rd December 2022. (emphasis is original).

75 See 'EU intellectual property office publishes approach for classifying virtual goods and NFTs' (*CMS Law-Now* 22nd August 2022) <https://cms-lawnow.com/en/ealerts/2022/08/eu-intellectual-property-office-publishes-approach-for-classifying-virtual-goods-and-nfts> accessed 27th December 2022. ('The term is not understood to mean the digital item itself, but instead is the means of certification and cannot be accepted for classification purposes. An acceptable example would be 'downloadable digital art, authenticated by an NFT')

76 'Trade mark law: new Nice Classification to enter into force, including digital goods with NFTs' (*Pinsent Masons* 15th December 2022) < https://www.pinsentmasons.com/out-law/news/neue-nizza-klassifikation-umfasst-digitale-gueter-mit-nfts> accessed 29th December 2022.

77 'Physical NFTs: Bridging the Gap Between Digital and Physical Worlds' (*Binance Blog* 22nd September 2022) <https://www.binance.com/en/blog/nft/physical-nfts-bridging-the-gap-between-digital-and-physical-worlds 7460772280213595786 > accessed 8th January 2022. ('Physical NFTs are digital tokens tied to real-world assets. Also referred to as phygital NFTs, these assets combine the digital and physical and can be used to prove ownership over real-world assets, such as artworks, fashion goods, property deeds, tickets, and more.'). See also Alex Bordenhttps, 'What Are Phygital NFTs? : Everything to Know (With Examples)' (*NFT Lately* 6th December 2022) accessed 4th January 2023; where the author cites as an example of a phygital asset 'the RTFKT x Fewociuos collaboration in which, buyers of an NFT would receive an actual pair of shoes featuring art by NFT artist Fewocious'.

78 However, it may also be necessary to determine if such hybrid goods with both physical and digital properties fit in with class 9 goods, or whether they can be categorized under a totally different class.

79 EU intellectual property office publishes approach for classifying virtual goods and NFTs (n 75)

80 CIPA v Registrar of Trade Marks (IP Translator), Case C-307/10

by their actual or potential competitors and thus to obtain relevant information about the rights of third parties."[81]

24 The most intriguing question remains, of whether a trademark registration for the physical goods would automatically extend to the corresponding virtual goods tokenized by NFTs. At this juncture, it is of paramount importance to draw the distinction between digital artwork and virtual goods; both of which can be tied to an NFT. For example, in *Hermès Int'l v. Rothschild*[82], the Court recognized that 'an NFT could link to a digital media file that is just an image of a handbag or could link to a different kind of digital media file that is a virtual handbag that can be worn in a virtual world'.[83] Whilst the degree of similarity between a physical commodity and a mere digital artwork representing the physical commodity may be too low to exclude this possibility; the question that has frequently been posed is whether the degree of similarity between a physical commodity and its virtual counterpart is sufficiently high to automatically extend a registration of the former to the latter.

25 The following excerpt highlights this point:

"For example, while the sale of *physical* fashion items both in the real world and via metaverse is likely to be protected by the trademark registration for "clothing" in Nice Class 25, the question for fashion brands intending to sell *virtual* goods via the metaverse is whether virtual versions of the clothing could also be covered by Class 25 or whether this might require additional trademark registrations in other goods and services classes. Again, this question is rather important for smaller, less established brands in particular, as well-known brands are more likely to be able to rely on their already established reputation and therefore can claim cross-class trademark protection."[84]

26 Although 'the Nice Classification in registration disputes must not be decisive for deciding similarity between the products'[85] it gives indications that can be used in the assessment of identity or similarity of goods/services. It has been pinpointed that:

"(...) Nice Classification provides significant guidance when deciding [similarity between the products], in particular in registration disputes where the products of the conflicting marks are documented, for the senior trademark as part of the registration certificate, and for the junior mark as part of the application. In infringement disputes, the EU trademark legislation stresses the influence of the products for which the senior trademark is registered."[86]

27 Even in Sri Lanka, the Nice classification serves more than a pure administrative function. The examining officer of the NIPO relies on the Nice Classification when conducting the requisite trademark database search to determine whether the mark under examination conflicts with a mark already filed or registered with the NIPO. So, the criticism that 'the new version of the Nice Classification provides no answer as to what extent digital goods can be confused with their real counterparts from [a trademark] law point of view – for example, whether the digital handbag is similar to the physical handbag'[87] cannot be easily ignored. Perhaps, had there been no omission on the part of the Nice Classification to specifically categorize 'virtual goods' under a particular class, this anomaly could have been avoided. Classifying it under class 9, for example would have provided the necessary guidance to the examining officers and the courts. For instance, the EUIPO and USPTO guidelines have explicitly provided for 'virtual goods' in class 9.[88] On the contrary however, it can be argued that 'downloadable digital files authenticated by non-fungible tokens' categorized under class 9 does cater to both digital artwork and virtual goods and that

81 Rasmus Dalgaard Laustsen, *The Average Consumer in Confusion-based Disputes in European Trademark Law and Similar Fictions* (Springer 2020) 88.

82 *Hermès Int'l* (n 57)

83 ibid. The Court further emphasized that the fashion industry has just started 'offering virtual fashion items that can be worn in virtual worlds online (most commonly, for now, in the context of videogames, but with potential to expand into other virtual worlds and platforms as those develop), and NFTs can be used to create and sell such virtual fashion items'.

84 MLL Meyerlustenberger Lachenal Froriep Ltd (n 41).

85 Laustsen (n 81) 332

86 ibid.

87 Trade mark law: new Nice Classification to enter into force, including digital goods with NFTs (n 76).

88 For EUIPO guidelines see Virtual Goods, Non-Fungible Tokens and the Metaverse (n 12): 'Virtual goods are proper to Class 9 because they are treated as digital content or images. However, the term virtual goods on its own lacks clarity and precision so must be further specified by stating the content to which the virtual goods relate (e.g. downloadable virtual goods, namely, virtual clothing)'; for USPTO guidelines see: USPTO, 'Registering trademarks for newer technologies: NFTs, blockchain, cryptocurrency, and virtual goods' <https://www.uspto.gov/sites/default/files/documents/TM-Newer-Technologies-handout.pdf> accessed 2nd January 2023.

the question of whether a digital good associated with an NFT is similar to the corresponding physical good is now an issue for 'substantive law'.[89]

28 There is no doubt that prospective registrants of goods associated with NFTs will benefit from the addition of the new item 'downloadable digital files authenticated by non-fungible tokens' to class 9 of the Nice Classification. As NIPO of Sri Lanka by practice follows the latest edition of the Nice Classification, a person seeking registration for NFTs-related goods in Sri Lanka will definitely benefit from this extension. Nevertheless, there are still gaps in the classification vis-à-vis the categorization of NFTs-related goods or services both at the global and domestic levels. Until a solution is reached at the international level, some guidelines can be issued by the Minister on these murky classification issues. As per Section 204 (2) (b) of the IP Act, the Minister is vested with powers to make regulations in respect of *inter alia* the classification of goods and services for the purposes of registration.

II. Establishing misleading / confusing similarity between virtual and physical goods in cases involving unauthorized registrations/ uses

29 The ambiguity concerning the similarity between the physical goods and their corresponding digital goods can have a serious impact on opposition matters, infringement suits and nullity actions, if the claimant is required to establish 'likelihood of confusion' under such action. It is trite law that '[i] n addition to similarity between the sign and the mark, the similarity of goods and services for which the signs are or shall be used must also be taken into consideration for assessing likelihood of confusion'.[90] Whilst it was highlighted in the previous discussion that the Nice classification is silent on the point whether a virtual good could be considered similar to its physical counterpart (perhaps, rightly so), it is pertinent to look at whether the traditional tests for assessing similarity between goods and services espoused by the judiciary throw any light upon the issue. One of the most widely accepted tests on the assessment of similarity between the goods or services is to be found in the EU case, *Canon KK v Metro-Goldwyn-Mayer Inc.*[91] where the European Court of Justice laid down a non-exhaustive list of criteria to be considered[92]:

"In assessing the similarity of the goods or services concerned, all the relevant factors relating to those goods or services themselves should be taken into account. Those factors include, inter alia, their nature, their end users and their method of use and whether they are in competition with each other or are complementary."[93]

30 The multifactor test introduced in Canon is considered to be less strict[94] than the test laid down in the UK case, *British Sugar plc v James Robertson & Sons Ltd.*[95] The view has been expressed that '[t]his liberal approach to similarity of goods should make it easier to demonstrate actionable confusion, and consequently will reduce the number of situations in which [trademark] owners will have to tolerate others from sharing their marks.'[96] Nonetheless,

89 See Lionel Bently et al, *Intellectual Property Law* (Oxford University Press 2022) 1053 (footnotes omitted).

90 Annette Kur, *European Intellectual Property Law: Text, Cases and Materials* (Edward Elgar Publishing Limited 2019) 251. In *British Sugar PLC v. James Robertson & Sons LTD.*, [1996] RPC 281, (EWHC), it was held that 'likelihood of confusion' was only to be considered after it had been established sequentially that the goods and the marks were similar. See also Catherine Seville, *EU Intellectual Property Law and Policy* (Edward Elgar Publishing 2016) 324. ('Likelihood of confusion presupposes both that the mark applied for and the earlier mark are identical or similar, and that the goods or services covered in the application for registration are identical or similar to those in respect of which the earlier mark is registered').

91 Case C-39/97 *Canon KK v Metro-Goldwyn-Mayer Inc* [1998] ECR I-5507

92 Laustsen (n 81) 332

93 *Canon KK* (n 91) I - 5509

94 See Helen Norman, *Intellectual Property Law Directions* (2nd edn, Oxford University Press 2014) 32

95 *British Sugar PLC* (n 90). The test required the following factors to be considered: (a) The respective uses of the respective goods or services; (b) The respective users of the respective goods or services; (c) The physical nature of the goods or acts of service; (d) The respective trade channels through which the goods or services reach the market; (e) In the case of self-serve consumer items, where in practice they are respectively found or likely to be found in supermarkets and in particular whether they are, or are likely to be, found on the same or different shelves; (f) The extent to which the respective goods or services are competitive. This inquiry may take into account how those in trade classify goods, for instance whether market research companies, who of course act for industry, put the goods or services in the same or different sectors.

96 Ilanah Simon Fhima, 'Same Name, Different Goods-Death of the Principle of Specialty' in Ilanah Simon Fhima (ed), *Trade Mark Law and Sharing Names: Exploring Use of the Same Mark by*

extension of this test to the assessment of similarity between physical goods and their virtual replicas does not seem to yield desirable results for the trademark owner, as the very nature, end users, methods of use and marketplace of NFTs-related virtual goods would naturally be different. For instance, the excerpt below highlights the peculiar and distinct nature, marketplace and consumer base of virtual garments which stand in stark contrast to those of the physical goods:

"Fashion companies can now reach new audiences that don't typically interact with brands in physical formats, stay ahead of the curve with younger consumers, monetise their digital assets in communities accustomed to paying for premium experiences, and test which designs are most attractive to users, so that they may subsequently direct their productive efforts towards those who buy designs for their avatars."[97]

31 To elaborate this point further, where the physical clothing is compared with the virtual garment tokenized by an NFT, it is self-evident that the nature of the goods juxtaposes with one another- one being a physical asset, the other a digital manifestation embodied in an NFT. Their end-users are different, as the coveted luxury garments are often purchased by luxury customers and the virtual garments are presumably purchased by gamers, collectors or crypto enthusiasts.[98] The idea has in fact been expressed that '[t]he target market for these NFTs is not necessarily fashionistas. In many cases, buyers of virtual garments are investors interested in their fashion value (...).'[99] The method of use of the goods would be different as virtual clothing would be used to dress an avatar or as a collectible. 'It will mean creating a completely new relationship with clothes. Fashion [in its traditional sense] has been considered a highly hedonic category that needs to be touched and worn to be fully enjoyed. The tactile experience has been considered very important [with regard to materialistic outfits]'.[100] Contrastingly, virtual clothing does not evoke similar sensations in consumers. At the same time, the two products can hardly be said to be in competition although in rare situations they could be complementing each other.[101] This is because the physical bags are sold in traditional markets or e-commerce platforms[102] whereas NFTs are sold in the crypto or NFT marketplaces. Thus, the application of the multi-factor test seems to go against any finding of similarity between the physical goods and their digital twins.

32 Another murky issue is the similarity between digital artwork embodied in NFTs and their physical counterparts. Even if one concedes that the Nice Classification provides some guidance on the assessment of similarity between digital artwork authenticated by NFTs and their corresponding physical goods by the sole fact of classifying them in distinct classes, (except in situations where the concerned physical goods also fall under Class 9), it may still be necessary to gauge the proximity between these two types of goods by resorting to traditional criteria, especially in trademark disputes involving third parties. In *Hermès Int'l v. Rothschild*, where the defendant Mason Rothschild created digital images of faux-fur-covered versions of the luxury Birkin handbags of plaintiffs Hermès and titled these images "MetaBirkins" and sold them using NFTs, the plaintiff *inter alia* claimed trademark infringement under the Lanham Act.[103] Interestingly,

Multiple Undertakings (Edward Elgar Publishing 2009) 116

97 Mercedes Rodriguez Sanchez and Guillermo Garcia-Badell, 'Dressing the Metaverse. The Digital Strategies of Fashion Brands in the Virtual Universe' in Ana Cristina Broega et al (eds.), *Advances in Fashion and Design Research: Proceedings of the 5th International Fashion and Design Congress, CIMODE 2022, July 4-7, 2022, Guimarães, Portugal* (Springer 2023) 395.

98 See Anndy Lian, *NFT: From Zero to Hero* (Anndy Lian 2022) 27 (noting that 'The current NFT market participants are mostly crypto users'). See also ibid 393: 'From the outset of this organic link between fashion and NFTs, digital native brands have forged the path that traditional analogue firms have followed. Lacking physical storefronts or well-known logos, their products have, nevertheless been embraced by a more technologically advanced cryptographic community'.

99 Claudia E. Henninger et al, *Sustainable Fashion Management* (Routledge 2023) 166

100 ibid 165 (citations omitted).

101 For example, where the NFT is used to authenticate a physical good.

102 See Pengtao Li, 'Emerging Trends of E-Business' in In Lee (ed.) *Encyclopedia of E-Business Development and Management in the Global Economy* (IGI Global 2010) 1162: ('Traditional commerce is defined as trade that occurs in traditional retail environments, such as face-to-face or over the phone. (...) E-commerce is trade that occurs over a retail website (...)').

103 *Hermès Int'l* (n 57). See also Yoder (n 11) 11 ('Trademark infringement, Hermès' first cause of action, is the unauthorized use of a trademark on or in connection with goods in a manner that is likely to cause confusion, deception, or mistake about the source of the goods. (....) Hermès has registered its BIRKIN trademark with the USPTO well before filing this the complaint, so its primary focus in the lawsuit will be on the likelihood of confusion between Hermés' BIRKIN mark and Rothschild's MetaBirkin mark. A likelihood of confusion between trademarks exists when "the marks are so similar and the goods for which they

it has been observed that:

"What may prove tricky for Hermès is showing that the physical goods it is known for are so closely related to Rothschild's digital MetaBirkins that consumers are likely to assume they originate from the same source. There are obvious differences in the products each party sells; the most glaring of which is that Hermès sells luxury tangible goods while MetaBirkins are intangible NFTs that only exist on a blockchain. At first glance, it may appear that MetaBirkins are the furthest thing from any product that Hermès sells, regardless of the name, but as more and more brands venture into the Metaverse, the likelihood of Hermès winning this argument increases."[104]

33 As pointed out in the above excerpt, the similarity between a physical good and a digital artwork representing such a good appears to be very remote at least at the first glance. But, in this case, Hermès has already produced evidence of actual confusion on the part of consumers about Hermès's affiliation with Rothschild's MetaBirkins collection.[105] Interestingly, the application of the multi-factor test to determine the similarity between phygital goods associated with NFTs and their physical counterparts would not be easy, yet, would be less challenging than applying the test to virtual goods or digital artwork tied to NFTs. However, when one takes into consideration the unconventional nature of NFTs, one is made to ponder whether the traditional tests of assessing similarity between goods and services are apt and fitting in the context of NFTs.[106]

34 Evidently, the assessment of similarity between goods and services becomes important where a statutory provision embodies the specialty principle. In fact, when one looks at the scheme of the IP Act of Sri Lanka, it appears that several sections of the IP Act are based on the so-called specialty principle in trademark law. The principle of specialty denotes that 'trademarks can only be protected in relation to the same or similar goods or services covered by their registration or use.' A limited exception to this principle is envisaged in the case of well-known trademarks. Thus, Section 104 (1) (a) of the IP Act denies registration to a mark that is misleadingly similar to a mark that is registered or filed by a third party for identical or similar goods or services. Similarly, Section 104 (1) (b) of the IP Act denies registration to a mark that is misleadingly similar to a mark used earlier in Sri Lanka for identical or similar goods or services. In like manner, Section 104 (1) (d) first limb, refuses registration to a mark that is misleadingly similar to a mark well-known in Sri Lanka for similar goods or services. Furthermore, Section 160 (2) of the IP Act stipulates that 'any act or practice carried out or engaged in, in the course of industrial or commercial activities, that causes, or is likely to cause, confusion with respect to another's enterprise or its activities, in particular, the products or services offered by such enterprise, shall constitute an act of unfair competition'. Therefore, when applying these sections, the courts or the NIPO will have to ascertain inter alia the similarity between the concerned goods or services. However, the ostensible lack of harmony that persists between traditional criteria for assessing similarity between goods or services and NFTs-related products or artwork leave room for ample legal uncertainty.

III. Application of the exhaustion and nominative fair use defences

35 The principle of exhaustion which is recognized in both USA[107] and EU denotes that the trademark owner's exclusive right to control the distribution of a trademarked good 'does not extend beyond the first sale of the product and that the resale by the first purchaser of the original article under the producer's trademark is neither trademark infringement, nor unfair competition'.[108] It must be noted however that exhaustion occurs, only with respect to the 'goods' which bear the trademark and which have been put on the market by the owner of such mark or with his consent. It by no means vitiates or transfers the trademark 'right' itself.[109] This is why, without

are used are so related that consumers would mistakenly believe they come from the same source.'"). (footnotes omitted).

104 Yoder (n 11) 12.

105 See *Hermès Int'l* (n 57).

106 See Jain (n 54) ('Many companies have yet to submit trademarks for metaverse, digital art, or NFT, owing to the fact that NFTs are still relatively young. As a consequence, a rigorous interpretation of trademark law would infer that there is no trademark infringement because the goods and services are unique.').

107 Sometimes, in the USA, this is referred to as the doctrine of first sale.

108 See Shubha Ghosh and Irene Calboli, Exhausting Intellectual Property Rights: A Comparative Law and Policy Analysis, (Cambridge University Press 2018) 66 citing *Sebastian International, Inc v Longs Drug Stores Corporation* 53 F 3d 1073, 1074 (9th Cir. 1995) (emphasis added).

109 Only those rights of resale and distribution which are available on that particular piece of good will get exhausted and other rights including the right to apply the mark on new products and commercialize such products shall remain exclusively with the trademark right holder.

Nike's permission, one can sell old Nike sneakers at garage sales, yet cannot manufacture and sell Nike-branded shoes.[110] But most importantly, exhaustion doctrine encapsulates the idea that where trademark rights have been exhausted after the first sale of genuine trademarked goods by the trademark owner or with his consent, resellers not only enjoy the freedom of reselling, but they are also free to use the trademark in advertising that brings the further commercialization of the goods to the attention of the consumers.[111] The Court of Justice of the European Union recognized this principle in *Parfums Christian Dior SA and Parfums Christian Dior BV and Evora BV case*.[112] The court observed that:

"If the right to prohibit the use of his trade mark in relation to goods, conferred on the proprietor of a trade mark under Article 5 of the Directive, is exhausted once the goods have been put on the market by himself or with his consent, the same applies as regards the right to use the trade mark for the purpose of bringing to the public's attention the further commercialization of those goods. (....) If the right to make use of a trade mark in order to attract attention to further commercialization were not exhausted in the same way as the right of resale, the latter would be made considerably more difficult and the purpose of the 'exhaustion of rights' rule laid down in Article 7 would thus be undermined."[113]

36 The complex issue that arises in the context of NFTs is whether the use of an NFT by a reseller of genuine trademarked goods for the purpose of authenticating such physical goods, is tantamount to a mere exercise of the trademark owner's exhausted right to attract attention to further commercialization. However, the answer to that question depends on how one would characterize an NFT. It follows that, if an NFT can be relegated to 'an advertising tag' on the physical goods legitimately purchased, then such use may not amount to trademark infringement. Yet, according to the court, what would be protected in terms of the exhaustion principle is the 'reseller's legitimate interest in being able to resell the goods in question by using advertising methods *which are customary in his sector of trade'*.[114] Therefore, even if one considers an NFT as a mere advertising tag in this instance, the question remains whether its use constitutes an 'advertisement method that is customary in the relevant sector of trade'. The ensuing legal confusion undoubtedly reflects the friction between technology and law.

37 Furthermore, the court pinpointed in *Parfums Christian Dior SA and Parfums Christian Dior BV and Evora BV case* that the defence of exhaustion cannot be invoked 'where there are legitimate reasons for the proprietor to oppose further commercialization of trade-marked goods, especially where the condition of the goods is changed or impaired after they have been put on the market'.[115] The court construed the term 'legitimate reason' to include even 'damage done to the reputation of a trademark'.[116] Thus, it is axiomatic that the ability of the NFT owner to rely on this defence is further curtailed by the so-called legitimate interests of the trademark owner. Thus, the extension of the exhaustion doctrine to NFTs-related matters is a daunting task.

38 An equally confounding issue is the applicability of the 'nominative fair use defence' to situations where the NFT is used merely for the purpose of authenticating a physical product. Nominative fair use is a judge-made doctrine that allows the use of a trademark by a [non-owner] to describe the trademark owner's goods or services if that use does not cause consumer confusion.[117] Hence, 'use of a mark to identify the mark holder's product or service, rather than the secondary user's is nominative fair use'.[118]

39 A three-part test has been developed in the USA case

110 Cramer and O'Rourke (n 45) 2.

111 See Martin Senftleben, 'Intermediary Liability and Trademark Infringement: Proliferation of Filter Obligations in Civil Law Jurisdictions?' in Giancarlo Frosio (ed.) *Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020) 390. See also: Apostolos G. Chronopoulos and Spyros M. Maniatis, 'Common Law and Civil Law Approaches to Trademark Exhaustion in Europe: The Distribution Function of Trademarks' in Irene Calboli and Jane C. Ginsburg, *The Cambridge Handbook of International and Comparative Trademark Law* (Cambridge University Press 2020) 572 ('a trademark proprietor has no authority to control by virtue of their exclusive right the further commercialization of trademarked goods already placed on the market with their consent'.)

112 *Parfums Christian Dior SA and Parfums Christian Dior BV and Evora BV case* (Case C-337/95) [1997] ECR 14 6013

113 ibid I - 6046

114 ibid I-6049 (emphasis added).

115 ibid I - 6048

116 ibid.

117 Jordan Phelan, 'Infringement or Identification?: Nominative Fair Use and the Resale of Luxury Goods' (2022) 91 Fordham L Rev 757, 759.

118 Aaron Schwabach, *Internet and the Law: Technology, Society, and Compromises: Technology, Society, and Compromises* (2nd edn. ABC-CLIO 2014) 110.

New Kids on the Block v. News America Publishing, Inc.,[119] for evaluating nominative fair use: (1) whether a product or service can be easily identified without using the trademark; (2) whether the mark is only used so much "as is reasonably necessary" in order to identify the product or service; and (3) whether the user of the mark can do anything that, in combination with the use of the mark, would imply that the trademark holder endorsed or sponsored the use.[120] The issue that crops up in the context of NFTs is whether the use of an NFT to authenticate genuine products of the trademark owner can be justified on the ground of 'nominative fair use'. The answer however depends largely on how NFTs are characterized. Even then, the NFT owner might find it challenging to establish that the use so contemplated by the NFT does not exceed the limitation imposed by the second criterion. The second criterion, in essence, involves 'an evaluation of whether the use was unreasonably excessive in the context of an otherwise legitimate use'.[121] Aaron Schwabach, for example, states that the use of the Volkswagen *logo* (rather than merely the name) to advertise the repair shop's services would not be insulated against liability on the basis of nominative fair use as such use would be deemed as "more than reasonably necessary to identify the service".[122] Despite the perplexing legal issues that emanate from the extension of the defences of exhaustion and nominative fair use to the NFTs authenticating physical assets; one must understand that protecting the resale market is of singular importance.[123] This principle would apply equally to the resale market involving NFTs. It has also been highlighted that:

"It has been repeatedly acknowledged that the producer of a good cannot prevent others from using the good's mark to truthfully describe the good. This basic belief is the foundation for both nominative fair use and first sale defenses, and "reflects the simple insight that anybody should be free to refer to goods and services by their brand names."[124]

40 In the ongoing case of *Nike Inc. v. StockX LLC*,[125] the USA courts will be compelled to wander into this hazy legal terrain. The case involves Nike filing a lawsuit against StockX, the operator of an online resale platform that sold NIKE sneakers amongst other things, on the ground that "[w]ithout Nike's authorization or approval, StockX is 'minting' NFTs that prominently use Nike's trademarks, marketing those NFTs using Nike's goodwill, and selling those NFTs at heavily inflated prices to unsuspecting consumers who believe or are likely to believe that those "investible digital assets" (as StockX calls them) are, in fact, authorized by Nike when they are not'.[126] StockX contends however, 'that each of its Vault NFTs is tied to a specific product, such as a pair of Nike sneakers it bought second-hand from its rightful owner, which is being sold on its marketplace'.[127] Furthermore, StockX 'opines that Nike's complaint ignores "settled doctrines of trademark law, including the doctrines of first sale and nominative fair use," and argues that their NFTs are more like claims tickets, title trackers, or receipts than products'.[128] However, an interesting feature of this NFTs-related reselling scheme is that '[t]he purchaser will not get possession of the sneakers unless the purchaser gives up the NFT (StockX calls this "redeeming" the NFT)'.[129] But the crucial question is whether StockX's use of the NFT embodying the NIKE trademark can be justified in terms of the doctrine of exhaustion and nominative fair use. The view has been expressed that:

"Together, First Sale and Nominative Fair Use are why the product-receipt distinction matters: A new product, including a virtual product bearing another entity's trademark, cannot be offered for sale without permission from the mark's owner, whereas a mere receipt (which could take the form of a physical piece of paper, an email, or a digital token

119 971 F.2d 302 (9th Cir. 1992).

120 ibid at 306, 308. See Phelan (n 117) 773.

121 Chronopoulos and Maniatis (n 111) 550.

122 Schwabach (n 118) 234. (emphasis added).

123 See Yvette Joy Liebesman and Benjamin Wilson, 'Trademark Exhaustion and the Internet of Resold Things' in Irene Calboli and Edward Lee (eds.), *Research Handbook on Intellectual Property Exhaustion and Parallel Imports* (Edward Elgar 2016) 439 ('Protecting the resale market increases consumer choice and spurs mark owners to innovate and bring new and improved products to the market.').

124 ibid 431.

125 *Nike Inc.* (n 58).

126 Case 1:22-cv-00983 <https://www.documentcloud.org/documents/21565635-nike-v-stockx> accessed 15th January 2023.

127 Kushman (n 60).

128 Cramer and O'Rourke (n 45). See also Brennan (n 55): 'StockX further answered that its NFTs do not violate any of Nike's rights for the following three reasons: (i) StockX's re-sale of genuine Nike products is protected by the first sale doctrine; (ii) StockX's use of images and names of genuine Nike products tied to "Vault NFTs" constitutes nominative fair use; and (iii) consumers are unlikely to be confused by StockX's Vault NFTs'.

129 Murray (n 3).

on a blockchain) requires no such permissions."[130]

41 Thus, according to this approach, the applicability of the two defences will depend on whether an NFT is characterized as a 'product' or 'receipt'. However, as already highlighted, the deep-rooted problem of the characterization of NFTs is wrapped in controversy and is manifested by the definition muddle of NFTs. Apart from the bizarre nature of NFTs, their incredible commercial value also adds to the complexity of the problem. For example, it has been commented that an 'NFT is the actual thing being purchased, and it is the valuable item in an ownership and "ownership" sense'.[131] Hence, 'the NFT obviously is separate in value as indicated by the pricing of the sneakers alone vs. the pricing of the Vault NFT, and the NFT is a different item because you cannot possess both the NFT and the sneakers'.[132] Specifically, with regard to the NIKE scenario, It has been pointed out that 'this price disparity suggests that, at least in the mind of some consumers (....) there was confusion about whether Vault NFTs were merely a means of authenticating and demonstrating ownership of physical sneakers or were a unique asset with a value distinct from their physical asset counterparts'[133]. Notably, '[i] f Vault NFTs are determined to be separate assets, then StockX's argument that it is protected against Nike's claims of trademark infringement by the first sale doctrine becomes more tenuous'.[134] Although when one looks at the NFT architecture an NFT hardly qualifies as an independent asset, when one considers its extremely high commercial value, designating an NFT as a mere receipt or ticket would seem to be a misnomer.

42 In any event, treating this question as simply a problem of nomenclature is an oversimplification of the issue. Finding a proper definition alone will not be dispositive of this problem, as one also needs to look into more intricate issues such as whether the legitimate interests of the owner of the trademark warrant the invoking of the doctrine of exhaustion or whether the criteria used to evaluate nominative fair use justify the use of the principle. However, where the Sri Lankan legal landscape is concerned, the problem appears to be even more complicated. The law relating to trademark exhaustion in Sri Lanka is laid down in Section 122 (b) of the IP Act. The said Section states as follows:

Section 122 -The registration of the mark shall not confer on its registered owner the right to preclude third parties –

(b) from using the mark in relation to goods lawfully manufactured, imported, offered for sale, sold, used or stocked in Sri Lanka under that mark, provided that such goods have not undergone any change.

43 Unfortunately, it is not at all clear from this provision whether this Section recognizes national or international exhaustion. In the absence of clear statutory language, the term 'lawfully imported goods' can even encompass goods lawfully purchased by third parties from markets outside the national borders. Based on this interpretation, the argument can be advanced that Section 122 (b) of the IP Act does recognize 'international exhaustion'. Yet, as the term 'lawfully imported' is not defined in the IP Act and there is an absolute dearth of judicial precedents delineating its scope, this interpretation is open to debate.[135] Thus, the controversy stemming from this ambiguous statutory provision can raise problems where the product which is authenticated by the NFT is in fact a parallel import. In such a case, the creator of the NFT cannot legitimately rely on the principle of exhaustion if Section 122 (b) does not recognize international exhaustion. Conversely, however, if Section 122 (b) is construed as allowing parallel imports then the NFT owner can rely on the principle of exhaustion in such a situation, provided other legal impediments are successfully removed. By way of contrast, the particular scheme of exhaustion embraced by certain other jurisdictions has sometimes been judicially or statutorily affirmed creating legal certainty. In the EU for example, the courts have confirmed the applicability of the principle of regional exhaustion.[136] Even with regard

130 Cramer and O'Rourke (n 45). See also Andrew C. Michaels, 'NFT Litigation is Raising Novel Trademark Questions, Law' [2022] Law360 <https://www.law360.com/articles/1521677/nft-litigation-is-raising-novel-trademark-questions> accessed 24th December 2022. (The author expresses a similar idea when he raises the question: 'Does buying a trademarked item give the buyer the right to create NFTs depicting the item? The answer may depend on whether the NFTs are considered a separate — or materially different — product, or whether the NFTs are — as StockX claims — merely a technological means to enable secondary trading and track ownership of a physical item').

131 Murray (n 3).

132 ibid.

133 Kushman (n 60).

134 ibid.

135 For a discussion on the principle of exhaustion, see Karunaratna, (n 70) 262.

136 See Irene Calboli, 'Trademark Exhaustion in the European Union: Community-Wide Or International? The Saga Continues' (2002) 6 Marquette Intellectual Property Law Review 84. ('At least for the time being, the ECJ has made clear that EEA-wide exhaustion is the only applicable criterion within the internal market, and national rules

to the USA, it has been acknowledged that it 'follows a system of international exhaustion with respect to trademark law and trademarked products'.[137]

44 It is appropriate at this juncture to also mention the anomaly which pervades the nominative fair use defence paradigm in Sri Lanka. There is no explicit recognition of the nominative fair use defence in the IP Act. However, other than Section 122 (b), the only provision which contemplates a diminution of the legal rights granted to the registered trademark owner is Section 122 (a) which provides as follows:

"The registration of the mark shall not confer on its registered owner the right to preclude third parties – (a) from using their bona fide names, addresses, pseudonyms, a geographical name, or exact indications concerning the kind, quality, quantity, destination, value, place of origin or time of production or of supply of *their goods and services*, in so far as such use is confined to the purposes of mere identification or information and cannot mislead the public as to the source of the goods or services"[138]

45 But a cursory reading of this provision reveals that it seeks to curtail the rights of the trademark owner on the basis of descriptive fair use rather than nominative fair use. It protects third parties who use registered trademarks for the purpose of designating the kind, quality, quantity, destination, value, place of origin or time of production or of supply *of their goods and services*. This clearly juxtaposes with the nominative fair use defence which protects third parties who use the registered trademarks to reference the *trademark owner's products or services*.[139] If the courts in comparative jurisdictions display a receptive mindset towards the defence of nominative fair use in NFTs-related matters, the non-recognition of the defence both in terms of the IP Act and judicial precedents in Sri Lanka can be extremely prejudicial to the owners of NFTs. Contrastingly, in the USA, under the law of trademark infringement nominative fair use is judicially created, whereas, under dilution law, the defense is statutory, established by the Trademark Dilution Reform Act[140] of 2005.[141] In a similar vein, the referential use defence which is the EU counterpart of the nominative fair use doctrine, is statutorily embedded. It is recognized in Article 14 (1) (c) of the EUTMR No. 2017/1001.[142]

IV. Application of statutory remedies to NFTs.

46 Another grim issue is the enforcement of injunctions and certain other remedies against the creators of infringing NFTs. For example, a court order demanding the creator of the infringing NFT to remove from commerce or delete the impugned NFT could prove very tricky. In *Juventus F.C. v Blockeras s.r.l*,[143] the Rome Court of First Instance issued an injunction ordering Blockeras inter alia to 'withdraw from the market and remove from every website and/or from every page of a website directly and/or indirectly controlled by the same on which such products are offered for sale and/or advertised, the NFTs (non-fungible tokens) and the digital contents associated therewith or products in general covered by the injunction'.[144] However, the infringing NFTs still appear on the relevant blockchain.

47 The reason is that 'none of the data in the blockchain can ever be deleted -That is by design. Therefore, all [the] data, once exposed cannot be deleted or changed.'[145] This quality of NFTs is attributable to the so-called immutability of the blockchain technology that underlies NFTs.[146] Nevertheless, several other

providing other exhaustion regimes are in contrast with Article 7(1) of the Trademark Directive').

137 Irene Calboli, 'The (avoidable) effects of territorially different approaches to trademark and copyright exhaustion' in Irene Calboli and Edward Lee (eds), *Trademark Protection and Territoriality Challenges in a Global Economy* (Edward Elgar 2014) 158.

138 Section 122 (a) of the IP Act (emphasis added).

139 See Mary Minow and Tomas A. Lipinski, *The Library's Legal Answer Book* (American Library Association 2003) 98.

140 15 U.S.C. § 1125(c) (3).

141 Samuel M. Duncan, 'Protecting Nominative Fair Use, Parody, and Other Speech-Interests by Reforming the Inconsistent Exemptions from Trademark Liability' (2010) 44 University of Michigan Journal of Law Reform 219, 227.

142 Article 14 (1) (c) states that 'the EU trade mark for the purpose of identifying or referring to goods or services as those of the proprietor of that trade mark, in particular, where the use of that trade mark is necessary to indicate the intended purpose of a product or service, in particular as accessories or spare parts'.

143 *Juventus F.C.* (n 61)

144 Trevisan and Cuonzo, 'Unofficial Translation' https://www.trevisancuonzo.com/static/upload/juv/juventus-nft-order---en.pdf accessed 10th June 2023.

145 Chris Duffey, *Decoding the Metaverse: Expand Your Business Using Web3* (Kogan Page 2023) 130

146 See Dwayne Anderson, *Non Fungible Tokens NFTs* (Estalontech 2021)11

means are available to the NFT owner to prevent its further circulation. Thus, the view has been expressed that '[e]ven though you can't delete an NFT, you can technically "burn" an NFT. Burning an NFT sends the NFT to a null or "burn" address. While the NFT still exists on the blockchain, it is effectively out of circulation and distribution'.[147]

48 In *Nike Inc. v. StockX LLC*[148], Nike has *inter alia* sought an order that StockX be required to deliver to Nike for destruction any and all Vault NFTs bearing Nike's marks.[149] If the court actually grants the relief requested by Nike, the next question is how they can effectuate the destruction of the infringing NFTs. The idea has in fact been expressed that 'the most practical thing for Nike to do would be to send the NFTs to a so-called burner wallet. This wouldn't destroy them but still achieve the same purpose.'[150] This has in fact been compared 'to a luxury brand seizing knock-off goods and then sticking them in a secure warehouse and throwing away the key'.[151]

49 Where the Sri Lankan trademark legal regime is concerned, the IP Act offers a blend of criminal and civil remedies to an owner of a trademark. However, several provisions of the IP Act dealing with criminal and civil remedies available to a trademark owner make reference to the term 'destroy'. For instance, Section 170 (3) (a) of the IP Act which deals with civil remedies for infringement of intellectual property rights recognized under the IP Act states that:

"The court shall have the power to order—

(ii) the infringing goods to be disposed of outside the channels of commerce or *to be destroyed* without the payment of any compensation";

50 Similarly, Section 186 (5) of the IP Act which provides for criminal sanctions in relation to 'other offences as to marks and trade descriptions' stipulates that:

"The Magistrate may, whether the alleged offender is convicted or not, order that every chattel, article, instrument or thing by means of or in relation to which the offence has or might have been committed shall be *destroyed* or declared forfeit to the State or otherwise dealt with as he may think fit."

51 If the local courts encounter NFTs-related trademark infringement cases in the future, it remains to be seen if the courts will leverage their creativity and interpret the word 'destroy' to include 'burning' in the context of infringing NFTs.

C. Conclusion:

52 The above analysis reveals several pitfalls in the current trademark legal regime in Sri Lanka with regard to NFTs-related trademark issues. Although it may still be premature for the Sri Lankan legal regime on trademarks to embrace fully blown, stand-alone legal provisions relating to NFTs, certain improvements can be made to the existing law with a view to enhancing its ability to tackle NFTs . For instance, some objective parameters can be laid down to establish its character, including, whether an NFT is to be treated as a cryptographic asset, a digital certificate or a unique unit of data, when it authenticates a virtual good, a physical good and digital art respectively, since adopting a bright-line definition for NFTs may be a challenging task. With regard to the gaps that exist in the classification vis-à-vis the categorization of NFTs-related goods or services, some guidelines can be issued by the Minister using the powers vested in him by the IP Act itself. Judiciary should be enlightened on the inappropriateness of faithfully adhering to the traditional judge-made criteria for assessing similarity between goods and services, where NFTs are concerned. It is also high time that Sri Lankan trademark law regime resolves the puzzling issue of whether it recognizes international or national exhaustion. At the same time, it is prudent to statutorily recognize the defence of nominative/referential fair use. The last two suggestions will have an overarching effect on the entire trademark ecosystem in Sri Lanka and specifically on the trademark defences legal landscape. Although NFTs-related trademark disputes have not yet been reported in Sri Lanka, one cannot guarantee that there will be no such disputes in Sri Lanka in the near

147 'How do you delete an NFT? What does it mean to burn an NFT and how to do it through Etherscan' (*Saminacodes* 30th June 2022) <https://samina.dev/how-do-you-delete-an-nft> accessed 5th February 2023. See also 'What Is Burning An NFT? A Complete Guide And Explanation'(*NFTexplained.info* 2023) <https://nftexplained.info/what-is-burning-an-nft-a-complete-guide-and-explanation/ > accessed 23rd December 2023: (An NFT can't be 'deleted', however it can be 'burned'. Once an NFT is minted or uploaded to the blockchain, it is considered immutable; this means it will exist on the blockchain forever. An NFT can be 'burned' by being sent to an inaccessible address, as it is removed from circulation.)

148 *Nike Inc.* (n 58).

149 Case 1:22-cv-00983 <https://www.documentcloud.org/documents/21565635-nike-v-stockx> accessed 15th January 2023.

150 Jeff John Roberts, Nike Wants to 'Destroy' Unauthorized NFTs—How Will That Work? (*Decrypt* 1st April 2022) <https://decrypt.co/96456/nike-destroy-unauthorized-nfts-how-will-that-work> accessed 12th January 2023.

151 ibid.

future. Therefore, this paper advocates a proactive approach to NFTs-related legal issues in Sri Lanka, taking into consideration the developments in the USA and EU.

Hybrid Speech Governance
New Approaches to govern Social Media Platforms under the European Digital Services Act? *

by **Wolfgang Schulz & Christian Ollig** **

Abstract: The normative development of communication rules on online platforms puts traditional notions of rulemaking and rule application in trouble. The overlap, interdependence, and inseparability of private and public communication rules on social media platforms should therefore be analyzed under the lens of a specific category: hybrid speech governance. This perspective can help to find appropriate approaches to contain private power without simply transferring state-centric concepts unchanged to platform operators. This applies to questions of the basis for validity of communication rules, rule of law requirements, and fundamental rights obligations. The EU's Digital Services Act (DSA) adopts this perspective of hybrid speech governance and thus finds initial legislative answers to the questions raised. Art. 14 DSA is noteworthy in that regard, but it is only the beginning of the story. Academia, practice, and jurisprudence will have to flesh out the DSA's approaches to hybrid speech governance in detail. In particular, the current parallel debate in the U.S. on the question of the constitutional obligations of social media platforms could benefit from this European approach as a source of inspiration–it does not seem out of the question that the Supreme Court will add a balancing model to the current dichotomy of state action doctrine. Only such a balancing model can do justice to the phenomenon of hybrid speech governance, for platform governance and beyond.

Keywords: Hybrid Speech Governance; European Platform Governance; Digital Services Act; Horizontal Effect of Fundamental Rights; State Action Doctrine

Recommended citation: Wolfgang Schulz and Christian Ollig, Hybrid Speech Governance
New Approaches to Govern Social media Platforms under the European Digital Services Act?, 14 (2023) JIPITEC 560 para 1.

A. Introduction

> *Yesterday was my last day at Twitter: the entire Human Rights team has been cut from the company. I am enormously proud of the work we did to implement the UN Guiding Principles on Business & Human Rights (...).*

1 With these words, Shannon Raj Singh, Former Human Rights Council at Twitter, now "X", commented on her resignation after Elon Musk's takeover of the platform.[3] Her comment sheds some

* This paper is based on a talk we gave at the Information Society Project, Yale Law School, on October 25, 2022. Thanks to Prof. Dr. Robert C. Post, Dr. Tobias Mast, Prof. Dr. Matthias C. Kettemann, who provided their great help in finalizing the article. Errors are entirely our own.

** Prof. Dr. Wolfgang Schulz is Professor of Law, University of Hamburg, and Director of the Leibniz Institute for Media Research | Hans Bredow Institute and of the Humboldt Institute for Internet and Society and UNESCO Chair for Freedom of Information and Communication. Christian Ollig, LL.M. (College of Europe), Maître en Droit (Cergy-Paris) is PhD Candidate at the University of Hamburg, Junior Researcher at the Leibniz Institute for Media Research | Hans Bredow Institute and Associated Researcher at the Humboldt Institute for Internet and Society.

3 Shannon Raj Singh on Twitter: "Yesterday was my last day

light on how platform operators structure the rules in their communication spaces. On the one hand, they shape online communication according to their own private rules. On the other, these private communication rules are increasingly influenced by standards set by public actors—such as the UN Guiding Principles on Business and Human Rights. In short, limits to free speech on online platforms result from two different sets of rules, namely private rules and state-set rules, interacting with each other.

2 The fact that not only entrepreneurial autonomy but also government rules have an impact on a product is nothing new. State actors regularly set rules to prevent the dangers posed by the production, distribution or consumption of a product—and this influences our product experience.[4] If coffeeshops are required by government regulations to warn us on our coffee mug that its content is potentially hot, then corporate compliance impacts product design. Nothing else is fundamentally true for the product of social media platforms: How we can communicate publicly with each other online is the result of private and public rules. Here, however, a special feature arises. Private rules and public rules are inextricably linked. The latter are not mere external requirements, but the resulting body of communication rules becomes the product itself.[5] In that sense, private and public rules are interconnected, they overlap, and are mutually dependent.

3 This phenomenon of overlapping and intertwining public and private rules poses challenges to traditional legal concepts. In particular, legal thinking in liberal democracies such as the EU and the U.S. has been characterized by the binary distinction between private and public rules.[6] Such a binary perspective is actor-centric. It focuses primarily on *who* sets rules. If the state sets law, different requirements have to be considered than if private actors set rules. Yet, such binary legal thinking fails to adequately map –and understand- what the regulatory structure of social media platforms actually is. We argue in this paper that, with a view to ordering in digital communication spaces, the focus should move away from the actors of rules to the actual emergence of communication rules and the corresponding regulatory structures. That does not mean that concepts like the state actor doctrine become obsolete, but that legal thinking can profit from changing perspectives. This new perspective consequently takes a look at the overlapping and coalescing of private and public communication rules on social media platforms. This is what we will call "hybrid speech governance".

4 In the non-legal analysis of norms, switching between these perspectives is already common. A phase that looked at the possibilities and limits of state control was followed by one that examined the normative structures that result from the setting of norms by different actors.[7] This change of perspective can easily be addressed by theories of law, such as Teubner's "reflexive law".[8] For legal practice, however, the actor-centric perspective is essential, as will be seen, for example, in the link to fundamental rights. But legal analysis can profit from looking at the structural level and is forced to do so to adequately deal with phenomena such as hybrid speech governance.

5 This all begs the fundamental question of how hybrid speech governance can fit into a legal system based on the binary distinction between state and private rules. It seems that the DSA recently passed by the EU[9] provides an initial legislative answer to this question. Indeed, the DSA takes up the phenomenon of hybrid speech governance in its Article 14. This prompts us to take a closer look at the hybrid normative field on social media platforms. We will first trace the origins of hybrid speech governance (B). Second, we will classify hybrid speech governance as a category of analysis (C). Third, we will specify what constitutional challenges hybrid speech governance raises (D). Fourth, we will shed light on how the DSA addresses these challenges (E). Fifth, against the background of the insights thus gained, we will take a look at parallel issues in the U.S. legal system (F).

6 The main goal of this paper is to argue for

[@ShannonRSingh] <https://twitter.com/ShannonRSingh/status/1588591603622772736> accessed 15 November 2022.

4 Wolfgang Schulz, 'Changing the Normative Order of Social Media from Within: Supervisory Bodies' in Edoardo Celeste, Amélie Heldt and Clara Iglesias Keller (eds), *Constitutionalising Social Media* (Hart Publishing 2022) 238.

5 *Schulz (n 4) 239.*

6 Matthias Goldmann, 'A Matter of Perspective: Global Governance and the Distinction between Public and Private Authority (and Not Law)' (2016) 5 Global Constitutionalism 48; Giovanni De Gregorio, 'Digital Constitutionalism across the Atlantic' (2022) 11 Global Constitutionalism 297.

7 Beate Kohler-Koch and Berthold Rittberger, 'The Governance Turn in EU Studies Review Article' (2006) 44 Journal of Common Market Studies 27; Stephen J Ball, 'The Governance Turn!' (2009) 24 Journal of Education Policy 537.

8 Gunther Teubner, 'Substantive and Reflexive Elements in Modern Law' (1982) 17 Law & Society Review 239.

9 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC ('Digital Services Act'; '***DSA***')

research specifically on structures of hybrid speech governance. While initial approaches to the general phenomenon of the hybridization of Internet governance can already be found,[10] our work is intended to provide a concrete prelude to more research in relation to hybrid speech governance. However, our thesis does not claim to reach conclusive answers. Here, our essential aim is to determine the phenomenon and specific problem areas of hybrid speech governance. In particular, we would like to highlight EU law as a starting point so as to stimulate the transatlantic dialogue on platform regulation.

B. The Origins of Hybrid Speech Governance

7 Legal regulation is an essential component of ordering on social media platforms.[11] If we look at the actors involved in speech regulation, this can be depicted as a pluralistic triangle of free speech regulation, as Balkin has graphically elaborated[12] (I). If, on the other hand, the focus is to be on the actual regulatory structures on social media platforms, the picture is different (II).

I. From an Actor-Centered Perspective...

8 In his triangular model, Balkin vividly systematizes the relationships between free speech actors in the digital world. On the first side of the triangle are the private communication rules of digital infrastructures (e.g., social media companies), which they impose on speakers.[13] When private parties provide other private parties with a space to communicate, they can autonomously regulate the freedom of speech exercised there as part of their freedom of contract. Thus, digital companies determine what speech is permitted on their platform by way of private ordering.[14] Platform operators regularly lay down such rules in their Terms and Conditions (T&C).[15] In these terms, they

10 From a U.S. perspective, Daphne Keller, 'Who Do You Sue? State and Platform Hybrid Power over Online Speech' (*Stanford PACS*) <https://pacscenter.stanford.edu/publication/who-do-you-sue-state-and-platform-hybrid-power-over-online-speech/> accessed 16 November 2022 has already addressed the intersection and interaction between private and public power on online platforms; Giovanni De Gregorio and Roxana Radu, 'Digital Constitutionalism in the New Era of Internet Governance' (2022) 30 International Journal of Law and Information Technology 68 view the takeover of public functions by private digital companies as a form of hybridization of Internet governance as well; Jean-Marie Chenou and Roxana Radu, 'The "Right to Be Forgotten": Negotiating Public and Private Ordering in the European Union' (2019) 58 Business & Society 74 illustrate how the regulation of search engines is causing the private-public dichotomy to blur. Sometimes self-regulation that comes about with the cooperation of government agencies is also called 'hybrid regulation', Wolfgang Hoffmann-Riem, 'Selbstregelung, Selbstregulierung und regulierte Selbstregulierung im digitalen Kontext' in Michael Fehling and Utz Schliesky (eds), *Neue Macht- und Verantwortungsstrukturen in der digitalen Welt* (Nomos Verlagsgesellschaft mbH & Co KG 2016) 41 et seq.

Otherwise, previous research on platform regulation has focused less on substantive hybrid communication rule structures and more on hybrid institutions, Kate Klonick, 'The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression' (2020) Vol. 129 Yale Law Journal 2418; Martin Fertmann and others, 'Hybrid Institutions for Disinformation Governance: Between Imaginative and Imaginary' (*Internet Policy Review*) <https://policyreview.info/articles/news/hybrid-institutions-disinformation-governance-between-imaginative-and-imaginary/1669> accessed 16 November 2022; Thomas Kadri and Kate Klonick, 'Facebook v. Sullivan: Public Figures and Newsworthiness in Online Speech' (2019) 93 Southern California Law Review 37; *Event: Surveying the Hybrid Speech Governance Landscape* (Directed by R Street Institute, 2022) <https://www.youtube.com/watch?v=0O2SgDd3S3k> accessed 16 November 2022; Schulz (n 4).

11 For a comprehensive analysis of the complex regulatory structures on the Internet, Matthias C Kettemann, *The Normative Order of the Internet* (Oxford University Press 2020).

12 Jack Balkin, 'Free Speech Is a Triangle' (2018) Vol. 118 Columbia Law Review 2011; Jack Balkin, 'Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation' (2018) 51 UC Davis Law Review 1151, 1186 et seqq

13 Balkin, 'Free Speech Is a Triangle' (n 12) 2021 et seqq.

14 See also Kate Klonick, 'The New Governors: The People, Rules, and Processes Governing Online Speech' (2018) 131 Harvard Law Review 1599; Heike Schweitzer, 'Digitale Plattformen Als Private Gesetzgeber: Ein Perspektivwechsel Für Die Europäische „Plattform-Regulierung"' (2019) Zeitschrift für Europäisches Privatrecht 1; Ulrich Dolata, 'Plattform-Regulierung. Koordination von Märkten und Kuratierung von Sozialität im Internet' (2019) 29 Berliner Journal für Soziologie 179; Matthias C Kettemann and Wolfgang Schulz, 'Setting Rules for 2.7 Billion: A (First) Look into Facebook's Norm-Making System; Results of a Pilot Study' (2020) Working Papers of the Hans-Bredow-Institut | Works in Progress.

15 Luca Belli and Jamila Venturini, 'Private Ordering and

decide what may and may not be said on their platforms. In many cases, these rules are stricter than what the state allows. In other words, this is "governance *by* platforms"[16].

9 On the second side of the triangle are rules by actors with public authority defining limits to free speech ("old-school speech regulation"):[17] Legislators shape the communication space through public rules, courts interpret these rules, and administrative authorities enforce them. Of course, even before the age of digital communication, this public body of rules consisted of criminal statutes, civil liability laws, and administrative orders.[18] Such rules directly define the permitted scope of free speech.

10 On the third side of the triangle, in the age of digitization old-school speech regulation is increasingly being joined by "new-school speech regulation".[19] This means that state actors are addressing the operators of digital infrastructures. Accordingly, the state sets rules that impose obligations on intermediaries.[20] Consequently, the state, in cooperation with private parties, only indirectly regulates free speech in these private infrastructures. One example is the German Network Enforcement Act[21], which will soon be replaced by the DSA. In other words, this is "governance *of* platforms."[22]

11 The three sides of the triangle may be presented as follows:[23]

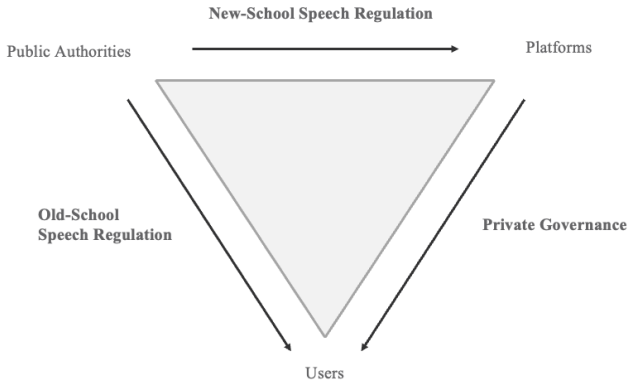


Figure 1: Balkin's Free Speech is a Triangle Model

12 This model is able to systematize who sets communication rules in the digital space: public authorities vis-à-vis platforms and speakers, platforms vis-à-vis speakers. This is a helpful perspective. It illustrates the authors and legal relationships in digital communication spaces. In particular, it can be used to identify dangers within the individual legal relationships,[24] in order to design suitable government regulation.[25]

---

the Rise of Terms of Service as Cyber-Regulation' (2016) 5 Internet Policy Review <https://policyreview.info/node/441> accessed 16 November 2022; Edoardo Celeste, 'Terms of Service and Bills of Rights: New Mechanisms of Constitutionalisation in the Social Media Environment?' (2019) 33 International Review of Law, Computers & Technology 122.

16 Tarleton Gillespie, 'Regulation of and by Platforms' in Jean Burgess, Alice Marwick and Thomas Poell, *The SAGE Handbook of Social Media* (SAGE Publications Ltd 2018); Tarleton Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media* (Yale University Press 2018).

17 Balkin, 'Free Speech Is a Triangle' (n 12) 2015; see also Jack Balkin, 'Old-School/New-School Speech Regulation' (2014) 127 Harvard Law Review 2296.

18 Cf. Balkin, 'Old-School/New-School Speech Regulation' (n 17) 2298.

19 Balkin, 'Free Speech Is a Triangle' (n 12) 2015 et seqq.; see also Balkin, 'Old-School/New-School Speech Regulation' (n 17).

20 On the trend of delegation of law enforcement by public authorities to private entities see Jody Freeman and Martha Minow (eds), *Government by Contract: Outsourcing and American Democracy* (Harvard University Press 2009); De Gregorio and Radu (n 10) 78.

21 Balkin, 'Free Speech Is a Triangle' (n 12) 2030 et seqq.

22 Gillespie (n 16).

23 Cf. Balkin, 'Free Speech Is a Triangle' (n 12) 2014. The presentation here is simplified and modified from the original model for presentation purposes. Our presentation focuses on constellations on social media platforms. In particular, voice, protest and exit by users vis-à-vis public authorities and digital infrastructures have been omitted here.

24 Such as collateral censorship and digital prior restraint in relation to new-school speech regulation, and arbitrary private bureaucracy without due process and transparency in relation to private governance, Balkin, 'Free Speech Is a Triangle' (n 12) 2016 et seqq.

25 Balkin, 'Free Speech Is a Triangle' (n 12) 2032 et seqq.; Jack Balkin, 'How to Regulate (and Not Regulate) Social Media' [2019] SSRN Electronic Journal <https://www.ssrn.com/abstract=3484114> accessed 16 November 2022.

II. … to a Governance-Centered Perspective

13 We argue that in addition to this actor-centered perspective, a governance-centered approach is necessary. If we are interested in the rules that actually govern free speech on a platform, it is not enough to focus only on the authors of the rules. Rather, we need to consider the connections between private and state rules of communication. State and private rules of communication interact. This can be illustrated by another focus on Balkin's model:

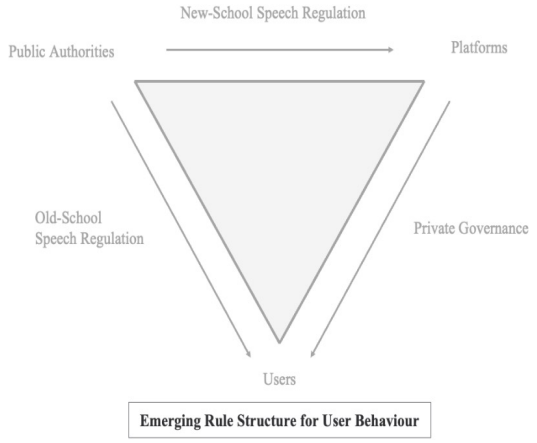


Figure 2: Hybrid Speech Governance Model

14 The focus of hybrid speech governance is not on the corners and sides of the triangle, but on its bottom. Here, the private and public ordering of free speech overlap in their outcome. To this extent, the actual outcome of the regulatory structure on social media platforms is a hybrid form of private and state rules, represented by the emerging pattern at the bottom of the illustration.

15 Those links between private and public communication rules have two central foci. On the one hand, private platforms are (increasingly) deciding voluntarily to comply with regulations that were originally directed only at public authorities. Private governance by platform operators is thus oriented toward public values. In other words, platforms are voluntarily integrating public ordering requirements into their private ordering (1). On the other hand, public authorities are (increasingly) obliging private platform operators to take into account public values that were originally only directed at public authorities. Therefore, traditional public ordering requirements are becoming mandatory for the private ordering of platform operators (2).

1. The Approximation of Private Ordering to Public Ordering Requirements

16 Influenced by the U.S. approach,[26] "digital liberalism" prevailed in the EU at the beginning of the 2000s.[27] European integration was primarily market-driven. Safe harbor regulations were intended to promote the free development of digital platform operators.[28] The entrepreneurial freedom of platform operators was paramount in the EU. This liberal environment provided the original impetus for the extensive private ordering of platforms.[29] However, it is becoming apparent that social media companies are more and more likely to voluntarily move closer to the logic of classic public ordering in their

26 For an extensive analysis of this approach in the U.S. see Elettra Bietti, 'A Genealogy of Digital Platform Regulation' (2023) Georgetown Law Technology Review <https://papers.ssrn.com/abstract=3859487> accessed 17 November 2022; see also Klonick (n 14) 1603 et seqq.

27 Giovanni De Gregorio, 'The Rise of Digital Constitutionalism in the European Union' (2021) 19 International Journal of Constitutional Law 41, 43 et seqq.; De Gregorio (n 6) 299; Amélie P Heldt, 'EU Digital Services Act: The White Hope of Intermediary Regulation' in Terry Flew and Fiona R Martin (eds), *Digital Platform Regulation* (Springer International Publishing 2022) 70.

28 For online intermediaries, a general exemption from liability for user-generated content was introduced in Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, particularly electronic commerce, in the Internal Market ('Directive on electronic commerce'; '***E-Commerce-Directive***'). Accordingly, intermediaries are not liable if, after becoming aware of the illegality of the stored information or content, they immediately remove it or block access to the illegal information or content (Article 14). Furthermore, they have no general obligation to monitor content (Article 15). Section 230 of the U.S. Communications Decency Act served as a model in this regard.

29 Robert Gorwa, 'The Platform Governance Triangle: Conceptualising the Informal Regulation of Online Content' (2019) 8 Internet Policy Review <https://policyreview.info/articles/analysis/platform-governance-triangle-conceptualising-informal-regulation-online-content> accessed 16 November 2022; Michael Denga, 'Plattformregulierung Durch Europäische Werte: Zur Bindung von Meinungsplattformen an EU-Grundrechte' (2021) Europarecht 569, 575 et seqq.; De Gregorio (n 6) 301 et seq. Others already saw limits to private rule-making by platforms in the E-Commerce-Directive, see Sophie Stalla-Bourdillon and Robert Thorburn, 'The Scandal of Intermediary: Acknowledging the Both/and Dispensation for Regulating Hybrid Actors' in Bilyana Petkova and Tuomas Ojanen, *Fundamental Rights Protection Online* (Edward Elgar Publishing 2020).

rulemaking.

17 Indeed, the rules of social media companies have become differentiated in recent years. While there were initially a few general house rules, today there are various interlinked normative texts that frequently change. Not only do the norms affect more and more subject areas, but regular hierarchies of norms can also emerge. These include abstract principles or values that would guide all the company's actions as well as concrete regulations that implement these principles or values.[30] When it comes to content moderation decisions, norms usually refer to the interests of others, the community, or the platform provider that may be affected by content or certain behavior.[31]

18 Not only does the process of making and changing these rules correspond to public ordering in its complexity,[32] platform operators also decide to integrate public values from democratically legitimized standards into their content moderation. Admittedly, insights into the actual sources of inspiration in rulemaking by platforms are quite limited.[33] Nonetheless, initial examples make it clear that platform operators are using the standards of public authorities as a guide for their private communication rules. For example, the normative content of communication rules is shaped by the U.S. legal tradition of the First Amendment.[34] In particular, regional characteristics of legal systems can also influence platform rules.[35] Platform operators are also implementing international human rights standards in their rules,[36] as shown not least by the tweet from the former Human Rights Council on Twitter that introduces this paper.

19 Social media platforms are increasingly basing their private ordering on standards that correspond to public ordering requirements. The more platform operators voluntarily implement such requirements, the more private ordering becomes interwoven with public values independent of state laws and public regulation. From the perspective of the platform users, this results in a hybrid set of rules consisting of private rules and public rules.

2. The Imposition of Public Ordering Requirements on Private Ordering

20 The second thrust in the emergence of hybrid speech governance stems from mandatory requirements by public authorities. In view of the growing importance of digital platforms, such requirements are ever more superimposed on private ordering.[37] In this way, they are shaping the regulatory structure in private online communication spaces.

21 This shaping of private ordering initially took place in Europe only through fragmentary specifications. European lawmakers began to fill out their mosaic of platform regulation—in the tailwind of the European Court of Justice's case law, which increasingly recognized the importance of online platforms for

30 Cf. Klonick (n 14) 1630 et seqq. who makes clear how general standards have evolved into increasingly concrete rules at YouTube and Facebook.

31 Cf. Evelyn Douek, 'Governing Online Speech: From "Posts-As-Trumps" to Proportionality and Probability' (2020) Vol. 121 Columbia Law Review 759, 763"Content moderation is a question of systemic balancing: Rules are written to encompass multiple interests, not just individual speech rights (...)".

32 Hannah Bloch-Wehba, 'Global Platform Governance: Private Power in the Shadow of the State' (2019) 72 SMU Law Review 27, 29; Schweitzer (n 14). On the proceduralization of private ordering at Facebook see also Kettemann and Schulz (n 14) 28 et seqq.; cf. also Thiago Dias Oliva, 'Content Moderation Technologies: Applying Human Rights Standards to Protect Freedom of Expression' (2020) 20 Human Rights Law Review 607, 157 et seq.

33 Ruby O'Kane, 'Meta's Private Speech Governance and the Role of the Oversight Board: Lessons from the Board's First Decisions' (2021) 25 Stanford Technology Law Review 167, 180.

34 Klonick (n 14) 1621; Kettemann and Schulz (n 14) 31.

35 Concerning Facebook see Chinmayi Arun, 'Facebook's Faces' (2021) Vol. 135 Harvard Law Review 236, 240; see also Alexendre De Streel and others, *Online Platforms' Moderation of Illegal Content Online: Laws, Practices and Options for Reform* (Publications Office 2020).

36 In the Global Network Initiative, for example, numerous platforms have committed themselves to observing principles based on international standards, in particular the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights; see also Gorwa (n 29) 11 et seq. For a comprehensive analysis of the voluntary implementation of International Human Rights Law in content moderation see Brenda Dvoskin, 'Expert Governance of Online Speech' <https://papers.ssrn.com/abstract=4175035> accessed 17 November 2022.

37 De Gregorio and Radu (n 10) 79 summarize this as follows: "The hybridization trend stems from state ambitions of tight control via private intermediaries in illiberal regimes, on the one hand, and the transfer of public functions to unregulated digital platforms in liberal regimes, on the other".

the exercise of users' fundamental rights.[38] The EU set the first limits on private communication rules for platform operators in order to protect copyrights online[39] or to prevent the online dissemination of terrorist content[40].[41] The EU also built up pressure on platform operators via numerous codes of conduct to shape their private communication rules in relation to certain dangers, such as those relating to hate speech or disinformation.[42] At the member state level, too, increasingly dense government regulation has loomed over the private ordering of social media companies. In Germany, for example, the Network Enforcement Act stipulates that social networking sites must delete illegal content as a result of user complaints;[43] furthermore, under an amendment to German media law, intermediaries may not discriminate against journalistic-editorial content;[44] the German Federal Court of Justice has also ruled that those sites may face constitutional obligations in their private communication rules[45,46]. In other EU member states, too, public ordering requirements have increasingly shaped the private ordering of platforms.[47]

22 Beyond these initially fragmentary requirements, the EU introduced comprehensive obligations for all intermediaries with its DSA in October 2022. The DSA aims to create a safe digital space: It intends to limit the distribution of illegal content; at the same time, the fundamental rights of users as enshrined in the Charter shall be protected (Article 1(1) DSA). Through detailed liability and due diligence provisions, private ordering by platform operators is shaped by this act.[48] In particular, the European legislature recognizes the platforms' T&C and codes as the basis for private governance.[49] This is the regulatory gateway through which the EU integrates public ordering requirements into private ordering by platforms.[50]

38 See CJEU, Judgement of 24 Nov 2011, Case C-70/10, Scarlet; CJEU, Judgement of 16 Feb 2012, Case C-360/10, Netlog. *See* De Gregorio, *supra* note 25 at 51–53.

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

40 Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online.

41 De Gregorio (n 27) 59 et seqq.

42 Although they are legally non-binding instruments, codes of conduct can have a *de facto* binding effect through pressure from governments, Keller (n 10) 6 et seq.; Fertmann and others (n 10); Gorwa (n 29) 13 et seq. This regulatory model is also taken up by the DSA in its Articles 45-47.

43 Section 3(2) No. 2, 3 German Network Enforcement Act of 1 Sep, 2017 (BGBl. I p. 3352), as last amended by Article 3 of the Act of July 21, 2022 (BGBl. I p. 1182)

44 Section 94 German Media State Treaty as amended by the Second Interstate Treaty Amending Interstate Treaties under Media Law (Second Interstate Treaty Amending Media Law) of 27 Dec, 2021 in force since Jun 30, 2022.

45 German Federal Supreme Court, Judgements of 29 Jul 2021, III ZR 179/20 and ZR 192/20; see also Matthias C Kettemann and Torben Klausa, 'Regulating Online Speech: Ze German Way' (*Lawfare*, 20 September 2021) <https://www.lawfareblog.com/regulating-online-speech-ze-german-way> accessed 18 November 2022; Matthias C Kettemann and Anna Sophia Tiedeke, 'Back Up: Can Users Sue Platforms to Reinstate Deleted Content?' (2020) 9 Internet Policy Review 1. For further examples of rulings in other countries, see Daphne Keller, 'The EU's new Digital Services Act and the Rest of the World' (2022) Verfassungsblog <https://verfassungsblog.de/dsa-rest-of-world/> accessed 2 August 2023.

46 In general, on the question of how T&C law is evolving into regulatory law in Germany Tobias Mast, 'AGB-Recht Als Regulierungsrecht' (2023) 78 JuristenZeitung (JZ) 287.

47 For example, in Austria the Federal Act on Measures for the Protection of Users on Communication Platforms, Federal Law Gazette I No. 151/2020 or in France the Law No. 2020-766 of June 24, 2020 to fight against hateful content on the internet, which was yet declared unconstitutional in large parts.

48 Cf. Giancarlo Frosio, 'Platform Responsibility in the Digital Services Act: Constitutionalising, Regulating and Governing Private Ordering' <https://papers.ssrn.com/abstract=4236510> accessed 18 November 2022.

49 See Article 14 and Article 27 DSA.

50 For the embedding of hybrid speech governance in the DSA, see section E.

C. Hybrid Speech Governance: An Analytical Category of its Own

23 Communication rule structure in the digital public sphere is thus developing into a hybrid of private and state rules. The question arises of whether this normative field cannot simply be captured using the conventional categories of governance. We argue that none of these categories can accurately capture the phenomenon of overlapping and intertwined rules (I). Against this background, we want to propose a definition of the distinct category of hybrid speech governance (II).

I. Hybrid Speech Governance as a Traditional Governance Mechanism?

24 The picture of platform governance is classically composed of three mechanisms, namely command-and-control regulation, self-regulation, and co-regulation.[51] The normative field of communication rules on social media platforms contains elements of all these forms of regulation. However, none of these classical forms accurately captures the actual set of over- lapping private and public communication rules:

25 In command-and-control regulation, the state determines commands and prohibitions in order to fulfill the control objectives. The addressees of the rules must follow the latter. The state monitors their compliance. In fact, public authorities increasingly make stipulations in communication spaces on social media platforms that influence the actual regulatory structure, such as rules stipulating that illegal content must be deleted. At the same time, social media companies, as fundamental rights bearers themselves, retain the leeway to autonomously determine their content moderation strategy on the market of digital platforms. Theoretically, of course, it would be conceivable to have a legal system in which public authorities prescribe in detail what communication rules must look like on these platforms.[52] In this case, platform governance would be classic command-and-control regulation. However, such a paternalistic system is alien to liberal democracies.

26 In self-regulation, the state essentially stays out of the process of regulation. It is assumed that the governance goals can be achieved through voluntary, social processes as a rule by the industry itself. As a decisive instrument of platform governance, self-regulation is, in many cases, the basis for shaping the rules of communication for social media companies. As illustrated, platform operators voluntarily submit to standards and thus shape their communication rules.[53] At the same time, this is only one component of the normative inventory of communication rules. These self-regulation measures are often supplemented by mandatory government requirements. Whether the implementation of public requirements is voluntary or serves to ensure compliance with public ordering requirements cannot regularly be traced: The interaction of private and public communication rules does not fully reflect the perspective of self-regulation.

27 It might seem obvious to classify the increasing overlap of private and public rules on social media platforms as a form of co-regulation. Co-regulation can be understood as self-regulation that is fitted into a framework of state law or takes place on a legal basis.[54] Co-regulation pursues the exclusive

51 Robert Gorwa, 'What Is Platform Governance?' (2019) 22 Information, Communication & Society 854, 861 et seqq.; Wolfgang Schulz and Thorsten Held, *Regulierte Selbstregulierung als Form modernen Regierens: Endbericht* (Hans-Bredow-Institut 2002); Gerald Spindler and Christian Thorun, 'Die Rolle Der Ko-Regulierung in Der Informationsgesellschaft Handlungsempfehlung Für Eine Digitale Ordnungspolitik' (2016) MultiMedia und Recht 1, 7 et seqq. who add market control to the picture. On different understandings of Internet governance, see Jeanette Hofmann, Christian Katzenbach and Kirsten Gollatz, 'Between Coordination and Regulation: Finding the Governance in Internet Governance' (2017) 19 New Media & Society 1406.

52 Schulz (n 4) 239.

53 Gorwa (n 51) 862 et seq.; Michael A Cusumano, Annabelle Gawer and David B Yoffie, 'Can Self-Regulation Save Digital Platforms?' (2021) 30 Industrial and Corporate Change 1259, 1271 et seqq.radio and television advertising, and computerized airline reservation systems. We follow this historical discussion with examples of digital platforms in the Internet era that have proven problematic in similar ways, with growing calls for government intervention through sectoral regulation and content controls. We end with some general guidelines for when and how specific types of platform businesses might self-regulate more effectively. Although our sample is small and exploratory, the research suggests that a combination of self-regulation and credible threats of government regulation may yield the best results. We also note that effective self-regulation need not happen exclusively at the level of the firm. When it is in their collective self-interest, as occurred before the Internet era, coalitions of firms within the same market and with similar business models may agree to abide by a jointly accepted set of rules or codes of conduct.

54 Schulz and Held (n 51); see also Christopher T Marsden, *Internet Co-Regulation: European Law, Regulatory Governance*

purpose of the common good. Only the means of self-regulation within the state framework is used to carry out this purpose.[55] In co-regulation, public ordering thus stands hierarchically above private ordering in two respects: Temporally, private ordering takes place only after the framework has been set by public ordering; normatively, private ordering takes place only to implement the public ordering framework.[56] Admittedly, the normative structure on social media platforms has parallels to co-regulation: Public authorities set a regulatory framework through new-school speech regulation; within this framework, social media platforms set their own law by way of private ordering. However, there is a key difference with co-regulation. In the case of communication rules on platforms, the state-set framework and the private communication rules inextricably comingle. In contrast to co-regulation, private communication rules do not necessarily serve the pure implementation of state interests. Rather, public welfare purposes of public ordering are intermingled with original corporate purposes of private ordering. To take a simple example: If we run a platform about dachshunds, then it is crucial that we can prohibit cat content on the platform and remove it when it is uploaded in violation of that rule to define the identity of the platform. At the same time, we might have to be compliant with general state-set rules governing platforms dealing with animals (e.g., regarding the sale of protected species).[57]

28 In that sense, private ordering and public ordering do not, then, exist in a hierarchical relationship, they overlap. They merge into a hybrid regulatory structure[58]—from a governance perspective, private product and public concerns become one.

II. A Definition of Hybrid Speech Governance

29 Accordingly, none of the typical forms of regulation can adequately capture the hybridity of communication rules on online platforms. Against this background, we propose a distinct category of hybrid speech governance. Hybrid speech governance is characterized by three elements.

- First, it refers to regulatory structures in which public and private communication rules overlap, i.e. govern the same behavior .[59] This applies regardless of whether platform operators apply public rules voluntarily or are obliged to do so.
- Second, public and private communication rules interact with each other: Government requirements shape the form of private platform rules; conversely, the economic interest in private platform rules[60] shapes the degree to which government requirements are expressed on the platform.[61]
- Third, this results in a regulatory structure in which private and public communication rules are inextricably linked.[62] The two levels of rules thus form the hybrid field of communication rules. In short, hybrid speech governance refers to the overlap, interdependence, and inseparability of private and public communication rules on social media platforms.

D. Constitutional Challenges of Hybrid Speech Governance

30 In liberal democracies, the requirements for rules differ depending on whether they are private or public rules. Applying this dichotomy between public and private rules to the category of hybrid speech governance encounters limitations. The question emerges as to how concepts based on this dichotomy can be applied with regard to hybrid

and Legitimacy in Cyberspace (Cambridge University Press 2011); Michèle Finck, 'Digital Co-Regulation: Designing a Supranational Legal Framework for the Platform Economy' <https://papers.ssrn.com/abstract=2990043> accessed 22 November 2022.

55 Hoffmann-Riem (n 10) 44.

56 Cf. Schulz (n 4) 239 et seq.

57 Schulz (n 4) 239.

58 It is this overlap that leads to hybridity; thus, unlike David Levi-Faur, 'Regulation and Regulatory Governance' in David Levi-Faur, *Handbook on the Politics of Regulation* (Edward Elgar Publishing 2011) 13 et seqq. we do not want to call forms of regulation in which private and public ordering can be separated 'hybrid regulation'.

59 On the intersection of state and private power see also Keller (n 10).

60 Kettemann and Schulz (n 14).

61 On the complex interaction between corporate and government interests in relation to Facebook cf. Arun (n 35).

62 On the inseparability of public and private ordering in the information society, see also De Gregorio and Radu (n 10) 82.

speech governance. In this respect, legal research is still in its infancy.[63] At its core, the query is to determine how constitutional concepts originally developed to justify and limit state power may be applied when power is exercised through a hybrid rule structure.[64] We would like to focus here on three fundamental aspects. First, there is the question of the basis for validity (*Geltungsgrund*) behind hybrid rule structures on platforms: Is it democratic legitimacy or private autonomy (I)? This is also linked to the question of whether and to what extent hybrid regulatory structures have to meet rule of law requirements that apply to state-set law (II). Third, there is the question of the extent to which fundamental rights obligations apply to hybrid rule structures (III). These questions may come up at the levels of rulemaking, rule implementation, rule interpretation, and rule enforcement. While we question whether and how state-oriented concepts apply to hybrid speech governance, we do not use our approach to address the question of whether platforms may fall under the concept of "state".[65] We rather stick to the state/non-state distinction with platforms as non-state actors; yet this does not preclude testing normative concepts developed for state acts for application to platforms.

I. The Basis for Validity of Communication Rules: Democratic Legitimacy or Private Autonomy?

"Classifying an act as public or private determines what kind of legitimacy it requires".[66]

31 State law has a unilateral effect on citizens and can be enforced by coercion. In view of this effect, the community in which the law is applied must legitimize this law democratically. Conversely, private rules are based on private autonomy.[67] These contractual obligations form the basis of private communication rules. Citizens are fundamentally free to enter into contractual ties with other citizens and these can entail rules for future behavior. Platform users are confronted with rules whose basis for validity is blurred: In hybrid speech governance public and private rules are intertwined. This complicates the question of the basis of validity of hybrid rule structures on platforms.[68] Are those rules based on the private autonomy of the platform operators and users or on the democratic legitimacy of state laws?

32 With regard to the rule structure on platforms, some scholars implicitly address the mix of state legitimacy and private autonomy. They emphasize the legitimizing character of state law for platform rules. Indeed, the private rules of online platforms could be legitimized by their compliance with state law, in particular with legal requirements for T&C. Indeed, on the one hand, T&C regulations provide for the approval of rules by users, while on the on the other, they serve the common good and platform rules based on them would thus gain legitimacy.[69] From the perspective of political science, a democratic-legitimacy framework could be transferred to private platform rules.[70] For example,

63 Cf. Stephan Dreyer and others, 'European Media Law in Times of Digitality' in Matthias Kettemann, Alexander Peukert and Indra Spiecker gen. Döhmann, *The Law of Global Digitality* (1st edn, Routledge 2022) 183.

64 On the necessity of new dimensions of constitutional law in the digital age cf. also Oreste Pollicino and Giovanni De Gregorio, 'Constitutional Law in the Algorithmic Society' in Hans-Wolfgang Micklitz and others (eds), *Constitutional Challenges in the Algorithmic Society* (1st edn, Cambridge University Press 2021) 14.

65 On this matter cf., e.g., Anupam Chander, 'Facebookistan' (2012) 90 North Carolina Law Review 1807; Susan Benesch, 'But Facebook's Not a Country: How to Interpret Human Rights Law for Social Media Companies' (2020) 38 Yale Journal on Regulation Bulletin 86; Anna Sophia Tiedeke, 'Self-Statification of Corporate Actors? : Tracing Modes of Corporate Engagements with Public International Law' (European University Institute 2022) Working Paper <https://cadmus.eui.eu/handle/1814/74562> accessed 14 August 2023.

66 Goldmann (n 6) 48.

67 At least in principle one may of course argue about the power imbalance between users and platform providers and the effect on private autonomy. Consequently, in Germany one way of binding private rules to constitutional rights builds on the laws for the control of general terms and conditions, cf. German Federal Supreme Court, Judgements of 29 Jul 2021, III ZR 179/20 and ZR 192/20.

68 Bloch-Wehba (n 32) 66; Gilad Abiri and Sebastian Guidi, 'From a Network to a Dilemma: The Legitimacy of Social Media' <https://papers.ssrn.com/abstract=4230635> accessed 24 November 2022 argue as follows: "Social networks are in a dilemma. The reason their legitimation crisis seems irresolvable is, simply, that they do not fit any existing cultural role. They are too public to be a corporation and too private to be a government".

69 On the legal situation in Germany see Louis Jakob Rolfes, 'The Legitimacy of Rules of Virtual Communities' (Humboldt-Universität zu Berlin 2022) <https://edoc.hu-berlin.de/handle/18452/24607> accessed 23 November 2022.

70 For an overview of approaches see, e.g., Nicolas Suzor,

some believe that platform governance requires a holistic combination of input, throughput and output legitimacy.[71] In particular, the focus has so far been placed too strongly on legitimacy through processes in the sense of throughput legitimacy,[72] while input legitimacy, i.e. the question of who makes decisions on rules, has been underexposed.[73] In this respect, regulation by the democratic state should be the main source of legitimacy in platform governance.[74]

33 Overall, the question of the basis of validity of hybrid rule structures will heavily depend on the underlying legal theory. This applies both to rulemaking in general[75] and to platform governance in particular[76]. The search for such basis is all the more challenging when the familiar dichotomous logic of private and public rulemaking is inadequate, as in the case of hybrid speech governance. In view of this phenomenon, new concepts will have to be devised.

II. The Requirements for Communication Rules: Rule of Law or Freedom of Contract?

34 The same holds true for the principle of the rule of law. This principle is originally state-centered. According to the principle, sovereign power is subject to obligations. On the one hand, these obligations can be formal. Accordingly, state power must be exercised in an orderly procedure. On the other hand, substantive requirements can arise from the rule of law principle.[77] These include, inter alia, the requirement of legal certainty, the guarantee of legal protection, the prohibition of arbitrariness, judicial independence, and the requirement of transparency.[78] However, the rule of law principle is directed exclusively at public authorities in order to limit the vertical balance of power. If, however, private individuals are in conflict, none of the private individuals is hierarchically superior from a legal point of view. Therefore, private persons cannot unilaterally issue orders over another private person. Rather, this horizontal relationship between private individuals is governed by the freedom of contract. According to this principle, everyone is free to choose whether to enter into a contract at all, with whom and to what content. Consequently, the content requirements for private agreements do not arise from the principle of the rule of law, but from the free will of the parties.

35 In the context of hybrid speech governance, nonetheless, mechanisms of state law and private agreements largely overlap. This raises the question of whether, and if so how, requirements of the rule of law principle should be applied to hybrid rule structures. In actor-centered legal thinking, this question falls into two aspects. First, in actions that influence private regulation: How can it be ensured that the state's obligations are not circumvented by the indirect effect on the actions of platforms? Secondly: Are the platforms themselves bound by the principle, or would they have to be bound by it through state regulation?

36 The emergence of hybrid speech governance will require understanding the rule of law principle from a non-state-centric perspective. Simply

Tess Van Geelen and Sarah Myers West, 'Evaluating the Legitimacy of Platform Governance: A Review of Research and a Shared Research Agenda' (2018) 80 International Communication Gazette 385.

71 Blayne Haggart and Clara Iglesias Keller, 'Democratic Legitimacy in Global Platform Governance' (2021) 45 Telecommunications Policy 102152. They build on Fritz Wilhelm Scharpf, *Governing in Europe: Effective and Democratic?* (Oxford University Press 1999); Vivien A Schmidt, 'Democracy and Legitimacy in the European Union Revisited: Input, Output *and* "Throughput"' (2013) 61 Political Studies 2.

72 Cf. also Kettemann and Schulz (n 14) 28 et seqq.

73 Haggart and Keller (n 71) 14 et seq.

74 Haggart and Keller (n 71) 15.

75 Gregor Bachmann, *Private Ordnung* (Mohr Siebeck 2006) 179 et seqq.

76 Haggart and Keller (n 71) 2.

77 Jeremy Waldron, 'The Rule of Law in Public Law' in Mark Elliott and David Feldman (eds), *The Cambridge companion to public law* (Cambridge University Press 2015); András Sajó, 'The Rule of Law' in Roger Masterman and Robert Schütze (eds), *The Cambridge Companion to Comparative Constitutional Law* (1st edn, Cambridge University Press 2019). For the example of European and German law see Calliess, 'EU-Vertrag (Lissabon) Art. 2 [Die Werte Der Union]' in EUV and AEUV (eds), *Calliess/Ruffert* (6th edn, 2022); Huster and Rux, 'GG Art. 20 [Bundesstaatliche Verfassung; Widerstandsrecht]' in Epping and Hillgruber (eds), *BeckOK Grundgesetz* (52nd edn, 2022) 138 et seq.

78 On specific requirements in German law see Jarass, 'GG Art. 20 [Verfassungsrechtliche Grundprinzipien; Widerstand]' in Jarass and Pieroth (eds), *Grundgesetz für die Bundesrepublik Deutschland* (17th edn, 2022) 37 et seqq. On EU law see Calliess (n 77) 27. See also Article 2 a) Regulation (EU, Euratom) 2020/2092 of the European Parliament and of the Council of 16 December 2020 on a general regime of conditionality for the protection of the Union budget.

transferring familiar rule of law principles to hybrid communication rule structures will not be helpful in this regard.[79] Scholars have made initial suggestions to transfer rule of law principles to private communication rules.[80] The governance-centric perspective of hybrid speech governance should play a central role in the further development of such rule of law standards on platforms.

37 Certainly, the fact that concepts of the rule of law are transferred to situations of private power is, of course, not a novelty in itself. Indeed, the legislature regularly responds by imposing mandatory requirements to situations in which power is unequally distributed among private parties in actual terms, e.g., in labor law, consumer protection law, or private utilities law. While legal traditions could develop for decades with respect to these areas of law, the transfer of rule of law principles to private ordering by platform operators is still being tested by lawmakers, jurisprudence and academia.

III. Fundamental Rights and Communication Rules: Entitlement and/or Obligation?

38 Hybrid speech governance also poses challenges to the structure of fundamental rights. In liberal democracies, the latter is generally based on the private/public dichotomy: Public authorities are obliged to observe the fundamental rights of private individuals, but are not entitled to invoke fundamental rights.[81] Conversely, private individuals are entitled to invoke fundamental rights vis-à-vis public authorities, but are not obliged to observe the fundamental rights of other private individuals. The basic concept is, therefore, that public authorities are obliged to respect fundamental rights, while private individuals are entitled to invoke those rights. This conception poses challenges for hybrid speech governance, all of those that are recently debated in constitutional law, based on the respective legal system.

39 A first challenge results from the positive obligation of state actors to protect the fundamental rights of citizens. Indeed, certain constitutional provisions oblige state actors to take legislative action.[82] This is rather alien to U.S. constitutional thinking, but quite common in Europe. This raises the question of the degree to which state actors must shape the hybrid communication order themselves by means of a minimum set of state communication rules on platforms, so as not to leave this field exclusively to private platform operators.

40 This also poses a second challenge. When prescribing public rules that shape hybrid speech governance, state actors must respect the fundamental rights of platform operators. When state actors regulate the private moderation of content, they interfere with the fundamental rights of platforms. In particular, the setting and exercise of private rules may itself be protected by fundamental rights, such as the entrepreneurial freedom, professional freedom, or freedom of expression of platform operators.[83] In this respect, the question arises as to the extent to which state actors may shape the hybrid regulatory structure themselves without disregarding fundamental rights interests. These rights have the same protective orientation as the rights of users to access information and the general information interest of the public, which we do not address separately here.

79 Especially since, from a state-centered perspective, the concept is already subject to national peculiarities, Geranne Lautenbach, *The Concept of the Rule of Law and the European Court of Human Rights* (Oxford University Press 2013).

80 Nicolas Suzor, 'The Role of the Rule of Law in Virtual Communities' (2010) 25 Berkeley Technology Law Journal 1817; Nicolas Suzor, 'Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms' (2018) 4 Social Media + Society; Niva Elkin-Koren and Maayan Perel, 'Guarding the Guardians: Content Moderation by Online Intermediaries and the Rule of Law' in Giancarlo Frosio (ed), Niva Elkin-Koren and Maayan Perel, *Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020); Stephan Koloßa, 'Facebook and the Rule of Law' (2020) Zeitschrift für ausländisches öffentliches Recht und Völkerrecht 509; cf. also Bloch-Wehba (n 32) 71 et seqq. arguing in favor of a transfer of administrative law principles (transparency, reasoned decision-making, user participation, and judicial review).

81 The national and international fundamental rights systems differ in the construction of the "state actor" and also vary in terms of concepts to (indirectly) bind non-state actor to fundamental rights.

82 ECtHR, Judgement of 6 May 2003, Application no. 44306/98, Appleby and others; Christian Starck, 'State Duties of Protection and Fundamental Rights' (2009) 3 Potchefstroom Electronic Law Journal/Potchefstroomse Elektroniese Regsblad; Kettemann and Tiedeke (n 45).

83 Cf. Ralf Müller-Terpitz, 'Soziale Netzwerke als Gegenstand des geltenden Rechts. Eine Rechtssystematische Einordnung' in Martin Eifert and Tobias Gostomzyk (eds), *Netzwerkrecht* (Nomos Verlagsgesellschaft mbH & Co KG 2018); Anna Kellner, *Die Regulierung der Meinungsmacht von Internetintermediären* (1. Auflage, Nomos 2019) 91 et seqq.; Samira Tief, *Kommunikation auf Facebook, Twitter & YouTube: Verfassungsrechtlicher Schutz der Informationsintermediäre und ihrer Nutzer durch die Medienfreiheiten* (1st edn, Duncker & Humblot 2020) 93 et seqq.Nomos 2019

41 A third challenge of hybrid speech governance concerns the attribution of rules to fundamental rights. In view of the overlap between state and private rules, it is sometimes difficult to classify their authorship. This also makes it unclear whether the state, which is bound by fundamental rights, or the platform operator, which is not bound by fundamental rights, is acting. If a private platform merely implements a public rule, this could possibly be attributed to the state. In particular, if state actors exert pressure on platform operators to enact a certain communication rule, it may be obvious to classify this as state action bound by fundamental rights, despite the outwardly private form of action.[84]

42 Finally, even if private action cannot be attributed to the state, the question arises as to whether platform operators can be obliged to respect the fundamental rights of their users —even though they are bearers of fundamental rights themselves. Concepts are increasingly being proposed to bind platform operators to fundamental rights with different binding effects when moderating content. For example, the German Federal Court of Justice has ruled that online platforms that are market-dominant and have an open communicative orientation must consider the fundamental rights of their users when moderating content. Essentially, this results in procedural obligations for platform operators when moderating content.[85] In other EU Member States, too, national courts are applying concepts to bind platform operators to fundamental rights in their content moderation.[86] Nevertheless, such concepts are still in their infancy; a profound understanding of the fundamental rights obligations of private platform operators is still lacking. In the future, it will be necessary to find suitable solutions in the area of hybrid speech governance in order to determine the scope of potential fundamental rights obligations.

E. The Digital Services Act Embracing Hybrid Speech Governance

43 The DSA addresses some of those challenges. Certainly, in principle, the DSA resorts to classic forms of regulation. Essentially, the European legislature relies on mechanisms of co-regulation. In particular, very large online platforms are to assess systemic risks themselves (Article 34) and take measures against such risks (Article 35). Similarly, the DSA provides for the development and implementation of voluntary standards and codes of conduct (Article 44 et seq.), in which the EU Commission is to play a supporting role. The regulation also standardizes commitments by platforms (Article 71 et seq.), which can be declared binding by the EU Commission. In addition to these mechanisms of co-regulation, the DSA contains forms of command-and-control regulation. For example, it obligates platform operators to provide procedural safeguards to users (Article 16 et seq.), imposes transparency requirements (Article 15, 24, 27, 39, 42), and provides fines for non-compliance (Article 74). Old-school speech regulation, i.e., direct regulation of what is permissible speech, is essentially left to the Member States by the EU.

44 In this respect, the approach of the DSA is first and foremost to address procedural requirements to the platform operators, but not to establish an online communication order with regard to content. Nevertheless, the DSA creates the content-related framework of the communication order. Article 14(4) reads as follows:

84 On this so-called 'jawboning' see Derek E Bambauer, 'Against Jawboning' (2015) 100 Minnesota Law Review 51; Keller (n 10) 5 et seqq.; David Greene, 'When "Jawboning" Creates Private Liability' (*Electronic Frontier Foundation*, 21 June 2022) <https://www.eff.org/deeplinks/2022/06/when-jawboning-creates-private-liability> accessed 30 November 2022."plainCitation":"Derek E Bambauer, 'Against Jawboning' (2015

85 Indeed, in examining Facebook's community standards, the Court interpreted Facebook's rules in the light of fundamental rights. The court thus concluded that Facebook may in principle set up communication rules in their T&C, even when their T&C go beyond national libel laws. This is because of Facebook's own fundamental rights. However, due to its users' fundamental rights, there must always be an objective reason for removing content and blocking user accounts. In addition, the platform must provide for certain procedural requirements in their T&C, for example information, statement of reasons, and the possibility of a counterstatement in the case of content deletions, see German Federal Supreme Court, Judgements of 29 Jul 2021, III ZR 179/20 and ZR 192/20; cf. also German Federal Constitutional Court, Decision of 22 May 2019, 1 BvQ 42/19, III. Weg; Daniel Holznagel, 'Overblocking Durch User Generated Content (UGC) – Plattformen: Ansprüche Der Nutzer Auf Wiederherstellung Oder Schadensersatz?' (2018) 34 Computer und Recht 369, 371 et seq.; Lena Isabell Löber and Alexander Roßnagel, 'Das Netzwerkdurchsetzungsgesetz in Der Umsetzung' (2019) Multimedia und Recht 71, 75; Simon Jobst, 'Konsequenzen Einer Unmittelbaren Grundrechtsbindung Privater' (2020) Neue Juristische Wochenschrift 11; Judit Bayer, 'Rights and Duties of Online Platforms' in Judit Bayer and others (eds), *Perspectives on Platform Regulation: Concepts and Models of Social Media Governance | Across the Globe* (Nomos Verlagsgesellschaft mbH & Co KG 2021) 38.

86 For the Netherlands see District Court of Amsterdam, Judgement of 9 Sep 2020, C/13/687385; for Italy see Court of Rome, Decision of 29 Apr 2020, 80961/19.

> "Providers of intermediary services shall act in a diligent, objective and proportionate manner in applying and enforcing the restrictions (provided for in their terms and conditions), with due regard to the rights and legitimate interests of all parties involved, including the fundamental rights of the recipients of the service, such as the freedom of expression, freedom and pluralism of the media, and other fundamental rights and freedoms as enshrined in the Charter."

45 In doing so, the DSA creates a new form of hybrid speech governance. Certainly, prior to the DSA, the EU's Terrorist Content Online Regulation[87] had already taken on the phenomenon of hybrid speech governance.[88] Article 5(1) of the regulation stipulates that the T&C upon which hosting service providers must moderate terrorist content have to respect the fundamental rights of users. Yet this provision only applies to the limited scope of public terrorist content online. As a result, the Terrorist Content Regulation is indeed the silent pioneer of hybrid speech governance. By contrast, the DSA now features prominently. This is because the DSA applies regardless of the subject matter of online content. Consequently, the DSA is the world's first comprehensive approach to address the challenges of hybrid speech governance. The DSA finds initial answers to the constitutional challenges mentioned above (I). At the same time, it also leaves a number of questions unanswered (II).

I. Answers to Constitutional Challenges Posed by the Digital Services Act

46 The DSA responds to the problem areas identified above by, on the one hand, recognizing the private law-making authority of the platform operators, but, on the other hand, integrating requirements into private ordering which are, in themselves, only imposed on state actors. This concerns the basis for validity of communication rules (1), rule of law requirements (2) and fundamental rights protection (3).

1. The Basis for Validity of Communication Rules: Private Autonomy in a Framework of Democratic Legitimacy

47 The DSA explicitly recognizes that the legal basis for content moderation are the T&C of online platforms. In this way, the European legislature stipulates that the basis for content moderation continues to be the private autonomy of the platforms and users. This is because the rules of communication on social media platforms continue to be in private hands, as provided for in their T&C. Accordingly, it is primarily the users' consent to the T&C that justifies the content moderation by platform operators. In order to be able to give this consent as autonomously as possible, the DSA provides for numerous transparency requirements for the benefit of users. For example, the T&C must contain information on any policies, procedures, measures and tools used for the purpose of content moderation, including algorithmic decision-making and human review, as well as the rules of procedure of their internal complaint handling system; furthermore, the T&C must be set out in clear, plain, intelligible, user-friendly and unambiguous language, and shall be publicly available in an easily accessible and machine-readable format (Article 14(1) DSA).

48 This model of consent is embedded in a framework of (weak) democratic legitimacy. The obligation to pursue general welfare objectives in T&C law can have a legitimizing effect. National T&C law regularly provides that the content of T&C can be reviewed on the basis of general interest purposes.[89] In particular, Article 14(4) of the DSA now explicitly states that platform operators must observe the fundamental rights of their users when checking the content of their T&C. The EU Charter of Fundamental Rights is in turn part of the democratically legitimized primary law of the EU. By effectively integrating the standards that follow from this into the T&C of the platforms, the platform rules can consequently gain democratic legitimacy, at least indirectly.

49 Overall, the response to hybrid speech governance by the EU is therefore a mixed legitimation model: In essence, the European legislature follows the logic of private ordering in the DSA, but ties this to public welfare purposes. The DSA does not provide for direct user participation in the development of communication rules. In the long term, greater democratic legitimacy in content moderation might be achieved through proposals such as social media councils. Such councils would be staffed by citizens or users to draft or enforce communication rules.[90] In

87 Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online.

88 João Pedro Quintais, Naomi Appelman and Ronan Ó Fathaigh, 'Using Terms and Conditions to Apply Fundamental Rights to Content Moderation' (2023) 24 German Law Journal 881, 890 view this as the source of inspiration for Art. 14(4) DSA.

89 Concerning German law Rolfes (n 69) 115 et seqq.

90 Matthias C Kettemann and Martin Fertmann, 'Making

Germany, for example, the government is planning to advance corresponding legitimacy models.[91]

2. The Requirements for Communication Rules: Rule of Law Guarantees in Content Moderation

50 It is true that, according to the language of the DSA, social media platforms remain free in principle to determine their communication rules within the framework of their T&C. However, the DSA obliges platform operators to comply with requirements that were originally imposed only on state actors as an expression of the principle of the rule of law.

51 First, content moderation must be proportionate under Article 14(4) DSA. According to its original understanding, the principle of proportionality is state-centric. It serves to limit public authority.[92] The principle states that state action may only pursue legitimate purposes in an appropriate, necessary and proportionate manner.[93] In this context, encroachments on fundamental rights by state actors should be as freedom-preserving as possible. With its Article 14(4) DSA, the European legislature is now explicitly transferring this state-centric concept to content moderation by private platform operators.[94] The concrete requirements for the application of the principle of proportionality in private content moderation have yet to be clarified.[95] Nevertheless, it is already clear that the EU is integrating requirements for public ordering into the private ordering of private platform operators. This is to be understood as recognition of hybrid speech governance.

52 Second, according to Article 14(4) DSA, moderation decisions must be "objective". This requires that moderation decisions be non-discriminatory and non-arbitrary.[96] Objectivity is a prohibition of arbitrariness. Users must be treated equally; unequal treatment must be justified. Binding particularly powerful digital companies to the principle of equality is a constitutional trend in the area of digital communications.[97] The DSA is now responding to this by integrating the obligation of equal treatment as a public ordering requirement into private ordering by platform operators.

53 Requirements, which in themselves stem from the rule of law principle in the vertical relationship between state actor and citizen, can also be found outside of Article 14(4) DSA. For example, Article 14 DSA provides in its paragraph 1 that the rules of communication must be written in clear, simple, understandable, user-friendly and unambiguous language and be publicly available in an easily accessible and machine-readable format. Very large platforms must also provide information on available remedies and redress mechanisms (Article 14(5) DSA). Simply put, the rules for private communications must be transparent and sufficiently specified in terms of the requirement for legal certainty. With these requirements, the European legislature is taking its cue from the rule of law, which otherwise only applies to state actors. The same applies to the introduction of legal protection mechanisms against moderation decisions. Here, the EU uses the logic of administrative law: Moderation decisions must be justified (Article 17), platforms must provide for an appeal procedure (Article 20), and offer external legal protection (Article 21).

3. Fundamental Rights and Communication Rules: Entitlement *and* Obligation

54 In particular, the DSA addresses the challenges that arise in view of the fact that private platform operators—unlike state actors—are in principle only entitled to invoke fundamental rights, but

Platforms Rules More Democratic: Are Social Media Councils the Way to Go?'; Matthias C Kettemann and Martin Fertmann, *Platform-Proofing Democracy. Social Media Councils as Tools to Increase the Public Accountability of Online Platforms* (Friedrich-Naumann-Stiftung für die Freiheit 2021).

91 SPD (Social Democrats), Bündnis90/Die Grünen (Greens) and FDP (Liberals), *Coalition Agreement of the German Government (2021-2025): Mehr Fortschritt Wagen - Bündnis Für Freiheit, Gerechtigkeit Und Nachhaltigkeit*, p 14.

92 Cf. Article 52(1) EU Charter of Fundamental Rights.

93 Verica Trstenjak and Erwin Beysen, 'Das Prinzip Der Verhältnismäßigkeit in Der Unionsrechtsordnung' (2012) Europarecht 265, 274 et seqq.; Wolf Sauter, 'Proportionality in EU Law: A Balancing Act?' (2013) 15 Cambridge Yearbook of European Legal Studies 439.

94 Systemic balancing by platforms based on the proportionality principle already corresponds to the reality of platform governance, see Douek (n 31).

95 For initial clarifications see Tobias Mast and Christian Ollig, 'The Lazy Legislature – Incorporating and Horizontalising the Charter of Fundamental Rights through Secondary Union Law' (2023) European Constitutional Law Review *Forthcoming*.

96 Recital 47 DSA.

97 See Wolfgang Hoffmann-Riem, *Recht im Sog der digitalen Transformation* (Mohr Siebeck 2022) 103.

not obliged to respect them vis-à-vis other private parties. So, it follows that, on the one hand, the European legislature confirms in its Article 14(4) DSA that platform operators may moderate content on the basis of their T&C. In this way, the EU respects the fact that platform operators are themselves protected by fundamental rights when moderating content.[98] This is also supported by the wording in Article 14(4) DSA "with due regard to the rights and legitimate interests of *all* parties involved"[99]. "All parties" includes platform operators and their respective fundamental rights. In this way, the lawmaker gives expression to the European legal tradition[100] of weighing fundamental rights among private parties.[101] In this respect, companies are afforded the flexibility to define their own communication rules by way of private ordering.

55 On the other hand, despite the recognition of a comprehensive balancing of fundamental rights, Article 14(4) DSA is clearly centered on the protection of fundamental rights *by*, not *for* platforms.[102] Article 14(4) DSA obliges private platform operators to respect users' fundamental rights when moderating content. With regard to content moderation, the DSA explicitly mentions users' fundamental rights only, namely their freedom of expression and the freedom and pluralism of the media. In recital 47, the DSA adds the freedom of information and refers to relevant international standards for the protection of human rights, such as the UN Guiding Principles on Business and Human Rights. With this obligation for digital companies to respect the fundamental rights of users, the European legislators are meeting the demands of the advocates of "digital constitutionalism".[103]

56 With Article 14(4) DSA, the European legislature thus takes up the phenomenon of hybrid speech governance. It states that platform companies are both bearers of fundamental rights and are obliged to respect the fundamental rights of users at the same time. Accordingly, the DSA recognizes that content moderation consists of an overlap of private ordering and public ordering. This goes beyond the constitutional doctrine of horizontal effects. According to this doctrine, courts in European member states already combine private ordering of content moderation with public ordering requirements. However, the EU no longer leaves the horizontal effect of fundamental rights to the courts, but codifies it explicitly in Article 14(4) DSA. This turns the judicial source of the horizontal effect of fundamental rights into a legislative source. In particular, the legislature provides courts with certain guidelines for the balancing process. Certainly, within this framework the courts have leeway to develop dimensions of horizontal effect.[104]

II. Questions Left Open in the Digital Services Act

57 However, the DSA also leaves a number of questions unanswered with regard to those constitutional challenges of hybrid speech governance. In particular, the incorporation of horizontal fundamental rights as enshrined in the Charter in an ordinary legislative act is a novel construction; this gives rise to a colorful bouquet of questions, the comprehensive answers to which will be given elsewhere. We will address only two aspects here. First, the wording of Article 14(4) DSA does not refer to rulemaking on communication rules (1). Second, the norm applies across the board to all platforms; the European legislature does not create a tiered system of obligations (2).

1. Rulemaking Covered by the Scope of Article 14 DSA?

58 Article 14(4) DSA, when strictly read, refers only to the application and enforcement of the communication rules stemming from the T&C. In contrast, the upstream level of rulemaking is not covered. It could be argued, therefore, that platforms are not bound by users' fundamental rights at the rulemaking level. In this case, platform operators would be essentially free to design their rules. Only in the concrete application and enforcement of the rules could fundamental rights evaluations become relevant. Such a reading would reduce the fundamental rights obligation to a procedural moment: When moderating content, platform operators would have to be able to plausibly demonstrate that they have taken fundamental rights into consideration in some form.[105] It is nevertheless more likely that the European legislators have wanted to bind platform

98 See also the mentions of the freedom to conduct a business und the freedom of contract in recitals 3, 45, 52 of the DSA.

99 Italics here only.

100 De Gregorio (n 6) 316.

101 Cf. Eva Skobel, *Regulierung nutzergenerierter Inhalte auf sozialen Netzwerken* (Universität Trier 2021) 310.

102 Cf. on the 'one-sided fundamental rights pathos' of the DSA Denga (n 29) 580.

103 Pollicino and Gregorio (n 64) 16 et seqq.

104 See section E. II. 2.

105 Mast and Ollig (n 95).

operators to fundamental rights when drafting their communication rules. Indeed, recital 47 of the DSA goes beyond the wording of Article 14(4) DSA and covers the design, application and enforcement of the T&C.[106] The DSA does not provide a clear cut response; a clearer formulation would have been desirable here.[107]

2. Graduation of Obligations for Platforms?

59 More serious than the above-mentioned ambiguity, however, is the fact that Article 14(4) DSA does not specify any criteria for weighing the scope of the intermediaries' obligations. This applies both in personal and in substantive terms.

60 In personal terms, it is noteworthy that the provision is located in the general part of the DSA. Accordingly, the provision applies to *all* intermediaries, regardless of their mode of operation or size. Consequently, small platforms that have not yet established themselves in the market are covered by the provision, as are platforms that dominate the market. According to the current conception, the dominance of a platform has no impact on the content of the communication rules.[108] For smaller platforms in particular, the far-reaching obligations of Article 14(4) DSA can mean an unjustified restriction of their contractual freedom.[109] The undifferentiated scope of application of Article 14 DSA is surprising, especially in light of the fact that obligations in the regulatory system of the DSA are otherwise determined by the size and functioning of an intermediary. Recital 47 does, however, emphasize the fundamental rights of very large online platforms; this might serve as a weighing criterion.

61 Article 14(4) DSA also remains vague in substantive terms. The legislature does not provide any concrete criteria for determining the substantive scope of the obligations under Article 14(4) DSA, in particular regarding the fundamental rights obligation of platforms.[110] The formulation that platforms must have "due regard" to the fundamental rights of users when moderating content leaves open the extent to which platforms may moderate content.[111] At least it can be inferred from the wording of Article 14(4) DSA that platforms should not be bound state-like, given the consideration of the platforms' own fundamental rights.[112] The case law of the European Court of Justice and the European Court of Human Rights could provide guidance in the balancing process, although this has so far only concerned vertical cases between state actors and citizens, not horizontal cases between platforms and citizens.[113] The emphasis on individual fundamental rights positions in Article 14(4) DSA, namely freedom of expression and freedom and pluralism of the media, could also inform the balancing process. The same goes for the reference to the UN Guiding Principles on Business and Human Rights in recital 47 which provide certain guidelines for internal company processes.[114] Furthermore, in line with rulings of Member States' courts, the fundamental rights obligations could vary depending on the market dominance of the platform, the communicative orientation of the platform, or the degree of dependence of the users on the platform.[115] The pressure exerted by state actors on private content moderation could also be taken into account when determining the extent of a fundamental rights obligation.

62 Overall, the open wording of Article 14(4) DSA leaves room for academia, practice, and courts to develop concrete criteria to approach the scope of substantive

106 Quintais, Appelman and Fathaigh (n 88) 894; Benjamin Raue, 'Art. 14 DSA' in Franz Hofmann and Benjamin Raue (eds), *Digital Services Act – Gesetz über digitale Dienste* (Nomos 2023) paras 74 et seqq.

107 Cf. also Evelyn Douek, 'Content Moderation as Systems Thinking' (2022) 136 Harvard Law Review 528 arguing that meaningful accountability of content moderation system may solely be achieved by design choices and tradeoffs at the upstream level of content moderation as a form of systems thinking.

108 Ilaria Buri and Joris van Hoboken, 'The Digital Services Act (DSA) Proposal: A Critical Overview' (Institute for Information Law, University of Amsterdam 2021).

109 Andreas Peukert, 'Zu Risiken Und Nebenwirkungen Des Gesetzes Über Digitale Dienste (Digital Services Act)' [2022] Kritische Vierteljahresschrift für Gesetzgebung und Rechtswissenschaft 57, 61 et seqq.

110 Cf. Jürgen Kühling, '»Fake News« und »Hate Speech« – Die Verantwortung Der Medienintermediäre Zwischen Neuen NetzDG, MStV Und Digital Services Act' (2021) Zeitschrift für Urheber- und Medienrecht 461, 470.

111 German Bundesrat Decision, Document 96/21 of 26 Mar, 2021, 10.

112 Cf. Quirin Weinzierl, 'Institutionalizing Parallel Governance' (*Verfassungsblog: On Matters Constitutional*, 18 December 2020) <https://verfassungsblog.de/institutionalizing-parallel-governance/> accessed 7 April 2022. Others see it as a state-like obligation, Denga (n 29).

113 More about these specifications Quintais, Appelman and Fathaigh (n 88) 895 et seqq.

114 Quintais, Appelman and Fathaigh (n 88) 896.

115 See German Federal Constitutional Court, Decision of 22 May 2019, 1 BvQ 42/19, III. Weg.

obligations of private platform companies. In particular, the application of other provisions of the DSA could be helpful in operationalizing the vague scope of Article 14(4) DSA. On the one hand, the procedural guarantees of the DSA, namely the obligation to give reasons for moderation decisions, the internal complaint handling system, out-of-court dispute settlement bodies or the right of appeal to the Digital Services Coordinator could contribute to the concretization of the requirements of Article 14(4) DSA.[116] In addition, the systemic risk assessment and the risk mitigation measures based on it can concretize the requirements of Article 14(4) DSA.[117] Moreover, the use of codes of conduct is also likely to promote the legal certainty of the substantive requirements of Article 14(4) DSA.[118] But ultimately, only the European Court of Justice or legislators will be able to make binding statements on the extent of Article 14(4) DSA.

F. Hybrid Speech Governance and the U.S. Legal Framework

63 It is questionable how this European approach relates to U.S. legal thinking, which significantly shapes the corporate compliance of large tech companies on the other side of the Atlantic. Indeed, the European approach of Article 14(4) DSA to legally embed hybrid speech governance runs counter to fundamental convictions in the U.S. legal system. While it is at least in principle compatible with the European understanding that requirements for state actors are transferred to private ordering—for example, through the horizontal application of fundamental rights—U.S. legal thinking is characterized by the idea of an autonomous sphere of private ordering and a strict limitation of the binding force of the constitution to state action.[119] Private ordering by platforms is extensively protected by the First Amendment in the USA; the First Amendment thus constitutes the limit of state regulation of private ordering.[120] This protection is underpinned by Section 230 Communications Decency Act and the Digital Millennium Copyright Act.[121] This provides the framework for a liberal system of private ordering by platform operators.

64 Admittedly, U.S. law, too, recognizes possibilities, through the state action doctrine, to draw private action into the scope of constitutional obligations by way of exception.[122] The public forum doctrine, in particular, may serve as a vehicle for tying private actors to fundamental rights.[123] Yet the Supreme Court traditionally applies a narrow understanding of the public forum.[124] Notably, against this backdrop, lower courts have thus far rejected the argument that private social media platforms constitute a public forum in which the First Amendment would have to be respected.[125]

116 Quintais, Appelman and Fathaigh (n 88) 903 et seqq.

117 Quintais, Appelman and Fathaigh (n 88) 905 et seqq.

118 Quintais, Appelman and Fathaigh (n 88) 907.

119 Pollicino and Gregorio (n 64) 17; De Gregorio (n 6) 312.

120 Keller (n 10) 17; De Gregorio (n 6) 312.

121 Keller (n 10) 3 et seq.; Kettemann and Tiedeke (n 45) 6; Jacob Kosakowski, 'Delete and Repeat: The Problem of Protecting Social Media Users' Free Speech from the Moderation Machine Notes' (2022) 55 Suffolk University Law Review 65, 71 et seqq.

122 For example in *Marsh v. Alabama*, 326 U.S. 501 (1946) the Supreme Court recognized that a private company's operation of a city performed a public function. Under these circumstances, a private company could be subject to the First Amendment. This jurisprudence, however, has been qualified to the extent that state action is now presumed only when the private entity exercises power that traditionally belonged exclusively to the state, *Jackson v. Metropolitan Edison Co.*, 419 U.S. 345, 352 (1974). For further restrictions imposed by case law, see Keller (n 10) 8.

123 In *PruneYard Shopping Center v. Robins*, 447 U.S. 74 (1980) the justices recognized that a private shopping mall could constitute a public forum in which the distribution of leaflets would have to be tolerated.

124 For example, in *Manhattan Community Access Corp. v. Halleck*, 587 U.S. (2019), the Supreme Court rejected a public forum in the case of a private operator of a public access television station.

125 *Johnson v. Twitter, Inc.*, No. 18CECG00078 (Cal. Superior Ct. 2018); *Prager Univ v. Google LLC*, No. 17-CV-06064-LHK, (N.D. Cal. 2018); *Nyabwa v. Facebook*, No. 2:17-CV-24, (S.D. Tex. 2018); *Prager University v. Google LLC*, No. 18-15712 (9th Cir. 2020). See also Jonathan Peters, 'The "Sovereigns of Cyberspace" and State Action: The First Amendment's Application (or Lack Thereof) to Third-Party Platforms' (2017) 32 Berkeley Technology Law Journal 989; Jane Bambauer, James Rollins and Vincent Yesue, 'Platforms: The First Amendment Misfits Symposium: Compelled Speech: The Cutting Edge of First Amendment Jurisprudence' (2022) 97 Indiana Law Journal 1047. This may only be judged differently in the case of profiles of public officials on social media platforms, *Knight First Amendment Institute at Columbia University v. Trump*, No. 18-1691 (2d Cir. 2019); see also Jason Wiener, 'Social Media and the Message: Facebook, Forums, and First Amendment Follies Notes' (2020) 55 Wake Forest Law Review 217. See also *Davison v. Randall*, No. 17–2002 (4th Cir. 2019).

65 The U.S. is though facing a "moment when everything might change":[126] It seems not to be excluded that the Supreme Court will draft a model to bind platforms to fundamental rights in a weakened form according to the EU model discussed above. Such concept would add a balancing model to the current dichotomy of the state action doctrine. Indeed, there is currently a jurisprudential debate about the extent to which social media companies may moderate the content of their users. According to the traditional approach, this depends on whether these companies act as state actors; only in this case would the companies be bound by constitutional law. Lower courts in the U.S. are at odds on this issue. The U.S. Court of Appeals for the 5th Circuit rejects the idea that "corporations have a freewheeling First Amendment right to censor what people say".[127] That is why in September 2022, the court upheld a Texas social media law, House Bill 20, which prohibits major platforms from deleting content based on a speaker's viewpoint. So, social media platforms are understood to be state actors. They must comply with the First Amendment. Notably, according to the Court, the law does not regulate "the Platforms' speech at all". It rather protects "*other people's* speech and regulates the Platforms' *conduct*". Conversely, in May 2022 the U.S. Court of Appeals for the 11th Circuit struck down key parts of a comparable Florida law.[128] It was unconstitutional for the state to ban social media companies from content moderation. The court argued that content moderation activities by platforms are "free speech" within the meaning of the First Amendment.

66 It will now be up to the Supreme Court to decide to what extent social media companies may moderate content.[129] In any case, the Supreme Court has no shortage of nuanced suggestions from academia to find answers to this question.[130] For now, the current constitutional framework for regulating hybrid speech governance in the USA is still subject to numerous ambiguities. Whatever legal path is viable for regulating the rules of communication on social media platforms, an option should be chosen that takes into account both the fundamental rights of the platform operators and the fundamental rights of the users. The European legal tradition, in which "fundamental rights and freedoms interact with each other in a dialectic relationship of balancing"[131], may serve as a source of inspiration for the Supreme Court and/or lawmakers. Only such a balancing model can do justice to the phenomenon of hybrid speech governance. This is because, as shown, on platforms, private and public interests have common intersections and do not exist in a dichotomous relationship. Article 14(4) DSA overcomes this dichotomy; the norm is a regulatory prime example. However, it is also clear that the approach of the DSA, which already breaks with traditional ideas in the EU,[132] would all the more have to overcome constitutional hurdles even more so in the U.S. legal system.

126 Daphne Keller, cited in David McCabe, 'Supreme Court Poised to Reconsider Key Tenets of Online Speech' *The New York Times* (19 January 2023) <https://www.nytimes.com/2023/01/19/technology/supreme-court-online-free-speech-social-media.html> accessed 14 August 2023.

127 *Netchoice, LLC v. Paxton*, No. 21-51178 (5th Cir. 2022).

128 *Netchoice, LLC v. Att'y Gen., Fla.*, No. 21-12355 (11th Cir. 2022).

129 Ann E. Marimow and Cat Zakrzewski, 'Landmark Texas, Florida social media cases added to Supreme Court term', The Washington Post (29 September 2023) <https://www.washingtonpost.com/politics/2023/09/29/supreme-court-social-media-florida-texas-google-facebook/> accessed 24 November 2023.

130 For example, some suggest that courts should adapt their public forum jurisprudence to the digital age. In particular, functional considerations could be given to whether a forum on a platform has public characteristics, see, Peters (n 125) 1022 et seqq.

Others go in a similar direction when they propose a subtype of the public forum, namely a "*social* public forum": Platforms are bound by the First Amendment only if they offer a digital space for the general public that is essential to public discourse, see Amélie Heldt, 'Merging the Social and the Public: How Social Media Platforms Could Be a New Public Forum' (2020) 46 Mitchell Hamline Law Review 1032 et seqq.

Some propose that legislators should act. Indeed, platforms, as gatekeepers of public discourse, could possibly be legally bound to more or less extensive must-carry obligations; at the same time, in light of the First Amendment, platform operators' discretion in moderation would have to be respected, see Keller (n 10) 18–27; see also Kosakowski (n 121) 89 et seq.Still others suggest that because of the platform companies' First Amendment rights, there should be no direct regulation of moderation practices. Rather, through the combined application of antitrust and competition law, privacy and consumer protection law, and intermediary liability, incentives should be provided for platform operators to create a healthy digital public sphere, see Balkin, 'How to Regulate (and Not Regulate) Social Media' (n 25). Some also argue that content moderation by platform operators is not protected by the First Amendment, which in turn could open up new regulatory options, Pauline Trouillard, 'Social Media Platforms Are Not Speakers' (2022]) Ohio State Technology Law Journal *Forthcoming*.

131 De Gregorio (n 6) 316.

132 Mast and Ollig (n 95).

G. Conclusion and Outlook

67 The normative development of communication rules on online platforms puts traditional notions of rulemaking and rule application in trouble. The overlap, interdependence, and in- separability of private and public communication rules on social media platforms should therefore be analyzed under the lens of a new category: hybrid speech governance. This perspective can help to find appropriate approaches to contain private power without simply transferring state-centric concepts unchanged to platform operators. This applies to questions of the basis of communication rules, rule of law requirements, and fundamental rights obligations.

68 The EU's DSA adopts this perspective of hybrid speech governance and thus finds initial legislative answers to the questions raised. However, this is only the beginning of the story. Academia, practice, and jurisprudence will have to flesh out the DSA's approaches to hybrid speech governance in detail. If the Brussels Effect[133] can contribute here to the radiation of European standards into U.S. law remains questionable, given the constitutional structures on the western side of the Atlantic.[134]

69 Further challenges will arise in the (not so distant) future. Considering the increasing importance of online platforms for the exercise of fundamental rights, the issues discussed will not only affect free speech rights. Other fundamental rights of users will be affected by platform rules, such as academic freedoms, artistic freedom, or entrepreneurial freedom. This is all the more true when platforms offer functions that go beyond mere communication, in the metaverse, for example. In this context, the hybrid rule structure will not only affect communication, but conduct more generally. Furthermore, orders within orders may emerge when third parties can create their own worlds with their own rules on platforms. The governance structure thus takes on yet another level: The state influences private rulemaking, which in turn influences the private order of the third parties. In other words, the complexity of platform governance continues to increase. Hybridization processes are also emerging outside the field of platform regulation, especially with regard to the question of how constitutional values can find their way into technical systems, a question that goes by the catchword of "Constitutional AI"[135].[136] While the development of responsible AI systems oriented to constitutional standards is still based primarily on entrepreneurial initiative, i.e. moral rules set by private companies for AI systems to adhere to, regulators could increasingly incorporate constitutional requirements into AI legislation -the EU's forthcoming AI Act already bears witness to the claim of "Constitutional AI" in its approach. All of this makes it necessary to delve into hybrid regulatory structures to find well-founded ways to legally deal with them.

133 Anu Bradford, 'The Brussels Effect' (2012) Vol. 107 Northwestern University Law Review 1; Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press 2020).

134 Cf. also Keller (n 45) who argues for a cautious export of the DSA to the U.S. and other jurisdictions based on initial experience with the practical application of the new European rules.

135 Yuntao Bai and others, 'Constitutional AI: Harmlessness from AI Feedback' <http://arxiv.org/abs/2212.08073> accessed 14 August 2023; Kyle Wiggers, 'Anthropic Thinks "constitutional AI" Is the Best Way to Train Models' (*TechCrunch*, 9 May 2023) <https://techcrunch.com/2023/05/09/anthropic-thinks-constitutional-ai-is-the-best-way-to-train-models/> accessed 14 August 2023.

136 Wolfgang Schulz and Christian Ollig, 'Teaching Norms to Large Language Models – The Next Frontier of Hybrid Governance' (*HIIG*, 24 May 2023) <https://www.hiig.de/en/teaching-norms-to-large-language-models/> accessed 14 August 2023.

The Right to Root: Constructing a Claim to Control Devices from the Right to Privacy

by **Ot van Daalen** *

Abstract: Empowering people with digital tools has been an enduring ideal throughout the history of computing. In some of the earlier visions, this was not only a matter of making life easier, it was also a matter of people gaining control over their digital tools. One solution to this problem which has been suggested is to provide users with a manual override to gain full control over a device, something called gaining 'root' – hence the 'Right to Root'. Yet, there are no policymakers who have seriously treated this as a possibility. For people pushing this right at a policy level, it would therefore be helpful to know whether this Right to Root can be constructed from human rights. In this article, I explore the European human rights-based arguments for a Right to Root, focusing on the right to privacy under the European Convention for Human Rights and the Charter of Fundamental Rights. I first discuss the origins of this ideal of gaining control over your own devices. I then show how users over the years have gained less control and how the Right to Root could enable them to regain control. I then explore how the Right to Root could be constructed from the right to privacy under the Convention and the Charter, by understanding it as a way to protect the values of autonomy, self-determination and seclusion. I conclude that a Right to Root can be grounded in the human right to privacy, but that further research is necessary to balance it with other interests, such as cybersecurity, traffic safety, health and intellectual property.

Keywords: Privacy; Self-Determination; Smart Devices; The Right to Root

Recommended citation: Ot van Daalen, The Right to Root: Constructing a Claim to Control Devices from the Right to Privacy 14 (2023) JIPITEC 580 para 1.

A. Introduction [1] [2]

1 Empowering people with digital tools has been an enduring ideal throughout the history of computing. In some of the earlier visions, this was not only a matter of making life easier, it was also a matter of people gaining *control* over their digital tools. But this vision never really materialised. Most of the devices we currently use, from smartphones to cars, are locked down, often collecting private data, while being controlled remotely. This locking down, data collection and remote control is enforced through information security measures – measures which are often difficult, and sometimes illegal to circumvent. As a result, although most people currently own their devices, only few actually control them.

2 One solution to this problem which has been suggested is to provide users with a manual override

1 * Ot van Daalen is assistant professor at the Institute for Information Law of the University of Amsterdam and founder of law firm Root Legal. He can be reached at o.l.vandaalen@uva.nl.

2 This work was supported by the Netherlands Organisation for Scientific Research (NWO), as part of the Quantum Software Consortium programme (project number 024.003.037 / 3368). Elements of this work are part of a PhD which was defended in October 2022: O.L. van Daalen, Making and Breaking with Science and Conscience: The Human Rights-Compatibility of Information Security Governance in the Context of Quantum Computing and Encryption (Van Daalen Press 2022).

to gain full control over a device, something called gaining "root" – hence the "Right to Root."[3] Yet, there are no policymakers who have seriously entertained this as a possibility. For people pushing this right at a policy level, it would therefore be helpful to know whether this Right to Root can be constructed from human rights.

3 This question, however, has received little scholarly attention to date, and most scholars which analysed this topic have done so from a US perspective. US-based Joshua Fairfield suggested in 2017 a "right to hack", based on the concept of ownership, which would also entail giving users the possibility of gaining root, but his analysis is grounded in US law.[4] Ido Kilovaty has argued that people should have the freedom to hack their devices, but this should be so in order to fix vulnerabilities found in these devices.[5] Pam Samuelson has argued that limitations on the "freedom to tinker" hamper competition, innovation and tinkererers' interests, and that this calls for restrictive interpretation of IP rules – but she does not ground this in human rights, and does not explicitly call for a Right to Root.[6] The right to repair, recently gaining traction in US and the EU, is somewhat related to the Right to Root, but it is primarily based on sustainability considerations, not human rights.[7] Finally, Ohm and Kim suggest the right to turn off the "smart" functions of devices; while Hoofnagle, Kesari and Perzanowski analyse some of the issues with "tethered devices" and suggest a "kill switch" – solutions which point in the direction, but fall short of gaining full control over a device.[8]

4 In this article, I explore the European human rights-based arguments for a Right to Root, focusing on the right to privacy under the European Convention for Human Rights (the Convention) and the Charter of Fundamental Rights (the Charter).[9] This exploration involves clearing two significant hurdles. First, it requires connecting the idea of control over devices with the right to privacy – a link which is not necessarily intuitive. Then, it requires support for the claim that freedom requires gaining *full* control, or "root".

5 I attempt to clear these hurdles by first discussing the origins of this ideal of gaining control over

3 See Cory Doctorow, "The Coming Civil War over General Purpose Computing" (August 23, 2012) <https://memex.craphound.com/2012/08/23/the-coming-civil-war-over-general-purpose-computing/> accessed May 28, 2021; Erica Portnoy and Peter Eckersley, "Intel's Management Engine Is a Security Hazard, and Users Need a Way to Disable It" (May 8, 2017) <https://www.eff.org/deeplinks/2017/05/intels-management-engine-security-hazard-and-users-need-way-disable-it> accessed December 28, 2021.

4 Joshua A. T. Fairfield, *Owned: Property, Privacy, and the New Digital Serfdom* (Cambridge University Press 2017), in particular ch. 8.

5 Ido Kilovaty, "Freedom to Hack" (2019) 80 Ohio State Law Journal 455 <https://kb.osu.edu/bitstream/handle/1811/88006/1/OSLJ_V80N3_0455.pdf> accessed March 24, 2023.

6 Pamela Samuelson, "Freedom to Tinker" (2016) 17 Theoretical Inquiries in Law 563.

7 See for example Anthony D Rosborough, Leanne Wiseman and Taina Pihlajarinne, "Achieving a (Copy)Right to Repair for the EU's Green Economy" [2023] Journal of Intellectual Property Law and Practice <https://academic.oup.com/jiplp/advance-article/doi/10.1093/jiplp/jpad034/7147057> accessed May 7, 2023; Aaron Perzanowski, *The Right to Repair: Reclaiming the Things We Own* (Cambridge University Press 2022).

8 See Paul Ohm and Nathaniel Kim, "Legacy Switches: A Proposal to Protect Privacy, Security, Competition, and the Environment from the Internet of Things" (2023) 84 Ohio State Law Journal 59; Chris Jay Hoofnagle, Aniket Kesari and Aaron Perzanowski, "The Tethered Economy" (2019) 87 The George Washington Law Review 783 <https://papers.ssrn.com/abstract=3318712> accessed November 19, 2020; and Christoph B Graber, "Tethered Technologies, Cloud Strategies and the Future of the First Sale/Exhaustion Defence in Copyright Law" (2015) 5 Queen Mary Journal of Intellectual Property 389 <http://www.elgaronline.com/abstract/journals/qmjip/5-4/qmjip.2015.04.02.xml> accessed February 24, 2022. See further Jonathan Zittrain, *The Future of the Internet - and How to Stop It* (Online edition 2009) for an earlier analysis; Rebecca Crootof, "The Internet of Torts: Expanding Civil Liability Standards to Address Corporate Remote Interference" 69 Duke Law Journal 583 on US civil law responses to "remote interference" with the "Internet of Things"; Margot E. Kaminski and others, "Averting Robot Eyes" (2017) 76 Maryland Law Review 983 <https://papers.ssrn.com/abstract=3002576> accessed March 24, 2023 for an analysis of design responses to deal with privacy risks associated with devices in the home; see Christina Mulligan, "Personal Property Servitudes on the Internet of Things" (2016) 50 Georgia Law Review 1121 <https://papers.ssrn.com/abstract=2465651> accessed March 24, 2023 for an analysis of potential responses to contractual and licensing restrictions on these devices; and Scott R Peppet, "Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent" (2014) 93 Texas Law Review 85 for an analysis of risks relating to discrimination, privacy, security and consent and potential responses.

9 This article will not focus on other human rights, such as the right to property and the right to freedom of expression, because they seem less likely candidates for grounding a Right to Root. The principles developed here are, however, also useful when applying those rights.

your own devices, an ideal which visionaries in the seventies of the past century considered to be closely connected to individual freedom. I then show how users over the years have gained less control and how the Right to Root could enable them to regain control. I then explore how the Right to Root could be constructed from the right to privacy under the Convention and the Charter, by understanding it as a way to protect the values of autonomy, self-determination and seclusion. I conclude that a Right to Root can be grounded in the human right to privacy, but that further research would be necessary to balance the Right to Root with other interests, such as cybersecurity, traffic safety, health and intellectual property.

B. The Right to Root: how it started...

6 The story of the Right to Root starts in the sixties and seventies of the past century, around Silicon Valley. Most of the computers at that time were being used in business, the military and academia.[10] There were, however, a number of computer pioneers who focused on what these machines could do to empower ordinary people. One of the people to develop this vision was Douglas Engelbart. Engelbart, born in 1929, decided early in his career that he would focus on augmenting the human intellect in order to enable humanity to cope with the increasing number of complex, yet urgent problems.[11] Computers could play an important role in this; he envisioned these devices as "giving the man maximum facility for directing all [computing] power to his individual task", and as a "very fast symbol-manipulating slave."[12] Another influential visionary from that time, Alan Kay, in 1972 sketched a similar vision for a "Personal Computer for Children of All Ages", which was supposed to also "augment" the learning process.[13]

7 Parallel to this, some people were underlining how computers could be a tool for liberation, not mere augmentation. One magazine for computer hobbyists, called the People's Computer Company, in their first issue of 1972 already suggested that computers have something to do with personal freedom: "Computers are mostly used against people instead of for people, used to control people instead of to *free* them, time to change all that – we need a People's Computer Company."[14] And in 1974, a computer enthusiast named Ted Nelson self-published *Computer Lib/Dream Machines*, a pamphlet which echoed the same vision: "I want to see computers useful to individuals, and the sooner the better, without necessary complication or human servility being required."[15] He wrote the pamphlet "for personal freedom and against restriction and coercion" and concludes with the rallying cry: "Computer power to the people!".

8 The first person, however, to clearly articulate how this freedom also required full control over software and hardware, was Richard Stallman. In the seventies, Stallman was working with one of the few computers in existence at MIT. When he tried to fix an issue with a jamming printer, he discovered that the printer driver was available only in compiled, binary code. This made it difficult for him to solve the jamming problem. The experience set him on a path which eventually resulted in a movement built around the ideal that people should have the *freedom* to run, share, study and change the software they use, because, in Stallman's words:[16]

> Freedom means having control over your own life. If you use a program to carry out activities in your life, your freedom depends on your having control over the program. You deserve to have control over the programs you use, and all the more so when you use them for something important in your life.

9 This idea kickstarted what is now known as the Free Software movement from mid-eighties onward, a movement centered around the vision that

10 See for example on business: James W. Cortada, *IBM: The Rise and Fall and Reinvention of a Global Icon* (The MIT Press 2019); see on academia Steven Levy, *Hackers* (1st ed, O'Reilly Media 2010)

11 Thierry Bardini, *Bootstrapping : Douglas Engelbart, Coevolution, and the Origins of Personal Computing* (Stanford, Calif : Stanford University Press 2000) 10–11 <http://archive.org/details/bootstrapping00thie> accessed May 31, 2022.

12 Ibid 18–19.

13 Alan C. Kay, "A Personal Computer for Children of All Ages" (Xerox Palo Alto Research Center 1972) <https://www.mprove.de/visionreality/media/Kay72a.pdf> accessed June 3, 2022.

14 Bob Albrecht and others, "Epilogue" (1972) 1 People's Computer Company <https://archive.computerhistory.org/resources/access/text/2017/09/102661095/102661095-05-v1-n1-acc.pdf> accessed June 3, 2022.

15 Ted Nelson, *Computer Lib/Dream Machines. New Freedoms Through Computer Screens.* (1974) <https://ia802805.us.archive.org/8/items/computer-lib-dream-machines/Computer%20Lib%2C%20Dream%20Machines%20%E2%80%93%20Ted%20Nelson%20%281974%29.pdf> accessed June 2, 2022.

16 Richard Stallman, "Why Free Software Is More Important Now Than Ever Before" [2013] *Wired* <https://www.wired.com/2013/09/why-free-software-is-more-important-now-than-ever-before/> accessed December 1, 2022.

software should be free as in free speech, not as in free beer. And although the movement initially was concerned with software, it has since then also extended its scope to hardware, because freedom in an information society requires full control over *all* aspects of digital tools.[17] So, what has become of this idea since?

C. ...How it's going

10 Fifty years later, little of this vision has become reality. There was a short period, in the early eighties, when people had a semblance of control. At that time, computers had just become *personal* computers, instead of centrally administered mainframes, to be used also in homes, not yet connected to the internet.[18] These personal computers combined keyboard, processing, storage and screen all in one device – no part of the machine was outside the house. And not only were all these components on one desktop, they could usually be fully administered by the owner. *In theory*: most personal computer users at that time were unable to exploit this power, because they didn't have the necessary expertise, because most of the software was not Free Software as described above, and because some computers also limited what hardware you could connect to it.

11 This temporary semblance of control changed for the worse when personal computers were outfitted with network technologies at some point in the late eighties. People soon started hooking up their personal computers to outside networks, first bulletin board systems, later public networks, eventually resulting in the internet as we know it. This advent of the internet heralded a profound shift in control over digital devices: it not only provided a way for people to connect *to* the outside world, but also provided the outside world with a direct path *into* people's computers.

12 And the outside world made good use of this. This direct path to users' computers enabled two things: collecting data on users, and controlling their devices. As to the collection of data: one of the earliest and still most relevant examples of this is the use of cookies, originally intended to allow a server to recognise a browser when doing things like online shopping, it was quickly repurposed to track people's surfing habits.[19] That, however, was only the beginning. Since then, many more devices have become a computer, and collecting data through these devices has not only became ubiquitous, it has also become much more detailed. If we focus on devices which everyone uses: both dominant smartphone platforms Android and iOS provide fine-grained access to smartphone sensors, enabling them to read information such as the location, camera, files and battery level of the phone.[20] The same with cars: for example, Tesla remotely collects data related to the usage, operation and condition of a vehicle – even using this once to track the whereabouts of a critical journalist.[21] Same for bikes: eBike manufacturers collect information on the speed limit, total distance and battery level of the bike (if you use their app).[22] And the same for fridges, lamps, watches – the list is endless.

13 As noted above, companies are using these remote connections to not only collect data, but also for remote control: to restrict functionality, remove material and in some cases even shut off devices from afar. Lenders in the US have been known to disable the ignition of a car if the owner is late in payments.[23] Similarly, a Ukranian dealer of John

17 See the *Respects your Freedom*-certification programme of the Free Software Foundation which certifies hardware which implements these ideals in hardware: *https://ryf.fsf.org*.

18 See on the history of personal computing Michael Swaine, Paul Freiberger and Brian P. Hogan, *Fire in the Valley: The Birth and Death of the Personal Computer* (Third edition, The Pragmatic Bookshelf 2014).

19 See John Schwartz, "Giving Web a Memory Cost Its Users Privacy" *The New York Times: Business* (September 4, 2001) <https://www.nytimes.com/2001/09/04/business/giving-web-a-memory-cost-its-users-privacy.html> accessed December 2, 2022; Lou Montulli, "The Irregular Musings of Lou Montulli: The Reasoning Behind Web Cookies" (May 14, 2013) <https://montulli.blogspot.com/2013/05/the-reasoning-behind-web-cookies.html> accessed December 2, 2022.

20 See Google, "Android Documentation" (2021) <https://developer.android.com/guide/topics/sensors/sensors_overview> accessed January 5, 2021, sections on Sensors, Location and Performance; Apple, "SRSensor. The Sensors an App Can Read" <https://developer.apple.com/documentation/sensorkit/srsensor#3681604> accessed June 22, 2021

21 Tesla, "Privacy Notice" (2022) <https://www.tesla.com/en_eu/legal/privacy> accessed December 2, 2022; Elon Musk, "A Most Peculiar Test Drive" (February 13, 2013) <https://www.tesla.com/blog/most-peculiar-test-drive> accessed November 18, 2020.

22 VanMoof, "VanMoof Privacy Statement" (2022) <https://www.vanmoof.com/en-NL/privacy> accessed December 2, 2022.

23 Michael Corkery and Jessica Silver-Greenberg, "Miss a Payment? Good Luck Moving That Car" (September 24, 2019) <https://dealbook.nytimes.com/2014/09/24/miss-a-payment-good-luck-moving-that-car/> accessed November

Deere used this functionality to shut down farming equipment stolen by Russia.[24] Tesla disables features of the car remotely, for example when a car changes hands.[25] BMW and Audi announced they can enable certain options, such as seat heating or parking assistance, over the internet – thus also giving them power to disable functionality.[26] And in 2009, Amazon removed copies of Orwell's *1984* remotely from the e-readers of its customers over a copyright claim.[27]

14 While manufacturers gained control over these devices, many of these devices simultaneously are often designed to limit control by the user. All phones from Apple, and most Android phones, only allow the user to access the functionality provided through the default operating system, and install apps via the already provided app stores.[28] Google Nest devices only run approved software through a feature called "verified boot."[29] What's more, attempts to circumvent these restrictions are often actively prevented. iOS updates from Apple have long been designed to block methods to circumvent these restrictions.[30] HP installed a "security update" which started rejecting all third-party ink cartridges five months after installation.[31] Philips has released an update to its smart lamps which blocked lamps not approved by Philips from working.[32] And Tesla detects and centrally logs when people try to upgrade their car themselves without paying for it.[33]

15 Finally, not only are attempts to circumvent these restrictions made more complex: the act of circumvention, and the tools used for circumvention, may also under certain circumstances be unlawful. The European Copyright Directive requires member states to restrict the circumvention of "effective technological measures" and the offering of circumvention tools; US laws contain a similar provision.[34] Most of the technological restrictions

18, 2020.

24 Emma Roth, "Remote Lockouts Reportedly Stop Russian Troops from Using Stolen Ukrainian Farm Equipment" (May 2, 2022) <https://www.theverge.com/2022/5/2/23053944/russian-troops-steal-millions-farm-equipment-ukraine-disabled-remotely-john-deere> accessed May 3, 2022.

25 Aaron Gordon, "People Are Jailbreaking Used Teslas to Get the Features They Expect" (February 1, 2020) <https://www.vice.com/en/article/y3mb3w/people-are-jailbreaking-used-teslas-to-get-the-features-they-expect> accessed November 18, 2020.

26 Tim Stevens, "Your Next BMW Might Only Have Heated Seats for 3 Months" (July 1, 2020) <https://www.cnet.com/roadshow/news/bmw-vehicle-as-a-platform/> accessed November 18, 2020; Audi, "Consistently Connected: Audi Introduces Functions on Demand" (October 7, 2020) <https://www.audi.com/en/company/investor-relations/talking-business/audi-functions-on-demand.html> accessed November 24, 2020.

27 Bobbie Johnson and San Francisco, "Amazon Kindle Users Surprised by 'Big Brother' Move" *The Guardian: Technology* (July 17, 2009) <https://www.theguardian.com/technology/2009/jul/17/amazon-kindle-1984> accessed November 18, 2020. Amazon in response said that it would change the systems so that this could not happen again.

28 It has been reported that Apple is preparing to allow for sideloading, e.g. installling apps via other app store than Apple's: Mark Gurman, "Apple to Allow Outside App Stores in Overhaul Spurred by EU Laws" *Bloomberg.com* (December 13, 2022) <https://www.bloomberg.com/news/articles/2022-12-13/will-apple-allow-users-to-install-third-party-app-stores-sideload-in-europe> accessed December 15, 2022.

29 Google Safety Center, "Google Nest Security & Privacy Features" (2022) <https://safety.google/nest/> accessed December 2, 2022.

30 Chaim Gartenberg, "Apple Releases iOS 13.5.1, Patching Out the Unc0ver Jailbreak" (June 1, 2020) <https://www.theverge.com/2020/6/1/21277281/apple-ios-13-5-1-patch-unc0ver-jailbreak-update-software-install> accessed January 5, 2021; Jenna Wortham, "Unofficial Software Incurs Apple's Wrath" *The New York Times: Technology* (May 13, 2009) <https://www.nytimes.com/2009/05/13/technology/13jailbreak.html> accessed January 5, 2021

31 Cory Doctorow, "Ink-Stained Wretches: The Battle for the Soul of Digital Freedom Taking Place Inside Your Printer" (November 5, 2020) <https://www.eff.org/deeplinks/2020/11/ink-stained-wretches-battle-soul-digital-freedom-taking-place-inside-your-printer> accessed November 18, 2020.

32 Joel Ward, "Philips Hue Excludes 3rd Party Bulbs with Firmware Update" (December 11, 2015) <https://zatznotfunny.com/2015-12/philips-hue-excludes-3rd-party-bulbs/> accessed November 18, 2020.

33 Rob Stumpf, "Tesla Can Detect Aftermarket Hacks Designed to Defeat EV Performance Paywalls" (September 7, 2020) <https://www.thedrive.com/tech/35946/tesla-can-detect-aftermarket-hacks-designed-to-defeat-ev-performance-paywalls> accessed November 18, 2020.

34 Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society 2001 (2001 OJ L 167/10), Art. 6; the new Copyright in the Digital Single Market Directive has retained this provision; Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market and amending Directives

limiting what people can do with their devices should be considered such "effective technological measures", because they restrict access to information or the copying of information without authorisation.[35] There have also been a number of cases where this provision has been used to restrict the sale of devices which remove copy protection measures.[36] Given how broadly these provisions have been interpreted in the past, this could mean that for example an exploit which allows for gaining full control over a phone is considered a product or service intended to circumvent an "effective technological measure" (but may profit from an exemption, see below). And while these rules may have been driven primarily by the desire to protect entertainment material, it is argued that the scope of these rules extends to fields far beyond movies and songs, such as the verification of printer cartridges and keycard systems for locks.[37] That is because it is argued that such systems restrict access to software, and software is protected by copyright as well.

16 Not only do the rules apply to virtually every kind of information with some security measure around it – the rules have a hard time distinguishing between legitimate and illegitimate circumvention. Whether you are breaking encryption to start your illicit filesharing empire, or doing it to share an out-of-copy version of a Shakespeare sonnet with your English teacher, rules prohibiting circumventions and related tools only partly take this into account. To be clear: there is some room for exceptions built into these laws, but it's limited. In the US, explicit exceptions to the circumvention prohibition have been adopted for certain uses in the public interest, such as *jailbreaking* (gaining full control over a device) and information security research, but these are narrowly defined.[38] The EU takes a different route: it prohibits all circumvention, but at the same time obliges member states to ensure that rightsholders under certain circumstances make available to users the means of benefiting from copyright exceptions.[39] This approach has made these exceptions depend on their national implementation, and more importantly, the carve-out is limited in its scope. Take *jailbreaking*: it is by no means certain whether this has a "commercially significant purpose or use."[40]

17 In short, the ideal of users gaining full control over their devices remained just that: an ideal, something which only very few people actually manage to have in practice, and sometimes even involves breaking the law.

96/9/EC and 2001/29/EC 2019 (2019 OJ L 139/92), rec. 7. A similar, but somewhat narrower provision can be found in the Software Directive; Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the Legal Protection of Computer Programs 2009 (2009 L 111/16). These follow from Article 11 of the WIPO Copyright Treaty; WIPO Copyright Treaty 1996. Article 18 of the WIPO Performances and Phonograms Treaty contains a similar obligation; WIPO Performances and Phonograms Treaty 1996. These rules have been transposed in the United States in section 1201 of the Digital Millennium Copyright Act (); Digital Millennium Copyright Act 1998.

35 The Court of Justice in *Nintendo* (2014) has ruled that "the concept of 'effective technological measures' is defined broadly", which also complies with the principal objective of the directive, which is to establish a high level of protection in favour authors; *Nintendo / PC Box* [2014], par. 27.

36 See for example ibid; *Nintendo modchips* [2010]; *Kabushiki Kaisha Sony Computer Entertainment Inc v Ball (Application for Summary Judgment)* (2004) [2004] EWHC 1738 (Ch); *Nintendo Co Ltd v Playables Ltd* [2010] [2010] EWHC 1932; *TubeBox* [2012].

37 In its litigation against the disclosure of vulnerabilities regarding the Mifare-chip in the Netherlands also relied on this provision, but the district court did not consider it proven that the algorithm in question was protected by copyright; *NXP / RUN (Mifare-chip)* [2008]; see Samuelson (n 5) for a discussion of US case law.

38 See U. S. Copyright Office, "Joint Study of Section 1201(g) of the Digital Millennium Copyright Act" (May 2000) <https://www.copyright.gov/reports/studies/dmca_report.html> accessed October 30, 2019 where it was concluded at that time that particular language to protect encryption research was premature; and Joseph P Liu, "The DMCA and the Regulation of Scientific Research" 18 38 where it was argued that encryption research needed better protection. The US Library of Congress in 2015, 2018 and 2021 provided for an exemption on the circumvention prohibition for "good-faith security research"; Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies 2021 201.40. The US Library of Congress also provided for exceptions protecting other public interests, such as circumvention for assistive technologies for blind people and for educational use.

39 Copyright Directive, Art. 6(4); see for the impact of these provisions on information security research Ot van Daalen, "In Defense of Offense: Information Security Research Under the Right to Science" (2022) 46 Computer Law & Security Review 105706 <https://linkinghub.elsevier.com/retrieve/pii/S026736492200053X> accessed July 11, 2022.

40 For example, the wording "commercially significant purpose or use other than to circumvent the technical protection" can be found in section 1201(a)(2) and 1201(b) of the as well, and the legislative history of those provisions suggests that "purpose or use" should be read together; Register of Copyrights, "Section 1201 of Title 17 A Report of the Register of Copyrights" (United States Copyright Office 2017), p. 14.

D. Enter the Right to Root

18 As a result, there have been a few calls for allowing users to gain root over the devices. In the beginning of this millenium, the first seeds for such an idea were planted in the context of a debate around the human rights implications of "trusted computing" infrastructure. At that time, Microsoft was working on hardware which could be used to approve software to run on a computer, ostensibly to improve user security. But security-expert Ross Anderson in 2002 suggested that this infrastructure could be used for removing or blocking software and other kinds of information on a computer remotely for all kinds of reasons.[41] The Free Software Foundation for the same reason was worried that it would affect the freedom of users to run the software they chose.[42] This discussion eventually died down, probably because of the pushback Microsoft received.

19 However, digital rights activist Cory Doctorow rekindled the discussion in 2012, when he gave a speech on the "coming civil war over general purpose computing."[43] This was at a time when "Trusted Party Modules" (TPMs) were starting to be installed in computers – in essence the same technology Microsoft was working on almost a decade earlier. TPMs are hardware chips which generate, store and process cryptographic keys "securely", that is, in line with the security policy set out by the designer of the system.[44] One application of TPMs is to check whether the software booting up the computer, the bootloader, has not been tampered with. If the TPM can confirm that the bootloader is intact, this provides a foundation of trust, which allows other software started up by the bootloader to be trusted as well. This means that whoever controls the TPM, also controls the computer.

20 TPM's as such are not problematic – the question is who gets to control the TPM. If this is, for example, the hardware manufacturer, or the operating system supplier, there is a risk that this control will be used to restrict user freedom, by prohibiting certain software from running on your device. If, on the other hand, the user controls the TPM, they can decide which software to trust.

21 This is not a purely technical question – as Doctorow points out, it has significant human rights implications. If the Chinese government through the use of TPMs can force Apple to block encrypted messaging apps on a phone, this directly affects activists in China, as they would have to move to communications means which are easier to surveil. Similarly, if the European Union can force Google to install software monitoring your conversations, the potential for abuse, chilling effects and wrongful accusations is enormous. And the human rights impact is even more profound when these devices are worn in, or around your body (think of cochlear implants, insulin pumps, bionic eyes and pacemakers).

22 Still, there are also potentially persuasive reasons for not letting owners or users determine what they can do with their devices. Doctorow gives the example of changing the software on self-driving cars, removing speed limits or overriding traffic rules – which could significantly affect traffic safety. And although self-driving cars are not common yet, manually removing speed restrictions from e-bikes is already happening. Another example where it could be problematic to grant users the freedom to run their own software, would be in a corporate environment, where this could lead to security risks.

23 The Electronic Frontier Foundation in 2017 suggested that users should be offered the ability to disable a certain security measure imposed by Intel chips which had the effect of blocking users from patching vulnerabilities.[45] The authors at the same time recognize that there are situations where this may impossible, or where this may pose a security problem in itself – in those cases they would require the possibility to audit, and control which services run on the chip to enable administrators to mitigate security risks. Similarly, US-based academic Joshua Fairfield advocates for a "right to hack."[46] This would entail at a minimum removing tracking devices from things people own, being able to repair these, controlling or stopping forced updates. More generally, it would entail the right to "modify [a device], improve it, sell it, back it up, switch formats or devices, or simply have it accept the owner's commands over those of the manufacturer or rightsholder."[47] This would also

41 Ross Anderson, "Trusted Computing FAQ" (August 2003) <https://www.cl.cam.ac.uk/~rja14/tcpa-faq.html> accessed March 24, 2023.

42 Richard Stallman, "Can You Trust Your Computer?" (2015) <https://www.gnu.org/philosophy/can-you-trust.en.html> accessed March 24, 2023.

43 Doctorow, "The Coming Civil War over General Purpose Computing" (n 2)

44 Microsoft, "Trusted Platform Module Technology Overview (Windows)" (February 17, 2023) <https://learn.microsoft.com/en-us/windows/security/information-protection/tpm/trusted-platform-module-overview> accessed February 24, 2023.

45 Portnoy and Eckersley, (n 2)

46 Fairfield (n 3) ch 8.

47 Ibid 198.

entail permitting users "root access in the device as shipped, and to stop removing root access via over-the-air update". Fairfield does ecognize the tensions with, for example, safety and security, but does not work this out further.[48]

24 Ido Kilovaty has also argued that people should have the freedom to hack their devices, but does not advocate for the possibility to gain root.[49] Pam Samuelson defends the "freedom to tinker", but also does not translate this in a Right to Root.[50] Ohm and Kim's proposal of a "legacy switch" would merely reduce the functionality.[51] The right to repair, recently gaining traction in US and the EU, is somewhat related to the Right to Root, but it is primarily based on sustainability considerations, not human rights.[52] Finally, Ohm and Kim suggest the right to turn off the "smart" functions of devices; while Hoofnagle, Kesari and Perzanowski analyse some of the issues with "tethered devices" and suggest a "kill switch" – solutions which point in the direction, but fall short of gaining full control over a device.[53]

25 Meanwhile, this development is becoming ever more urgent – if only because Windows 11 can only run on computers with a certain TPM.[54] Furthermore, some have recently been ringing the alarm bell about remote attestation, which is a check by an online service provider whether you're running trusted operating system (or software) on your computer, something which also requires TPMs to function.[55]

26 So, an important question is whether you can argue that the Right to Root follows from human rights.

E. How this relates to the right to privacy

27 There are many human rights angles to this question, but I discuss only one: the right to privacy (and data protection). I chose privacy primarily because it is closely related to autonomy, the central concern of those arguing for full control over devices. Other rights could also be useful for supporting a Right to Root – in particular the rights to property and the right to freedom of expression. But the right to property can be restricted through contractual means, and it is questionable to what extent positive obligations can limit such restrictions.[56] The right to freedom of expression is furthermore only applicable to the extent that these devices play a role in freedom of expression, something which is less clear in the case of devices such as thermostats and cars. Nevertheless, I expect the framework developed in this context to be also useful in the context of construction of a Right to Root from the foundation of other human rights.

I. Conceptual frameworks around privacy

28 Before trying to locate the Right to Root in the case law on the right to privacy under the Convention and the Charter, it is useful to consider where the Right to Root fits more generally in the *concept* of privacy. For our purposes, the typology of privacy presented by Koops and others is useful as a location device.[57] The following diagram summarizes their findings:

48 Ibid 225.

49 Kilovaty (n 4).

50 Samuelson (n 5).

51 Ohm and Kim (n 50).

52 See for example Rosborough, Wiseman and Pihlajarinne, (n 0); Perzanowski, (n 0).

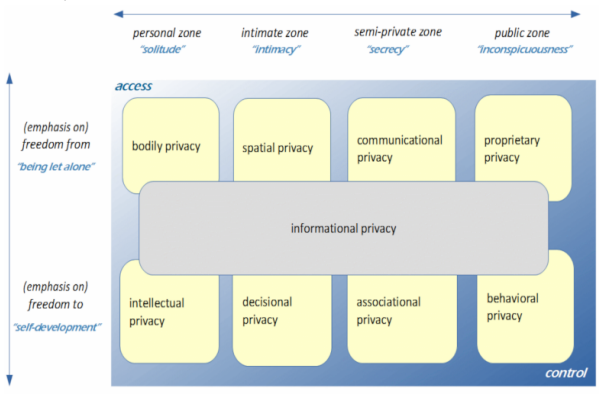
53 See Ohm and Kim, (n 50); Hoofnagle, Kesari and Perzanowski, (n 0); and Graber, (n 0). See further Zittrain, (n 0) for an earlier analysis; Crootof, (n 0) on US civil law responses to "remote interference" with the "Internet of Things"; Kaminski and others, (n 0) for an analysis of design responses to deal with privacy risks associated with devices in the home; see Mulligan, (n 0) for an analysis of potential responses to contractual and licensing restrictions on these devices; and Peppet, (n 0) for an analysis of risks relating to discrimination, privacy, security and consent and potential responses.

54 Microsoft, "Windows 11 Specs and System Requirements | Microsoft" <https://www.microsoft.com/en-us/windows/windows-11-specifications> accessed March 29, 2023.

55 Gabriel Sieben, "Remote Attestation Is Coming Back. How Much Freedom Will It Take?" (July 29, 2022) <https://gabrielsieben.tech/2022/07/29/remote-assertion-is-coming-back-how-much-freedom-will-it-take/> accessed March 24, 2023.

56 See ECHR, "Guide on Article 1 of Protocol No. 1 - Protection of Property" (ECHR 2022), sec. II.C.1.

57 Bert-Jaap Koops and others, "A Typology of Privacy" (2017) 38 University of Pennsylvania Journal of International Law 483 <https://scholarship.law.upenn.edu/jil/vol38/iss2/4>.



29 In their overview, Koops et. al. distinguish two axes. On one axis, they contrast the framing of privacy in negative and positive terms: the right to privacy can be understood to encompass a spectrum, ranging from emphasis on the right to be left alone (negative aspects), to emphasis on self-development (positive aspects).[58] On the other axis, Koops et. al. describe the different domains in which privacy operates, ranging from the private to the public: privacy not only protects activities in private, but also increasingly protects things we do in public.

30 Along the first axis, the Right to Root is located mostly under self-development: it is a way to gain control over devices, a way to extend what you can do with your machines. Logically, if digital tools play an important role in our life, then full control over those tools can further our possibilities for development, and thus our freedom: it enables you to share a book (if you disable digital rights management), to use an alternative app (if you circumvent the official app store), or to drive faster with your bike (if you override speed settings). In other words; of all the goals which privacy aims to protect, the Right to Root is related primarily to the principles of autonomy and self-determination (below I'll discuss case law on this).

31 But if you look more closely, the Right to Root arguably spans this entire axis, not only the self-development aspect of it: it also has a relationship with the right to be let alone – or seclusion – because of the control *others* have over these devices. This control, as discussed above, is about limiting the functionality of devices, disabling them and collecting data via these devices. And gaining full user control over these devices is an important condition for removing the control of others: you can only replace Google's operating system on your smartphone with a version without all the Googly bits, if you first gain control over your device, if you gain "root".

58 See the diagram on p. 482 of ibid.

32 On the second axis, distinguishing between the private and the public domain, the Right to Root is located in the private realm. First, it is about *your* personal devices. Many of these devices are in the *home*, traditionally considered one of the most private places and often explicitly protected in national constitutions. Some of these we take with us continuously – they are in effect an extension of the body, a domain which could be considered even more private. Some are even worn *in* the body – think of digital pacemakers, cochlear implants and insulin pumps. Furthermore, the *information* on the devices is intended to be accessed by the user, not by others: the books you read on your e-reader are part of a private activity, and the smart thermostat in your house displays its readings for your benefit, not for the outside world. Some devices contain your most intimate thoughts – when you keep a diary on your computer for example. And while some of it may be intended for others – for example the email conversation stored on your phone which you were having with your friend – even then: private communications are also considered at the core of the right to privacy.

33 So, to recap: the Right to Root is strongly connected to the values of autonomy, self-development and seclusion as protected under the concept of privacy, and it is located primarily in the private domain. Given this understanding of the Right to Root, the question then is whether the existing case law on the right to privacy under the Convention and the Charter provides support for such a right.

II. The right to integrity and confidentiality of IT systems

34 One intuitive starting point for this inquiry is not found in case law of the Convention and the Charter, but instead in the decision on the right to integrity and confidentiality of IT systems of the German constitutional court. In 2008, the German Constitutional Court reviewed a German law allowing the state to enter computers remotely, and in the context of this law clarified how devices are protected under the right to privacy.[59]

59 See *Online-Durchsuchung* [2008]; Wiebke Abel and Burkhard Schafer, "The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems – a Case Report on BVerfG, NJW 2008, 822" (2009) 6 SCRIPT-ed 106 <http://www.law.ed.ac.uk/ahrc/script-ed/vol6-1/abel.asp> accessed November 23, 2018; Karavas Vaios, "Das Computer-Grundrecht. Persönlichkeitsschutz Unter Informationstechnischen Bedingungen" (2010) 7 Neue Zeitschrift für Sozialforschung 95; see also Mirja Gutheil and others, "Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of

35 In its decision, the Court observed that the fundamental rights to confidential communication, inviolability of the home and informational self-determination currently recognised under the German constitution do not provide sufficient protection against the state searching an IT-system remotely. This is because of the potentially wide-ranging nature of such a search. The Court in response discerned a new fundamental right which protects against "access by the state in the area of information technology also insofar as the state has access to the information technology system as a *whole*, and not only to individual communication events or stored data" (emphasis mine).[60] In other words, it argued that integrity and confidentiality of the *device* is protected under the right to privacy. The German court based this new right under the general "right of personality" under the German Constitution, which serves as a backstop when other rights cannot provide protection. It came to this conclusion firstly because personal computers and other computerised devices have become central to the *development* of personality, especially when they are part of a network.[61] It further argues that these devices also *endanger* personality, partly because of the amount of personal information being processed by them, partly because of how outsiders can gain access to this data.[62]

36 As we will see below, the reasoning of the German court – emphasising how these devices both further individual freedom through their possibilities and restrict freedom through the amount of control they afford to others – can also be found in Convention and Charter case law.

III. The right to privacy under the Convention

37 Of the four distinct concepts protected by the right to privacy under the Convention, private life, correspondence, family life and the home, private life and correspondence are most relevant for this article. The concept of "family life" relates to issues such as marriages and family reunification.[63] The notion of the "home" revolves mostly around themes such as housing, the protection of homes of journalists and lawyers and the environment surrounding a home.[64]

38 As to the notion of "private life": the Court has repeatedly emphasised that it is a broad term not susceptible to exhaustive definition.[65] This is relevant, as it demonstrates that this concept lends itself well to the dynamic interpretation the Court has developed over the years. And the Court has, through this dynamic interpretation, read into the Convention support for the concepts of seclusion, autonomy and self-determination.

39 As a starting point, the Court has in its case law repeatedly noted that the "very essence of the Convention is respect for human dignity and human freedom", also in the context of Article 8.[66] Zooming in on the value of seclusion, it has considered that Article 8 includes "the right to live privately, away from unwanted attention."[67] And it has emphasised

Practices" (Directorate-General for Internal Policies of the European Parliament 2017) Study for the LIBE Committee for an overview of similar laws.

60 *Online-Durchsuchung* (n 58), par. 201.

61 par. 172-174

62 par. 177-180

63 See ECHR, *Guide on Article 8 of the European Convention on Human Rights: Right to Respect for Privacy and Family Life, Home and Correspondence* (Council of Europe 2022) ch III <https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf> accessed October 17, 2018.

64 See ibid IV. Intuitively, one could argue that the fact that something is in the home, as most digital devices are, is a relevant consideration when applying Article 8 of the Convention. The case law does not provide support for this, however. Instead, privacy-related cases with regard to devices in the "home" have been handled under the header of private life and correspondence (see below for an overview). Koops and Hoepman explore how the home could be understood to not only protecting the space between physical walls, but also the space between digital walls, affording functionally equivalent protection to remote storage of private information; See Jaap-Henk Hoepman and Bert-Jaap Koops, "Offering 'Home' Protection to Private Digital Storage Spaces" (2020) 17 SCRIPTed 359 <https://research.tilburguniversity.edu/en/publications/offering-home-protection-to-private-digital-storage-spaces> accessed November 13, 2020.

65 *Niemietz v Germany* [1992], par. 29; *Pretty v The United Kingdom*, par. 61

66 *Christine Goodwin v The United Kingdom* [2002], par. 90; *Pretty v. The United Kingdom* (n 65), par. 65. See later for similar wording; *Bouyid v Belgium* [2015], par. 89; *Svinarenko and Slyadnev c Russia* [2014], par. 138; *El-Masri v The former Yugoslav Republic of Macedonia* [2012], par. 248. As follows from the wording of the Court, human dignity is a concept central to the *entire Convention*, but the above cases demonstrate that it is also central to informing the scope of the protection afforded under Article 8.

67 *Smirnova v Russia*, par. 95; later reiterated in *inter alia Couderc and Hachette Filipacchi Associés v France* [2015], par.

the importance of autonomy, in cases focusing on the right to self-determination (euthanasia, discrimination of transgender people).[68] More recently, the Court has even read into Article 8 "a form of informational self-determination, allowing individuals to rely on their right to privacy as regards data which, albeit neutral, are collected, processed and disseminated collectively and in such form or manner that their Article 8 rights may be engaged."[69] And while these values cannot be connected as easily to the concept of "correspondence", the Court has also interpreted this notion broadly, covering a wide range of media, extending to real-time and stored interception, to content as well as metadata, to professional and personal communications, to interception as well as to the impeding of correspondence.[70]

40 Still, even if the right to privacy under the Convention may in theory protect the values underlying the Right to Root, this is only the beginning of the analysis. The next question is what this means for legal measures in this area: to what extent may the government impinge on the Right to Root, and does it have positive obligations in this regard? Answering these questions is not straightforward. This is because the developments described above are mostly the results of actions by non-state actors, such as device manufacturers and commercial service providers. Thus the case law on negative obligations cannot be applied directly, and instead functions more as inspiration for the development of state obligations under the case law on *positive* obligations under Article 8. I discuss both.

IV. The relevance of negative privacy obligations under the Convention

41 As to the negative obligations under Article 8 of the Convention, the gist of the case law of the Court centers around the risk of abuse of surveillance powers by states. This abuse, according to the Court, can be prevented by clear and proportionate laws, as well as oversight (for example by courts).[71] As to the proportionality, it is firstly important to note for purposes of this article that this hinges on the seriousness of the interference, which in turn has to do with criteria such as the sensitivity and richness of the data involved, the number of people affected, the amount of data processed and the duration of the surveillance.[72] Sometimes, the privacy impact is so great that it does not matter what the risk of abuse is: for example, the "blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences" was considered to be incompatible, regardless of the existence of safeguards against abuse.[73] This is relevant for the analysis under the positive obligations framework, because this case law suggest that when it comes to devices, any interference will quickly deemed to be serious.

42 The Court has also clarified how developing technology can further the risk of abuse. In *Szabó* (2016), the Court warned for example about the potential for abuse, given the "formidable technologies" at the disposal of governments and "the magnitude of the pool of information retrievable by the authorities."[74] It has also repeatedly underlined that the continuously advancing sophistication of surveillance technologies increases the risk of arbitrariness.[75] Furthermore, in *Zakharov* (2015), the

83; *Satakunnan Markkinapörssi Oy and Satamedia Oy v Finland* [2017], par 130; *Bărbulescu v Romania* [2017], par. 70.

68 *Pretty v. The United Kingdom* (n 65), par. 61; *Christine Goodwin v. The United Kingdom* (n 65), par. 90.

69 *Breyer v Germany* [2020], par. 75.

70 See for example *Buglov v Ukraine*; *X V The United Kingdom* [1978]; *Christie v The United Kingdom* [1994]; *Malone v The United Kingdom* [1984]; *Klass and others v Germany*; *Taylor-Sabori v The United Kingdom*; *X And Y V Belgium* [1982]; *Copland v The United Kingdom*; *Bărbulescu v. Romania* (n 66); *Niemietz v. Germany* (n 69); *Wieser and Bicos Beteiligungen GmbH v Austria*; *Iliya Stefanov v Bulgaria* [2008]; *Frérot v France*; *Mehmet Nuri Özen and others v Turkey*; *Halford v The United Kingdom* [1997]; See *Golder v United Kingdom* [1975], par. 43.

71 See e.g. , *Roman Zakharov v Russia* [2015]. for the development of these principles; and *Centrum för Rättvisa v Sweden (Grand Chamber)* [2021], par. 253; and *Big Brother Watch and others v United Kingdom (Grand Chamber)* [2021], par. 339 on proportionality.

72 See for example *S and Marper v United Kingdom* [2008], par. 104; *Breyer v. Germany* (n 68); *Uzun v Germany*; *Szabó and Vissy v Hungary* [2016]; *Weber and Saravia v Germany* [2006]; *Iordachi and others v Moldova*; *Roman Zakharov v. Russia* (n 71); *Uzun v. Germany* (n 71).

73 *S and Marper v. United Kingdom* (n 71), par. 125.

74 *Szabó and Vissy v. Hungary* (n 71), par. 73, 79.

75 *Catt v The United Kingdom* [2019], par. 114; *Big Brother Watch and others v. United Kingdom (Grand Chamber)* (n 74), par. 322; *Centrum för Rättvisa v. Sweden (Grand Chamber)* (n 74), par. 236; *Roman Zakharov v. Russia* (n 71), par. 229; *Szabó and Vissy v. Hungary* (n 71), par. 62; see also the Court in *S and Marper v. United Kingdom* (n 71), which observed that "the protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential

Court examined one particular aspect of this: where the security services and the police have direct technical access to communications and are thus in theory able to circumvent the judicial authorisation procedure, this makes the system particularly prone to abuse, especially since this access is not logged.[76] This is relevant in the context of the Right to Root, because others such as device manufacturers and service providers, often have *direct* access to devices. Although these decisions have been taken in the context of state surveillance, this also gives us an idea on how to assess the far-reaching monitoring and control by others.

43 Technology – and in particular information security measures – can also *mitigate* the risk of abuse, according the Court. In *Big Brother Watch* (2021), the Court for example considered that a state, when transferring intelligence information to other states, must ensure that the receiving state, in handling the data, has "in place safeguards capable of preventing abuse and disproportionate interference.[77] And in *Centrum för Rättvisa* (2021), the Court concluded that, in order to minimize the risk of unlawful access, intelligence services should be obliged to retain logs and a detailed record of each step in bulk interception operations.[78] This is relevant, because it could be argued that the control afforded by the Right to Root is a security measure which could prevent such unlawful access – something which is also discussed in the context of positive obligations below.

V. Positive privacy obligations under the Convention

44 As is well-known, although the object of Article 8 of the Convention is "essentially" to protect the individual against arbitrary interference, the Court has also read into this provision a positive obligation to respect the rights therein.[79] In the context of Article 8, the question is whether member states are under circumstances obliged to take "measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves."[80]

45 Generally speaking, the nature of a positive obligation (and the margin of appreciation) will depend on the particular aspect of the right to privacy which is at issue and the interests at stake.[81] In its case law, the Court has considered it firstly relevant whether "fundamental values" or "essential aspects" of private life are at stake.[82] There is a narrower margin of appreciation where "a particularly important facet of an individual's existence or identity is at stake, or where the activities at stake involve a most intimate aspect of private life."[83]

46 Here, the case law discussed above on the seriousness of the interference in the context of negative obligations provides an idea of where we could look for such fundamental values or essential aspects – think of highly sensitive data, bulk data, continuous control and direct access. Most of the devices to which the Right to Root would extend tick those boxes.

47 Finally, two cases on positive obligations are particularly relevant to the questions discussed here: *I. v. Finland* and *K.U. v. Finland*, where the Court underlined that states have a positive obligation to protect private information against *unauthorised access* by others, by requiring the taking of information security measures.[84] As noted, there is an obvious connection to the Right to Root here, in the sense that one way to prevent data collection is to gain full control. Whether that connection is sufficient to support legislative intervention is something I discuss in the conclusion.

benefits of the extensive use of such techniques against important private-life interests." (par. 112).

76 *Roman Zakharov v. Russia* (n 71), par. 270, 272. On the other hand, in *Kennedy*, the Court considered the fact that there was no evidence of abuse of the powers a reason for considering the measures compatible with Article 8; *Kennedy v United Kingdom*, par. 168.

77 *Big Brother Watch and others v. United Kingdom (Grand Chamber)* (n 74), par. 362.

78 *Centrum för Rättvisa v. Sweden (Grand Chamber)* (n 74), par. 311-316.

79 See *Marckx v Belgium*, par. 31; see in the context of Art. 6 *Airey v Ireland* [1979], par. 25; see further *X and Y v The Netherlands* [1985], par. 23.

80 *X and Y v. The Netherlands* (n 78), par. 23; *Odièvre v France* [2003], par. 40; *Evans v The United Kingdom* [2007], par. 75.

81 See *Hämäläinen v Finland* [2014], par. 66-68.

82 See *X and Y v. The Netherlands* (n 78), par. 27; *MC V Bulgaria* [2003], par. 150 and 153; *KU V Finland* [2008], par. 43 and 46; *IC V Romania*, par. 51 and 52.

83 *Söderman v Sweden* [2013], par. 79; see *Evans v. The United Kingdom* (n 79), par. 77 regarding "a particularly important facet of an individual's existence or identity".

84 *I v Finland* [2008]; *Z v Finland* [1997]; see also *K.U. V. Finland* (n 81), par. 49.

VI. The rights to privacy and data protection under the Charter

48 Since the Charter has come into effect, the Court of Justice has also played a significant role in interpreting the scope of the right to privacy (and data protection). The Charter grants at least the same protection as the Convention, so the European Court of Justice was able to build on decades of case law when it started to apply the right to privacy under Charter. The Charter protects the right to privacy and the right to data protection in separate provisions, Articles 7 and 8 respectively. The Court, however, often discusses these together and the relevance of the right to data protection as an individual ground for constructing the Right to Root is limited, so case law on data protection will not be discussed separately.[85]

49 Similar to the Convention, the risk of abuse of state powers is central to the assessment of negative obligations in the context of surveillance, evaluated on the basis of the objective of an interference, the seriousness of the interference and measures to prevent abuse.[86] This assessment involves aspects such as the number of people affected, the nature of the data, the duration of the measure and whether automated processing is applied.[87] Again, these are all factors pointing to the protection of devices under the right to privacy.

50 In this context, the Court has also investigated the security measures prescribed by the legislature. In *Digital Rights Ireland*, it considered the required security measures insufficient, in particular because they permit providers to take into account economic considerations when determining the level of security they apply.[88] And in *Tele 2* it considered that, given "the quantity of retained data, the sensitivity of that data and the risk of unlawful access to it, the providers of electronic communications services must, in order to ensure the full integrity and confidentiality of that data, guarantee a particularly high level of protection and security by means of appropriate technical and organisational measures."[89] This is relevant, because gaining root over devices is one way to ensure device security.

51 Finally, one aspect relevant in this context is that the European legislator explicitly extended protection to devices through the ePrivacy Directive (in 2002), which required member States to ensure that the storing or gaining access of information on connected devices requires consent.[90] The Directive clarified that these connected devices are "part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms". It further emphasises that "spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users". Later, the EU Court of Justice in *Planet49* also touched on this, acknowledging that it follows from recital 24 of the ePrivacy Directive, that any information stored in the terminal equipment of users of electronic communications networks are part of users' private sphere protected under the Convention, which "applies to any information stored in such terminal equipment, regardless of whether or not it is personal data, and is intended to protect users from the risk that hidden identifiers and other similar devices enter those users' terminal equipment without their knowledge."[91]

F. Conclusion

52 One important takeaway from the case law is that the values of autonomy, self-determination and seclusion which underpin a Right to Root can be found in the case law of the right to privacy under the Convention and the Charter, as well as the right to confidentiality and integrity of IT systems recognised by the German constitutional court. Many devices are considered to fall within the private sphere, regardless of the data tbat it

85 See for example *Bavarian Lager* [2007], par. 118; *Satamedia* [2008], par. 52; *Promusicae* [2008], par. 63; *Volker und Markus Schecke and Eifert* [2010], par. 47; later repeated in *ASNEF* [2011], par. 41; *Schwarz v Bochum* [2013], par. 25 and 26; *Schrems I* [2015], par. 91; *Tele2 Sverige and Watson and Others* [2016], par. 100.

86 See *Digital Rights Ireland and others* [2014]; *La Quadrature du Net* [2020]; *Tele2 Sverige and Watson and Others* (n 85); *Ministerio Fiscal* [2018]; *Opinion 1/15*, par. 149; *Privacy International v United Kingdom* [2020]; *Schrems II* [2020].

87 See for example *Digital Rights Ireland and others* (n 85); *Tele2 Sverige and Watson and Others* (n 85); *Schrems I* (n 86); *SABAM / Netlog* [2012]; *Scarlet / SABAM* [2011].

88 *Digital Rights Ireland and others* (n 85), par. 67.

89 See for similar consideration *Tele2 Sverige and Watson and Others* (n 85), par. 122.

90 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 as Amended by Directive 2006/24/EC and Directive 2009/136/EC 2002, Art. 5(3).

91 *Planet49* [2019], par. 70.

contains. Devices tick many of the boxes relevant to proportionality and necessity assessment under the right to privacy (and data protection), such as the sensitivity and amount of data, as well as whether there is continuous control and direct access to the device.

53 It is also recognised in the case law that security measures are an important way to prevent unlawful access to information in the private sphere, but the courts do not prescribe which measures are most appropriate to mitigate unlawful access – in particular the case law on security measures in the context of the right to privacy does not yet make the connection to the Right to Root.

54 So where does this leave the Right to Root? One conclusion is that the current situation, where rooting might in some cases be illegal, interferes with the right to privacy. One could perhaps even argue that the right to privacy protects anyone who would manually override their device – effectively creating immunity for criminal and civil liability for the act of circumvention. Such an argument would, however, also have to take into account the other interests at stake, including traffic safety (for cars), health (for medical devices) security (for example for company-managed devices) and intellectual property (for DRM).

55 The few policy proposals pointing in the direction of a mandatory Right to Root have not really developed this tension, and further research on resolving this is necessary. This involves, firstly, better understanding *the extent* to which gaining root supports autonomy, self-determination and seclusion in different domains; this may, for example, be less important with regard to a smart thermostats, given their limited functionality, but more important with regard to phones. It also involves identifying the role of restrictions in devices for safeguarding the different interests. For example, to what extent does a speed limit on bikes further traffic safety; to what extent does DRM prevent copyright infringement?

56 Conversely, it involves an understanding of the impact of on these interests when one removes restrictions in systems. One distinction which is probably relevant in this context is between single-user and multi-user systems. For single-user systems, security measures are often intended to protect the system against the user. This can be done for example to restrict the functionality of the device, usually for economic reasons – and these restrictions are usually imposed by a vendor or supplier of a device. This is different for multi-user systems. In multi-user systems, there are good reasons for security restrictions – to prevent people from snooping in files without authorisation, for example, or to prevent them from spending other peoples' money. In this instance, a manual override of security measures would only create a huge security hole, without much gain in individual freedom. These are not the places where the right to privacy should impose a manual override.

The Regulation of Emerging Technologies in Greek Law

by **Antonios Broumas and Paola Charalampous** *

Abstract: The statue 4961/2022 in Greek Law sets out the national framework for the regulation of emerging technologies under conditions of trustworthiness, safety and cybersecurity, consumer protection, respect for fundamental rights and the democratic rule of law.

Part A' of the Law (articles 1-27) aims to establish an adequate institutional framework for the accomodation of the potential of AI by public and private sector bodies under conditions of fairness and security, as well as to strengthen the resilience of the public administration against cyber threats. In the context of serving this purpose, Part A of the Law includes regulations for (a) the development of artificial intelligence, and (b) upgradinginformation security and data protection in the public sector.

Part B of the Law (articles 28-57) aims at the exploitation by the public sector and the private market of the potential unleashed by advanced technologies and the maintenance of good practices, with the ultimate goal of consolidating the digital transformation of the country. For this purpose, Part B of the Law includes regulations regarding (i) the Internet of Things ("IoT"), (ii) Unmanned Aircraft Systems ("UAS"), (iii) distributed ledger, and (iv) 3D printing.

Keywords: Regulation, Emerging Technologies, Greece

Recommended citation: Antonios Broumas and Paola Charalampous, The Regulation of Emerging Technologies in Greek Law, 14 (2023) JIPITEC 594 para 1.

A. Introduction

1 The digital transformation of societies offers both challenges and opportunities, which are relevant to law. Regulatory interventions in relation to technology are mainly triggered by market failures, regulatory gaps, equity / fairness purposes and long-term public policy goals[1].

2 Along these lines, the European Union (EU) has taken a principled prescriptive approach for the regulation of technology, committed to putting people at the centre of the digital transformation, supporting solidarity and inclusion, promoting freedom of choice in a fair digital environment, fostering participation in the digital public space, increasing safety, security and empowerment, ensuring privacy and individual control over data and promoting sustainability[2]. To this end, the Digital Decade Policy Programme 2030 of the European Commission sets out the general objective on a Union level of

* Antonios Broumas is Attorney at Law, Digital Law Lead, EY Law Greece.

Paola Charalampous is Attorney at law, Compliance officer.

1 Jacques Pelkmans; Andrea Renda (2014). How Can EU Legislation Enable and/or Disable Innovation, p. 11.

2 European Declaration on Digital Rights and Principles for the Digital Decade, 2023/C 23/01, 23.1.2023, available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32023C0123(01).

the promotion of a human-centred, fundamental-rights-based, inclusive, transparent and open digital environment where secure and interoperable digital technologies and services observe and enhance Union principles, rights and values and are accessible to all, everywhere in the Union[3].

3 The digital transformation policy of the Greek state is mainly determined by the 2020-2025 Digital Transformation Bible issued by the Ministry of Digital Governance in June 2021[4]. The Bible sets out general principles for national policy making, which have also been adopted at statutory level by virtue of article 3 of the Framework Law 4727/2020 on digital governance[5]. Even though these principles primarily refer to the deployment of technology in the public sector, the Bible also provides for principles relevant for regulatory interventions in respect of emerging technologies, such as the principles of equality, trustworthiness and trust, openness and transparency, integrity, security and confidentiality.

4 In this context, on 27 July 2022, the Greek Law 4961/2022 "on emerging information and communication technologies, the reinforcing of digital governance and other provisions" was published and set in force[6], except for the provisions regarding artificial intelligence, which entered into force on 1 January 2023, and the provisions regarding Internet of Things devices, which entered into force on 1.3.2023.

5 The new Law sets out the national framework for the regulation of artificial intelligence ("AI"), the Internet of Things (IoT), the provision of postal services using Unmanned Aircraft Systems ("UAS"), the use of distributed ledger technologies ("DLT") and the conclusion of smart contracts, as well as the protection of works of three-dimensional printing ("3D Printing").

3 European Commission (2022). Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030, OJ L 323, 19.12.2022, p. 4–26, available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022D2481.

4 Greek Ministry of Digital Governance (2021). 2020-2025 Digital Transformation Bible, available: https://digitalstrategy.gov.gr/website/static/website/assets/uploads/digital_strategy.pdf.

5 Greek Government Gazzette 184/A/23-09-2020, available: https://www.et.gr/api/DownloadFeksApi/?fek_pdf=20200100184.

6 Greek Government Gazzette 146/A/27-07-2022, available: https://www.et.gr/api/DownloadFeksApi/?fek_pdf=20220100146.

B. Background, Purpose & Scope

6 Law 4961/2022 regulates the utilization and use of a basic set of contemporary emerging technologies with significant economic and social impact. It thus lays down the conditions for the rapid adoption and development of these technologies in Greek economy and society, with the ultimate goal of promoting the country's digital transformation.

7 In terms of scope, the new Law enacts vertical obligations for providers of products and services related to AI, IoT and UAS in the transport industry, and horizontal requirements for the use of AI and 3D printing, while laying the foundations for conducting transactions with DLTs and smart contracts.

8 In this respect, the Law introduces prescriptive statutory interventions in areas which have been deemed by the Greek legislature as constituting regulatory gaps producing sub-optimal outcomes in relation to public policy objectives, such as the protection of end-users, the promotion of innovation and the resilience of key emerging technologies vis-à-vis cyber-risks.

9 The purpose of Law 4961/2022 is, on the one hand, the lawful, safe and secure development, deployment and use of AI technologies by public and private entities and, on the other hand, the accommodation of the potential of IoT, UAS, DLT and 3D Printing for the public sector and the market[7].

10 The provisions of Law 4961/2022 unfolds in four parts, which concern, among other things, the digital upgrade of public administration (Part A') and the utilization of emerging technologies by public bodies and private entities (Part B').

11 In specific, Part A' of the Law (articles 1-27) aims to establish the adequate institutional framework for the exploitation of the potential of AI by public and private sector bodies under conditions of fairness and security, as well as to strengthen the resilience of the public administration against cyber threats. In the context of serving this purpose, this part includes regulations for (a) the development of artificial intelligence, and (b) the upgrade of information security and data protection in the public sector.

12 Furthermore, Part B of the Law (articles 28-57) aims at the exploitation by the public sector and the private market of the potential unleashed by advanced technologies in line with good practices, with the ultimate goal of consolidating the digital transformation of the country. For this purpose, Part B of the Law includes regulations regarding (i) the Internet of Things ("IoT"), (ii) Unmanned Aircraft

7 See articles 1 and 30 of Law 4961/2022.

Systems ("UAS"), (iii) distributed ledger, and (iv) 3D printing.

C. The Greek Legal Framework for the Regulation of AI

13 The application of artificial intelligence ("AI") technologies is expected to transform the economy, work and society in general. Still, the provision, deployment and use of AI systems raises serious ethical issues[8], whereas it also poses risks for fundamental rights, the safety and security of persons and property and the democratic rule of law[9].

14 Taking into account the forthcoming adoption of the Artificial Intelligence ("AI") Act by the European Union ("EU")[10], the Greek Law 4961/2022 introduces supplemental national provisions for the regulation of AI use in the Greek public and private sectors. In respect of coherence, the Greek law does not generally overlap with the subject matter of the forthcoming AI Act, by regulating (i) the deployment of AI in the public sector; (ii) the use of AI in the private sector with specific requirements related to ethical use and the protection of employees.

15 The national framework follows a prescriptive "risk-based" approach for the regulation of AI in line with the proposed AI Act, enacting the following obligations per category of obligated entities:

I. AI in the Public Sector

16 Provision by Statute: Except for the Ministries of National Defense and Citizen Protection, the use of AI systems is permitted only by a special provision by statute, which includes appropriate safeguards for the protection of the rights of natural or legal persons affected by these systems[11].

17 Algorithmic Impact Assessment: Before deploying AI systems, in addition to performing a data protection impact assessment of Regulation (EU) 2016/679 ("GDPR"), public bodies shall have the obligation to execute algorithmic impact assessments in order to evaluate the risks that may arise to the rights, freedoms and legitimate interests of the persons affected by such AI systems[12]. Appropriate safeguards for the protection of the rights of persons affected by the use of AI systems shall be further specified through the issuance of a Presidential Decree[13].

18 Operational Transparency: Each public body shall publicly disclose information, inter alia, about the commencement of operation and the operating parameters of any AI systems deployed as well as on the decisions taken or supported through them. Any complaints by affected persons on violations of transparency obligations shall be examined by the National Transparency Authority[14].

19 Register of AI Systems: Each public body shall maintain a register of the AI systems it uses[15].

II. AI in the Private Sector

20 AI in the Employment Context: Prior to the deployment of an AI system, which affects the decision-making process concerning employees, existing or prospective, and has an impact on their conditions of employment, selection, recruitment or evaluation, private entities shall provide relevant information to the employee. This obligation also applies to digital platforms in respect of natural persons linked to them by employment or independent service contracts or project agreements. For any violation of this obligation, the Labor Inspectorate may impose monetary sanctions[16].

8 European Commission High-Level Expert Group on AI ("AI HLEG"), Ethics Guidelines for Trustworthy Artificial Intelligence, 8 April 2019, available: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419.

9 OECD Working Party and Network of Experts on AI, Advancing accountability in AI, Governing and managing risks throughout the lifecycle for trustworthy AI, February 2023, No. 349, available: https://www.oecd-ilibrary.org/deliver/2448f04b-en.pdf?itemId=%2Fcontent%2Fpaper%2F2448f04b-en&mimeType=pdf.

10 European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act), COM/2021/206 final, available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206.

11 See article 4 of Law 4961/2022.

12 The institution of the algorithmic impact assessment of the Greek Law 4961/2022 draws elements from the corresponding institutions established in the Canadian Directive on Automated Decision Making and the US 2022 Algorithmic Accountability Act (H.R. 6580).

13 See article 5 of Law 4961/2022.

14 See article 6 of Law 4961/2022.

15 See article 8 of Law 4961/2022.

16 See article 9 of Law 4961/2022.

21 Ethical Use of Data: Any medium- or large-sized undertakings within the meaning of article 2 of Law 4308/2014[17], shall be obliged to adopt a policy for the ethical use of data, which includes information on the measures, actions, and procedures they apply to data ethical issues when using AI systems. In addition, entities obliged to issue corporate governance statements in accordance with article 152 of Law 4548/2018, must include in it information about their data ethics policy. The content of such policies shall be further specified through the issuance of a Joint Ministerial Decision[18].

22 Record of AI Systems: Any medium- or large-sized undertakings within the meaning of article 2 of Law 4308/2014 shall maintain a record of the AI systems deployed[19].

III. AI & Public Procurement

23 Finally, the new Law establishes the following national requirements for public procurement procedures for the design or development of AI system[20]:

24 i. The contractor shall furnish the contracting authority with information necessary to fulfil its transparency requirements on AI system operation stipulated in the Law;

25 ii. The AI system shall be delivered in such a way so that the contracting authority be able to study its mode and parameters of operation, to further improve it and to publish or make available, in any way, those improvements; and

26 iii. Appropriate measures will need to be taken to bring the AI system in line with applicable laws, in particular, regarding the protection of human dignity, the respect for private life and the protection of personal data, non-discrimination, equality between women and men, freedom of expression, universal access for persons with disabilities, workers' rights, and the principle of good administration.

27 It is explicitly stipulated that the provisions of Law 4961/2022 on AI technologies do not affect the rights and obligations provided for in the GDPR and supplementary Law 4624/2019 on the protection of personal data.

28 Finally, the new Law establishes, on the one hand, a Coordinating Committee for AI with responsibilities for the drafting of the National Strategy for AI and, generally, the formulation of policy around AI and, on the other hand, a Committee for the supervision of the strategy, which ensures the implementation, the coordination of the competent bodies and manages its enforcement.

29 To carry out their work, the two committees receive data and know-how from the national AI Observatory, also established by the Law, which has the duty to monitor and report on technological developments and policies around AI in the country and at an international level.

D. Provisions on Information Security & Data Protection

30 Law 4961/2022 further establishes the following institutions for shielding the country against threats related to information and network security[21]:

31 The General Directorate of Cybersecurity of the Ministry of Digital Governance is designated as the National Cybersecurity Certification Authority in accordance with article 58 of Regulation (EU) 2019/881. Ministerial decisions shall define the monitoring procedure and the bodies assessing the products, services and ICT procedures vis-a-vis the requirements of European cybersecurity certificates, as well as the relevant sanctions in case of non-compliance.

32 The Ministry of Digital Governance establishes the Hybrid Threat Analysis Observatory, i.e. the advisory body of the National Cybersecurity Authority with responsibility related to the analysis and prevention of hybrid threats in the field of cybersecurity.

33 The General Directorate of Cybersecurity of the General Secretariat for Telecommunications and Post of the Ministry of Digital Governance is designated as the national coordination center as per Article 6 of Regulation (EU) 2021/887.

34 In each central government body, an Information and Communication Systems Security Officer ("ICSSO") is

17 According to the respective provisions of Law 4308/2014, medium-sized undertakings are those which fulfill two or more of the following criteria: (i) 250 employees, (ii) a turnover of up to €40 million and (iii) a net balance sheet total of up to €20 million. For large-sized undertakings the respective criteria increase up to: : (i) 250 employees, (ii) a turnover of up to €40 million and (iii) a net balance sheet total of up to €20 million

18 See article 10 of Law 4961/2022.

19 See article 10 of Law 4961/2022.

20 See article 7 of Law 4961/2022.

21 See articles 3-26 of Law 4961/2022.

appointed, with the task of supervising the security of the entity's network and information systems and ensuring the issuance of a risk analysis plan and the security policy of the Body's ICT systems.

35 Each public body having a critical infrastructure also designates a Security Coordinator, who carries the duties of the ICSSO for this particular infrastructure.

36 Regulation 2019/881 on ENISA (the European Union Agency for Cybersecurity) created a European Union-wide cybersecurity certification scheme in the field of information and communication technology and strengthened ENISA by defining its specific role and responsibilities. The General Data Protection Regulation focuses on "Data Protection by Design", where components related to both privacy and security meet, whereas the European Regulation on Cybersecurity focuses on "Security by Design", which enables the products' designers and constructors to receive the relevant certification and consequently strengthens the public confidence in the above products and services[22].

37 As per the new Law, providers of public electronic communication networks are required to have in place and align with an information security risk assessment plan, which they shall update on an annual basis. Also, a procurement plan in relation to the equipment obtained and the participation of third-party suppliers.

38 Finally, a register of data protection officers of public sector bodies is established as well as a relevant committee for the exchange of expertise and cooperation with ISDPS.

E. The Greek Legal Framework for the Regulation of IoT

39 According to the European Commission, "machine-generated data is created without the direct intervention of a human by computer processes, applications or services, or by sensors processing information received from equipment, software or machinery, whether virtual or real"[23].

40 Machine-generated data can be both personal or non-personal in nature. Machine-generated data that may result in the identification of an individual qualify as personal data, as in the case of data generated by wearable devices[24].

41 Law 4961/2022 sets out a comprehensive framework of national rules for the cybersecurity of Internet of Things ("IoT") devices through the enactment of primary statutory provisions and secondary administrative rules. The Law also establishes the National Cybersecurity Authority as the authority competent for the supervision and implementation of its rules.

42 According to the definitions of Law 4961/2022, IoT means any technology that[25]:

(a) allows devices or a group of interconnected or related devices, through their internet connection, to perform automatic processing of digital data; and

(b) enables the collection and exchange of digital data, in order to offer a variety of services to users, with or without human participation.

43 Law 4961/2022 imposes legal obligations on both manufacturers and importers / distributors and, also, operators of IoT devices[26].

44 According to the provisions of the new Law, manufacturers are required to accompany IoT devices with a declaration of compliance with the technical safety specifications, indicated in the law, as well as instructions for use and information on safe use.

45 In addition, each manufacturer is obliged to have a management process in place in relation to its IoT devices, in cases where it is ascertained by the user that: a) a security incident occurs, or b) a vulnerability exists in the security parameters of the device. This process should include appropriate documentation by the manufacturer about the nature and possible forms of occurrence of the security incident or the vulnerability, detailed instructions for dealing with them, as well as indicative measures to mitigate potential adverse consequences.

46 Importers and distributors are required to verify that the IoT devices they import or distribute are accompanied by a relevant declaration of compliance, as stipulated in the new Law, refrain from further import or distribution in case of absence and cooperate with competent public authorities for

22 A. Michailaki, Law and Ethics in the applications of augmented reality, Nomiki Vivliothiki, 2022, p. 24-25.

23 European Commission, Communication on "Building a European Data Economy, COM/2017/09 final, available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:9:FIN.

24 I. Igglezakis, "The Law of the Digital Economy", 2022, Sakkoula Publications, p. 52.

25 See article 31 of Law 4961/2022.

26 See articles 32-35 of Law 4961/2022.

matters of compliance with the provisions of the Law.

47 On the other hand, operators of IoT devices are obliged to follow the technical safety specifications of the devices they deploy and use. They should also appoint an IoT Security Officer to monitor the security measures of their devices. Furthermore, they are required to maintain a register of IoT devices, updated on an annual basis and, each time they put into service a new IoT device. Finally, each IoT operator should carry out an impact assessment of the planned personal data processing operations related to the operation of the IoT technology device.

48 The National Cybersecurity Authority is appointed as the competent authority to oversee the implementation of the national IoT security framework[27]. The Authority has the power to:

49 Require from manufacturers, importers, or distributors of IoT devices to take all necessary corrective actions in order to comply with the applicable legislation.

50 Order the temporary withdrawal from the market of IoT appliances presenting risks and their replacement in the market only if such risks have been removed.

51 Upon the Authority's recommendation, the competent body of the Ministry of Digital Governance may impose penalties of up to € 15,000 and, in case of relapse, of up to € 100,000 on non-compliant manufacturers, importers, distributors and operators.

52 Forthcoming ministerial decisions shall specify the technical specifications and safety measures of IoT devices, the obligations of manufacturers, importers, and suppliers of such products as well as the relevant sanctions in case of non-compliance.

53 It should be stressed that, to the extent that generated data constitutes personal data, providers and operators of IoT devices shall also be obliged to ensure a level of security appropriate to the risk by implementing appropriate technical and organizational security measures in line with article 32 of the GDPR[28]. Furthermore, should generated data also constitute communications and related traffic data, providers and operators of IoT devices shall be obliged to comply with the provisions of article 4 of Law 3471/2006 on the confidentiality of communications, transposing Directive 2002/58/EC into Greek law.

F. Provisions on the Use of UAS in the Context of Postal Services

54 With the aim of promoting innovation through the emerging technology of UAS in the postal sector, the new Law 4961/2022 lays down a set of rules facilitating the adoption of UAS technologies by postal service providers in conditions of legal certainty and clarity.

55 In specific, articles 43-46 of Law 4961/2022 amend the respective provisions of Greek Framework Law 4053/2012 on Postal Services[29], by introducing rules on the use of Unmanned Aircraft Systems ("UAS") in the postal sector.

56 The new Law explicitly stipulates that the provision of postal services, for which a general or special permit has been granted, in all or part of the Greek territory, may be carried out using UAS, subject to approval by the National Telecommunications and Post Commission ("NTPC")[30].

57 The use of frequencies by UAS for the provision of postal services shall be governed by the Delegated Regulation (EU) 2019/945 and the Implementing Regulation (EU) 2021/664[31].

58 According to the new Law, the technical characteristics and safety specifications of UAS used for the provision of postal services, as well as any other relevant issue, shall be specified through a decision issued by the Minister of Digital Governance, following an opinion of the NTPC and the Civil Aviation Authority[32].

27 The General Directorate of Cyber Security, part of the General Secretariat of Telecommunications & Posts of the Ministry of Digital Governance, has been designated as the National Cybersecurity Authority of Greece. The official website of the Authority is available here: https://mindigital.gr/dioikisi/kyvernoasfaleia.

28 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).

29 Greek Government Gazzette 44/A/07-03-2012, available: https://www.et.gr/api/DownloadFeksApi/?fek_pdf=20120100044.

30 See article 45 of Law 4961/2022.

31 See article 46 of Law 4961/2022.

32 See article 45 of Law 4961/2022.

G. The Greek Legal Framework for the Regulation of DLT & Smart Contracts

59 At EU level, distributed ledger technologies ("DLTs") are already regulated by the MiCA[33] and DLT[34] Regulations. The national provisions of Law 4961/2022 complement these Regulations, by only regulating the applications of DLTs in smart contracts. In particular, the new Law 4961/2022 incorporates general rules for the validity and force of proof of smart contracts in a future-proof manner in order to promote the deployment and use of respective general-purpose technological solutions in the country.

60 Statue 4961/2022 defines "distributed ledger" as the repository of information that maintains records of transactions, and which is shared and synchronized between a set of DLT network nodes, using a consensus mechanism[35].

61 Furthermore, a blockchain is defined as a special type of distributed ledger technology that records data in blocks, which are connected to each other in chronological order and form a chain of a consensual, decentralized and mathematically verifiable nature, which is mainly based on the science of cryptography[36].

62 The foregoing definitions are fully aligned with the respective definitions of DLT and in article 3 of the MiCA and article 2 of the DLT Regulations.

63 Statue 4961/2022 goes forward to define a smart contract as a set of coded computer functions, which is finalized and executed through distributed ledger technology in automated electronic form through instructions for the execution of actions, omissions, or tolerances, which are based on the existence or not of specific conditions, according to terms recorded directly in electronic code, scheduled commands, or programmed language[37].

64 In smart contracts, trust in the person of the counterparty is replaced by trust in the very system of blockchain technology to which they belong. Because of the technical guarantees it provides, that system is presumed not to make any errors. The nature and role of participants in the DLT ecosystem determines their legal liability for any damage caused by their acts or omissions[38].

65 The new law lays down the foundations for the validity of smart contracts executed within the jurisdiction of Greece. According to its provisions, the recording of data or the execution of contracts may be freely conducted through a blockchain or other DLT, rendering valid the declarations of will exercised in such a form[39]. Smart contracts bind contracting parties as per the general provisions of the Greek Civil, including its provisions on invalidity of private contracts or declarations of will[40].

66 The provisions of Law 4961/2022 also stipulate that the submission of information or data about smart contracts executed through blockchain or other DLT fulfills the legal concept of private document[41] and suffices as valid proof for their execution before national courts. An official expert report may also be submitted for the verification of the transposition of the respective software code into text[42].

33 Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937, available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1114.

34 Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology, available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R0858.

35 See article 31 of Law 4961/2022.

36 See article 31 of Law 4961/2022.

37 See article 31 of Law 4961/2022.

38 L. Kanellos, 'Smart Contracts: Legal challenges and business prospects', Nomiki Vivliothiki, 2021, p. 163.

39 See article 47 of Law 4961/2022.

40 See articles 130, 138, 159, 174-179 and 140-157 respectively of the Greek Civil Code.

41 According to article 445 of the Greek Code of Civil Procedure, private documents, drawn up in accordance with the law, if their authenticity has been recognized or proved, constitute valid evidence that the statement they contain originates from the issuer of the document, but counter-evidence is permissible. Under the same conditions, private documents constitute valid evidence as to the content of declarations of will.

42 See article 51 of Law 4961/2022.

H. The Greek Legal Framework for the Regulation of 3D Printing

67 The Greek framework Law 2121/1993 on copyright does not include specific provisions for the regulation of authors' rights in relation to 3D printing designs and works. In this context, the Greek legislature has prioritized the adequate protection of intellectual property rights in this area as means to promote the unencumbered production, distribution and consumption of respective works of authorship. To this end, articles 53-57 of Law 4961/2022 set out the national framework for the regulation of the copyright law implications of 3D printing.

68 3D printing may be defined as the additive manufacturing technique by which, through successive deposition of successive layers of material, three-dimensional objects are made. This method has wide use in the production of spare parts and application in architecture, medical technology, weapons industry, industrial technology, etc[43].

69 In the new Law, "3D Printing" is defined as the process of uniting 3D printing materials through the technique of prosthetic successive stratification of such materials by using new technologies, especially 3D printers, and aiming on printing a physical object based on a digital model[44].

70 The new Law introduces the following amendments to Greek Framework Law 2121/1993 on copyright regarding works of speech on 3D printing[45]:

71 Any Computer Aided Design File (C.A.D. File) is explicitly characterized as a protected work of speech, as long as it includes a source code.

72 3D printers are expressly subject to a 4% private levy on their value for the benefit of authors and right-holders of neighboring rights.

73 Moreover, the new Law prohibits the use, sharing and hosting on online platforms of digital models or digital design files with the help of a computer or digital files of a typical triangle language or digital model design databases, without the prior permission of their right-holder[46].

74 As an exception, such acts are lawfully conducted without the permission of their right-holder if they are carried out solely for: (a) private, judicial or administrative use; (b) use for the benefit of persons with disabilities; (c) use for temporary or ancillary phases of a technological process that do not have independent economic significance; d) the fulfillment of educational or research purposes; (e) news purposes; or (f) the use of images or objects in public places or exhibitions in museums or in exhibits catalogues, provided that, in the above cases, the normal utilization of the work or other protected subject-matter is not affected and the legitimate interests of the author or the rightful owner are not unduly prejudiced.

75 The new Law also provides for the liability of online platform providers, through which digital models or digital files, without source code related to the 3D printing process, are used, shared, or hosted, in cases that, after becoming aware of the infringement, they do not take all necessary measures to remedy it[47].

76 Finally, the new Law establishes the liability of the creator or legal owner or seller, as the case may be, towards consumers for defective digital models or files related to the 3D printing process or three-dimensional printed objects or three-dimensional printers or scanners.

I. Critical Evaluation of the Greek Legislation on Emerging Technologies

77 According to well-established practices, the regulation of technology ought to be comprehensive, coherent, proportionate, evidence based, fit for purpose, future-proof and open to innovative solutions in a context of ever more rapid technological, societal and environmental change[48].

78 The subject-matter of the Greek Law 4961/2022 is focused on specific technologies, which have been held as "emerging" technologies of significant economic potential and social impact. The two-fold purpose of the Law is the constitution of an institutional environment appropriate, on the one hand, for the diffusion of the use of such technologies in Greek society, to accommodate innovation and facilitate digital transformation, and, on the other

43 M. Milapidou, 'New Technologies in Health: Medical, Legal and Ethical Issues', Nomiki Vivliothiki, 2021, p. 94.

44 See article 31 of Law 4961/2022.

45 See article 53 of Law 4961/2022.

46 See article 54 of Law 4961/2022.

47 See article 55 of Law 4961/2022.

48 European Commission Staff Working Document (2021). Better Regulation Guidelines, Brussels, 3.11.2021, SWD(2021) 305 final, p. 8, available: https://commission.europa.eu/document/download/d0bbd77f-bee5-4ee5-b5c4-6110c7605476_en?filename=swd2021_305_en.pdf.

hand, the pre-emption of possible harms or sub-optimal outcomes arising from these technologies (e.g. cyber-threats). In respect of AI regulation, the Law also employs a proportionate approach, imposing obligations only to medium- or large-sized undertakings. Furthermore, the Law establishes a robust institutional framework for the supervision of most of its requirements related to cybersecurity and AI.

79 Taking into account its Explanatory Statement, the Greek Law on emerging technologies appears to employ a patchy, rather than systematic, approach for the regulation of emerging technologies, by addressing certain regulatory gaps in the Greek legal order in relation to specific technologies. Furthermore, the choice of these technologies as the subject matter of regulation or the identification of respective gaps does not seem to arise on the basis of an evidence-based approach, thus running the risk of missing technologies or gaps that also require regulation due to their potential or impact. Furthermore, the Law is not the solid outcome of a comprehensive national innovation strategy and, therefore, falls short of a systematic and holistic approach to accommodate the potential of emerging technologies and effectively boost the digital transformation of the public and private sectors. Finally, the possible overlaps of the provisions of the Law with already adopted or forthcoming EU legislation, especially the AI Act, the Data Governance Act[49] and the NIS 2 Directive[50], may result in lack of regulatory coherence or over-regulation.

80 Overall, Law 4961/2022 constitutes a distinct national approach to the regulation of emerging technologies in the member-states of the European Union, with innovative national provisions that may be appropriate for other national jurisdictions.

J. Conclusion

81 Artificial intelligence is a rapidly evolving technological field that is expected to radically transform major aspects of Greek society, such as the economy, health, as well as entrepreneurship and innovation. In addition, the Internet of Things is at the core of the fourth industrial revolution, offering solutions in many areas of economic and social life, such as extremely fast response services, reliable remote solutions, using applications with greater ease, decision support, better resource allocation and remote control of services. Furthermore, the use of Unmanned Aircraft Systems in postal services presents advantages in terms of environmental protection (smaller environmental footprint) and access to critical or island areas, as well as areas with difficult access. Accordingly, the lack of regulation in respect of distributed ledger technologies results in legal uncertainty for innovative businesses and acts as disincentive for attracting investment, while at the same time the potential of these technologies remains untapped. Finally, the diffusion of 3D Printing technologies across business sectors requires the protection of respective intellectual property rights[51].

82 The provisions of Law 4961/2022 establish a national regulatory framework aspiring to promote these emerging technologies in Greece under conditions of trustworthiness, safety and cybersecurity, end-user protection, respect for fundamental rights and the democratic rule of law. Yet, the Law falls short of constituting a comprehensive national approach to the regulation of innovation. It therefore, remains to be seen whether the provisions of the new Law will contribute to technological innovation and result in a positive impact on the overall digital transformation of the public and private sectors of the country.

49 European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act), COM/2022/68 final, available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN.

50 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148, available: https://eur-lex.europa.eu/eli/dir/2022/2555.

51 See Explanatory Statement to Law 4961/2022.

Enabling Patent Transactions Through the Use of Blockchain Technology

by **Arina Gorbatyuk and Thomas Gils** *

Abstract: Access to complete, accessible, up-to-date, and accurate patent information is a prerequisite for transacting patents efficiently. Whereas patent registers administered by patent offices aim to communicate patent information to the public, they face limitations in the era of rapid innovation, partially due to manual input and verification of data. In this paper, we argue that integrating blockchain technology into patent registers could assist in remedying certain limitations of conventional 'reference' registers by combating territorial fragmentation, improving patent ownership tracing, and increasing the visibility of patents that could be traded. We further investigate to what extent blockchains are conducive to enabling patent transactions and explore the possibility of transforming patent registers into patent marketplaces.

Keywords: Intellectual Property, Patents, Patent Transactions, Ownership Transparency, Patent Registers, Blockchain, Distributed Ledger Technology

Recommended citation: Arina Gorbatyuk and Thomas Gils, Enabling Patent Transactions Through the Use of Blockchain Technology, 14 (2023) JIPITEC 603 para 1.

A. Introduction

1 Blockchain technology is regarded as a game changer in the information technology world as it allows recording and exchanging information in a decentralised manner on an unprecedented level. Since the introduction of the technology more than a decade ago, its application to various fields has been explored both in theory and practice. Intellectual property (IP) is not an exception. IP practitioners, scholars, and policymakers have been actively examining whether blockchains can be instrumental in registering, managing, and enforcing IP rights.[1]

* Dr. Arina Gorbatyuk (corresponding author), Researcher Fellow, KU Leuven Centre for IT & IP Law (Belgium); arina.gorbatyuk@kuleuven.be; Sint-Michielsstraat 6 - box 3443 3000 Leuven Belgium; Thomas Gils, Researcher, KU Leuven Centre for IT & IP Law / Knowledge Centre Data & Society (Belgium); thomas.gils@kuleuven.be; Sint-Michielsstraat 6 - box 3443 3000 Leuven Belgium.

1 Marco Barulli, 'IP Is a Journey: Blockchain and Encrypted Storage Are Your Best Friends' [2021] WIPO Magazine <https://www.wipo.int/wipo_magazine_digital/en/2021/article_0002.html> accessed 1 September 2023; Balázs Bodó, Daniel Gervais and João Pedro Quintais, 'Blockchain and Smart Contracts: The Missing Link in Copyright Licensing?' (2018) 26 International Journal of Law and Information Technology 311; Birgit Clark, 'Blockchain and IP Law: A Match Made in Crypto Heaven?' [2018] WIPO Magazine 6; Birgit Clark, 'Crypto-Pie in the Sky? How Blockchain Technology Is Impacting Intellectual Property Law' [2019] Stanford Journal of Blockchain Law & Policy <https://stanford-jblp.pubpub.org/pub/blockchain-and-ip-law> accessed 1 September 2023; Gönenç Gürkaynak and others, 'Intellectual Property Law and Practice in the Blockchain Realm' (2018) 34 Computer Law & Security Review 847; Julia Hugendubel, 'Blockchain Technology and Intellectual Property – A Basic Introduction' [2021] SSRN Electronic Journal <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3917801> accessed 1 September 2023; Anne Rose, 'Blockchain: Transforming the Registration of IP Rights and Strengthening the Protection of Unregistered IP Rights' [2020] WIPO Magazine <https://www.wipo.int/wipo_magazine_digital/en/2020/article_0002.html>

2 Currently, this technology is mainly applied to processes regarding creative works that are subject to copyright protection. The benefits that this technology provides are evident as it can tackle many notorious flaws of copyright protection. As creative works are generally not subject to registration, it poses challenges for identifying and verifying authorship and offering centralized visibility of developed works.[2] In particular, one of the most popular implementations of blockchain technology in the field of copyright is proof-of-ownership (such as WIPO PROOF, Pixsy, Bernstein[3]) that allows users to obtain a digital 'fingerprint' (in the form of a token accompanied by a blockchain certificate) of any file, including files containing copyright-protected assets, potentially useful to verifying authorship and enforcing copyright.[4] Furthermore, multiple blockchain-based non-fungible token (NFT) marketplaces, such as Monegraph, Crypto.com or OpenSea,[5] have recently been created to support the development and exchange of digital art, music, or other digital assets.[6] Such platforms also frequently assist in managing associated IP rights.

3 The utility of applying blockchain technology to patents is less explored, with fewer initiatives related to applying blockchain technology in the domain of patents being implemented to date. While at first glance this technology can be advantageous, for instance, in combating hurdles associated with territoriality of patents or manual processing of data. In this paper, we claim that to efficiently establish patent transactions interested parties need access to complete, accessible, up-to-date, and reliable patent data that patent offices at times fail to provide. We investigate whether the current drawbacks could be remedied by integrating blockchain technology into patent registers and to what extent blockchains are conducive to facilitating patent transactions by matching the 'seller' with the 'buyer'.

4 To stimulate openness and visibility of developed knowledge, patent offices have already established registers to disclose patent-related information.[7] However, patent information is fragmented as it is gathered by various offices. In addition, patent offices apply different standards to disclosing the assembled patent information to the general public which affects its 'global' accessibility.[8] Furthermore, patent offices are predominantly in charge of patent prosecution and do not play an active role in patent exploitation and patent transactions.

5 Facilitating patent transactions is indispensable to securing the efficient functioning of the patent system which is meant to advance science and technology. More than three million patent applications are filed annually worldwide, and more than one and a half million are granted.[9] The EPO alone received a record number of patent

accessed 1 September 2023; D Tapscott and A Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World (Penguin Publishing Group 2016).

2 Marie-Christine Janssens and others, 'Copyright Issues on the Use of Images on the Internet', *Research Handbook on Intellectual Property and Cultural Heritage* (Edward Elgar publishing; Cheltenham 2022).

3 For more information on WIPO PROOF see <https://www.wipo.int/wipoproof/en/)>; Pixsy - <https://www.pixsy.com/register/>; Bernstein - <https://www.bernstein.io/> accessed on 1 September 2023.

4 Frederick Mostert, 'Digital Date-and-Time-Stamping: The Evidentiary Value and Practical Significance of WIPO PROOF' [2021] *WIPO Magazine* <https://www.wipo.int/wipo_magazine_digital/en/2021/article_0001.html> accessed 1 September 2023. This digital fingerprint is also used to obtain a timestamp on developed know-how and trade secrets that can be instrumental to generate evidence in case of disputes.

5 For more information on Monegraph, see https://www.monegraph.com/technology/; Crypto.com - <https://crypto.com/nft/marketplace>: OpenSea - <https://opensea.io/about> accessed on 1 September 2023.

6 Hugendubel (n 1) 1; Seyed Mojtaba Hosseini Bamakan and others, 'Patents and Intellectual Property Assets as Non-Fungible Tokens; Key Technologies and Challenges' (2022) 12 Scientific Reports 2178, 2; Nikos Kostopoulos and others, 'Demystifying Non-Fungible Tokens (NFTs)' (EU Blockchain Observatory and Forum 2021) 4 <https://www.eublockchainforum.eu/news/new-thematic-report-demystifying-nfts> accessed 1 September 2023.

7 The accessibility of those registers, however, depends on how technologically advanced are the respective patent offices.

8 In particular, WIPO acknowledges the importance of the digital transformation of IP offices for the efficient functioning of the global IP system and states that "most offices in developing countries have limited resources and face challenges to adopt digital business services", such as "online services, including search, registry and filing systems; efficient and standardized business processes for IP administration; integration into regional and international IP systems to enable the digital exchange of data and documents". See WIPO, 'IP Office Business Solutions' <https://www.wipo.int/global_ip/en/activities/ip_office_business_solutions/index.html> accessed 4 September 2023.

9 WIPO, 'World Intellectual Property Indicators 2021' (2021) <https://www.wipo.int/edocs/pubdocs/en/wipo_pub_941_2021.pdf> accessed 1 September 2023.

filings in 2021,[10] which was promptly broken with a 2.5% patent application increase in 2022.[11] These trends make it ever more challenging for all the relevant actors to navigate through the maze of patent rights to secure their freedom to operate. As will be explained in Section B, patents cannot be exploited without explicit authorisation from rightsholders, unless an exception or limitation applies.[12] As a result, enhancing the efficiency of establishing patent transactions comes to the fore, as most patent transactions are still established by virtue of 'classical' lengthy and costly contractual negotiations. Furthermore, to establish any transaction, third parties should not only be aware of the content of the patented invention but also have the means to identify current rightsholders in a certain and efficient manner. As will be highlighted in Section C, accurate information on patent rightsholders changes may not always be promptly obtainable by patent offices.

6 In Section D, we argue that integrating blockchain technology into patent registers is an instrumental solution that allows (within the boundaries of identified limitations) to (1) combat the territorial fragmentation of patent registers, (2) tackle the lack of transparency of patent ownership by enabling improved patent ownership tracing, and (3) increase the visibility of patents that could be licensed or assigned. Furthermore, blockchain technology could facilitate the establishment of patent transactions by offering the possibility to digitise and (semi-) automate certain associated processes. In particular, one could even tokenise a patent, trade patents in an NFT form and automate this process by relying on smart contracts, as explored by private actors (such as IPwe).[13] Whether the theoretical benefits of automating trade in patents are in line with the nature of patent protection remains to be analysed.[14] Moreover, the implementation of blockchain technology as means of (allegedly more efficient) governance and exchange of patents is not without (legal) hurdles that are hard not to notice and even harder to overcome.[15] Some limitations of this technology in the context of enabling patent transactions are concisely addressed.

7 Finally, in Section E, this article debates the issue of privatisation of patent governance in light of the launch of private patent marketplaces.[16] Patent disclosure and dissemination of patent information are currently predominantly governed by patent offices as intermediaries guarding the legislatively established balance between the interests of patent owners and society, the so-called 'quid-pro-quo' of the patent system (also known as a 'social contract').[17] However, the implementation

10 EPO, 'Patent Applications in Europe Reach Record Level in 2021' (2022) <https://www.epo.org/news-events/news/2022/20220405.html> accessed 1 September 2023.

11 EPO, 'Innovation Stays Strong: Patent Applications in Europe Continue to Grow in 2022' <https://www.epo.org/news-events/news/2023/20230328.html> accessed 4 September 2023; EPO, 'Patent Index 2022 - Statistics at a Glance' <https://www.epo.org/about-us/annual-reports-statistics/statistics.html> accessed 4 September 2023.

12 For more information, see <https://www.wipo.int/patents/en/topics/exceptions_limitations.html> accessed on 1 September 2023.

13 Hugendubel (n 1) 6; Bamakan and others (n 6) 2.

14 On a more fundamental level, the tension between the law and blockchain technology has been thoroughly studied by Primavera De Filippi and Aaron Wright, Blockchain and the Law: The Rule of Code (Cambridge, Massachusetts : Harvard University Press 2019). In essence, they claim that the rules of law and the rules of code could coexist and even achieve certain synergy. In particular, they state that "blockchain-based protocols and smart contracts can be used to model or represent laws and embed them directly into the fabric of a blockchain-based network to ensure the automatic execution and ex-ante enforcement of these rules". Nonetheless, open-ended legal provisions to date are not suited for implementation via a computer code.

15 See Section D.II.2.

16 For the purpose of clarity, we would like to explain the terminology applied in this article. By 'patent register' we understand a conventional 'reference' patent register or database governed by a patent office. The term 'blockchain-based patent platform' is used to refer to a patent register that has been transformed into a platform by means of integrating blockchain technology into the patent register. Such a platform may or may not support a transactional functionality. By using the term 'blockchain-based patent marketplace' we signal that the platform supports a transactional functionality (in other words allows to trade patents via the platform).

17 In brief, the patent system is based on the utilitarian premise that without patent protection inventors (or by succession other associated parties) would not be sufficiently motivated to innovate since they would not be able to recuperate invested resources as any third party could replicate their invention without investing the same efforts and enduring the same costs. In return for these exclusive patent rights, patent applicants are instructed to publicly disclose their work to disseminate related technological information to the public, reduce wasteful duplication of innovative efforts, and stimulate cumulative innovation. This legislatively established balance is just and straightforward, yet fragile. Robert P Merges, Justifying Intellectual Property (Cambridge, Mass : Harvard University Press 2011) 2.

of blockchain-based patent marketplaces governed by private actors (such as IPwe[18]) may distort this fragile balance as they partially aim at taking over functions of patent registers without abiding by the principles of transparency and accessibility of patent information to any interested third party. This article concludes that if patent marketplaces were to be established, patent offices with the aid of blockchain (or another digital) technology would be best placed to offer such services as, contrary to private solutions, they have the potential of developing a 'global' marketplace, instead of a 'local' shop access to which is restricted to selected members.

B. Patents as valuable assets

8 Patents have increasingly become one of the core corporate assets. It is even claimed that patents (as well as other IP rights) can be far more valuable than tangible assets as their trade can generate significant revenues.[19] A trend toward patent monetisation is observed by economic and managerial scholars in the increasing number of patent transactions and associated generated profits.[20] This trend corresponds with the upturn of so-called 'markets for technology'.[21]

9 The rise of patent monetisation or patent trade can be linked to multiple trends, among which are the increase in research and development (R&D) decentralisation and specialisation and the expansion of overlapping patent rights, also known as patent thickets.[22] As a patent gives its owner the right to exclude others from exploiting the patented technology in any way, apart from the exempted ones, third parties interested in getting access to certain technology do not have many options but to attempt to obtain the required authorisation from a relevant rightsholder. Thus, interested third parties are expected to engage in various types of patent transactions, such as assignment or (cross-) licensing agreements, with patent rightsholders to avoid infringing granted rights.

10 As for any (intellectual) property transaction, the main prerequisites of a patent transaction are the knowledge of a subject matter that is potentially available for trade and the identity of a person who is authorised to grant permission to exploit a patented invention on negotiated terms. The subject matter of a patent transaction is rather easy to track as patents are registered rights.[23] However, the identification of relevant rightsholders can cause difficulties. At times, it may be challenging to trace them as patents can be assigned or certain patent rights licensed without it being reflected in patent registers.[24] Considering that these two prerequisites are essential for enabling patent transactions, it is instrumental to ensure that the information on both the subject matter and the identity of a relevant rightsholder is accessible to third parties.

11 Especially for patent-dense industries, in which patent thickets are prominent, the creation of various forms of patent pools has been seen as a solution to ensure that patented technologies can be exchanged in an efficient manner. In this context, bilateral negotiations can be time-consuming and impractical as access to multiple patented technologies is often required to ensure the freedom to operate. These pools can take different forms and are subject to various governance schemes.[25] The core function of patent pools is the creation of an ecosystem in which members share access to selected patented inventions that are related to a particular technology in a certain industry sector

18 For more information on IPwe, see <https://ipwe.com/> accessed on 1 September 2023.

19 Jeffrey Cohen, *Intangible Assets: Valuation and Economic Benefit* (Wiley 2005); Henry William Chesbrough, *Open Innovation: The New Imperative for Creating and Profiting from Technology* (Harvard Business Press 2003).

20 Peter C Grindley and David J Teece, 'Managing Intellectual Capital: Licensing and Cross-Licensing in Semiconductors and Electronics' (1997) 39 California Management Review 8; Kevin G Rivette and David Kline, Rembrandts in the Attic: Unlocking the Hidden Value of Patents (Harvard Business School Press 2000).

21 Alfonso Gambardella, Ashish Arora and Andrea Fosfuri, *Markets for Technology: The Economics of Innovation and Corporate Strategy* (Cambridge, Mass: The MIT Press 2004).

22 Luis Miotti and Frederique Sachwald, 'Co-Operative R&D: Why and with Whom?: An Integrated Framework of Analysis' (2003) 32 Research Policy 1481, 1482; Bronwyn H Hall and others, 'A Study of Patent Thickets' (Intellectual Property Office 2013) 17 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4094057> accessed 1 September 2023; Bruce S Tether, 'Who Co-Operates for Innovation, and Why: An Empirical Analysis' (2002) 31 Research Policy 947, 947; Carl F Fey and Julian Birkinshaw, 'External Sources of Knowledge, Governance Mode, and R&D Performance' (2005) 31 Journal of Management 597, 600.

23 See Section C.

24 See Section C.

25 WIPO, 'Patent Pools and Antitrust - A Comparative Analysis' (2014) 6 <https://www.wipo.int/export/sites/www/ip-competition/en/docs/patent_pools_report.pdf> accessed 1 September 2023.

(e.g., COVID-19 Technology Access Pool (C-TAP)[26]; Medicines Patent Pool (MPP)[27]). To simplify, various patents are contributed to pools by their owners with the aim of cross-licensing, whereas other interested parties are typically allowed to have access to the pooled patents on standard contractual terms.[28] The clear advantage of such pools is the optimisation of granting access to selected patents without engaging in lengthy bilateral negotiations with multiple patent holders that entail high transaction costs.

12 Patent pools are currently one of the core mechanisms used to optimise patent transactions. However, they are applied only in specific cases that are often related to public health or telecommunication standards. Such efficiency does not exist when exchanging other patented technologies, and interested parties are expected to gather all the relevant information to initiate patent transaction negotiations on an individual basis. Blockchains may, however, open opportunities for simplifying patent trade, as explained in Section D, by increasing transparency of patent data, digitising transactions, and reducing associated administrative and transaction costs.[29]

C. Patent registers as patent databases

13 Patent offices are bound by the obligation to secure the visibility of patent-related information by disclosing to third parties the data collected from patent applicants.[30] The disclosure function of the patent system is considered to be one of the core benefits for society as it prevents wasteful duplication of R&D efforts and stimulates follow-on innovation.[31] By making this information public, patent offices signal which inventions are currently protected and cannot be exploited without the authorisation of relevant rightsholders. The shared patent information also allows third parties to study disclosed inventions and use them within the established exceptions and exemptions[32] during the patent term and without any limitations after the protection lapses. It additionally indicates which patent assets are potentially available for trade.

14 The collected information is generally communicated via patent bulletins and patent registers governed by IP offices on national or regional levels. Patent registers serve as patent databases transmitting patent data to the public. The scope of shared information and mode of access differ per office. Some IP offices developed user-friendly publicly accessible (patent) databases, such as the European Patent Office (EPO) Espacenet[33] and the World Intellectual Property Organization (WIPO) Patentscope[34], which disseminate patent documents of national and regional patent offices, as well as international Patent Cooperation Treaty (PCT)[35] applications. The shared information contains multiple valuable details, including the content of inventions (delimiting the scope of protection), the territory of protection, relevant dates (priority, application, publication, grant), classifications, and other important bibliographic data, such as information on inventors, applicants, and owners of patents or patent applications.

15 Patent registers and databases provide sufficient information to third parties interested in obtaining

26 For more information, see <https://www.who.int/initiatives/covid-19-technology-access-pool> accessed on 1 September 2023.

27 For more information, see <https://medicinespatentpool.org/> accessed on 1 September 2023.

28 Robert P Merges, 'Institutions for Intellectual Property Transactions: The Case of Patent Pools', *Expanding the Boundaries of Intellectual Property* (Oxford University Press 2001).

29 Bamakan and others (n 6) 2; Hugendubel (n 1) 10; Ronny Hauck, 'Blockchain, Smart Contracts and Intellectual Property. Using Distributed Ledger Technology to Protect, License and Enforce Intellectual Property Rights' (2021) 1 Legal Issues in the Digital Age 29 <https://lida.hse.ru/article/view/12369> accessed 1 September 2023.

30 For instance, many patent offices are obliged to publish patent applications after the expiry of a period of eighteen months from the date of filing or the priority date (e.g. Art. 21 Patent Cooperation Treaty, Art. 93 European Patent Convention, United States Code, Title 35, Section 122 (35 U.S.C. 122).

31 Arina Gorbatyuk and Adrián Kovács, 'Patent Notice (Failure) in the Era of Patent Monetization' (2022) 53 IIC - International Review of Intellectual Property and Competition Law 506, 510; Benjamin N Roin, 'The Disclosure Function of the Patent System (Or Lack Thereof)' (2005) 118 Harvard Law Review 2007, 2009; Edmund W Kitch, 'The Nature and Function of the Patent System' (1977) 20 The Journal of Law and Economics 265, 278.

32 For more information, see <https://www.wipo.int/patents/en/topics/exceptions_limitations.html> accessed on 1 September 2023.

33 For more information on the EPO Espacenet, see <https://worldwide.espacenet.com/> accessed on 1 September 2023.

34 For more information on the WIPO Patentscope, see <https://patentscope.wipo.int/search/en/search.jsf> accessed on 1 September 2023.

35 Patent Cooperation Treaty (PCT) 2002.

access to patents. However, they have several major limitations that may hinder the efficient and smooth establishment of patent transactions.

16 First, even though the scope of collected data is largely harmonised, thanks to international cooperation and underlying treaties[36], the collection and communication of the patent data is decentralised, as patents are granted on national or regional levels. The PCT route could be viewed as an exception as it centralises the application process. This decentralisation creates fragmentation which hinders the accessibility and visibility of collected data. The issue of fragmentation is partially mitigated through the introduction of 'global' patent databases, such as EPO Espacenet and WIPO Patentscope. However, the completeness of those databases depends on the level of digitisation of data collected by underlying national or regional patent offices. Furthermore, one of the apparent constraints on the accessibility of data are languages in which patent applications are instructed to be filed. The EPO and WIPO attempt to overcome this barrier by inbuilding automatic translations into their databases.

17 The collection, processing, and maintenance of the data are currently primarily conducted manually, even when relying on electronic systems, such as ePCT (WIPO), myEPO (EPO), or DPMAdirektPro (the German Patent and Trade Mark Office (DPMA)).[37] This means that the (electronically) communicated data must be first processed by the patent office before being displayed in patent registers. Thus, the trade-off faced by patent offices at the moment is between the immediate availability of updated patent data (so-called real-time updates) and data reliability (ensuring that the data is accurate and complete). The preference is currently given to reliability. Patent applicants or owners commonly have no means to insert information directly into the registers. They are first asked to provide the requested information to responsible patent office officials. This trade-off is justifiable as communication of inaccurate information without any subsequent verification is potentially more harmful than a delay in disseminating the relevant information.

18 Second, patent applicants and owners are responsible for communicating any legislatively required updates to patent offices to ensure that patent registers contain accurate data. For instance, they are generally instructed to register assignment and licensing agreements to ensure that all relevant rightsholders are known to the public. Despite the underlying obligations[38], rightsholders, at times, fail to communicate this information to patent offices, which limits the transparency of patent rightsholders.[39] Thus, third parties interested in establishing a patent transaction may be forced to endure unnecessary costs to obtain this essential information to initiate a negotiation process.

19 Finally, patent databases governed by patent offices are 'reference' databases. Patent offices are instructed to disclose essential patent-related information to society, but they are not legislatively expected to act as active intermediaries between patent rightsholders (potential 'sellers') and third parties (potential 'buyers'). These business relationships are currently predominantly governed privately. However, considering the importance of patent trade, it is high time to examine whether patent offices, in fact, should take on board additional functions that could be of value to knowledge exchange and technological advancement and whether the integration of blockchain technology into patent registers could remedy the identified challenges and shortcomings of current patent registers.

D. Patent blockchains as digital patent platforms

20 To establish whether blockchain technology could be instrumental in facilitating patent trade, it is first necessary to comprehend its essential technical characteristics. Understanding the functionality of this kind of distributed ledger technology will allow us to demonstrate how it can assist in resolving some of the identified constraints of conventional 'reference' patent registers.

36 Susy Frankel and Daniel J Gervais, *Advanced Introduction to International Intellectual Property* (Edward Elgar 2016) 88, 98.

37 For more information on ePCT see <https://www.wipo.int/pct-eservices/en/index.html>; myEPO - <https://www.epo.org/applying/online-services/myepo.html>; DPMAdirektPro - <https://www.dpma.de/service/elektronische_anmeldung/dpmadirekt/index.html> accessed on 1 September 2023.

38 For instance, in Belgium the notification of a license needs to use a specific form made available by the Belgian Intellectual Property Service, whereas in Turkey patent assignments need approval of a notary public. See, Belgium: Art 34 of the Royal Decree of 2 December 1986 on the application, granting and maintenance of patents for inventions. Turkey: Gürkaynak and others (n 1) 858. Other differences in legislative norms can be reviewed in Section 5 'The Recording of Patent Ownership Changes' in Gorbatyuk and Kovács (n 31).

39 Gorbatyuk and Kovács (n 31) 516.

I. Essential characteristics of blockchain technology

21 The key characteristics of blockchains are in their structure and functionality. Structurally, blockchains should be thought of as shared ledgers or databases, distributed over the participants to a network ('nodes'), consisting of time-stamped 'blocks' that are chained to each other by including a reference to the preceding block. Functionally, they are intended to store individually accessible information in a transparent and tamper-resistant manner, while possibly also supporting a transactional functionality.[40]

22 There are several types of blockchains hosting different types of nodes.[41] Some nodes are rather passive (*read*-permission), while others can fulfil a more active role (*write-*/*commit*-permission).[42] A '*read*'-permission allows a node to access the ledger and see transactions, whereas a '*write*'-permission empowers a node to create transactions and send them to the network. A '*commit*'-permission grants a node the ability to update the state of the ledger (e.g., miners or validator nodes).

23 In *permissionless* blockchains, as depicted in Table 1, every node has a *commit*-permission, which allows them to validate transactions and let (mining) nodes add blocks. A *permissioned* blockchain, on the other hand, will reserve *write*- and/or *commit*-permissions to a subset of the nodes in the network. In other words, only some of the nodes are able to validate transactions and add blocks to the chain (*commit*) or enter into transactions (*write*).[43] These blockchains are considered less transparent and are not regarded as pure *peer-to-peer* networks.

24 Another relevant distinction is the one between public and private blockchains. *Public* blockchains are open to and available for anyone (e.g., by downloading the relevant software, one can join the respective blockchain network).[44] Conversely, *private* blockchains are not open to everyone and only admit certain participants (*read*-permission). This type of blockchain often falls in the category of 'enterprise blockchains'.

25 As a consequence of their transparency and accessibility, *public permissionless* blockchains (e.g., Bitcoin) employ encryption and run on so-called consensus mechanisms (e.g. Proof-of-Work, Proof-of-Stake).[45] These mechanisms ensure a certain level of infrastructural security to hold off possible attacks of maleficent nodes and guarantee the tamper-resistance of added information. *Private permissioned* blockchains do generally not need these security measures as participants trust each other and have different prerogatives.[46]

40 Aaron Wright and Primavera De Filippi, 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia' [2015] SSRN Electronic Journal 4–8 <https://www.ssrn.com/abstract=2580664> accessed 1 September 2023; Konstantinos Christidis and Michael Devetsikiotis, 'Blockchains and Smart Contracts for the Internet of Things' (2016) 4 IEEE Access 2292, 2293; European Commission and others, *Study on Blockchains: Legal, Governance and Interoperability Aspects* (Publications Office 2020) 26–28 <https://op.europa.eu/en/publication-detail/-/publication/939fe2cc-5784-11ea-8b81-01aa75ed71a1/language-en> accessed 1 September 2023.

41 Tapscott and Tapscott (n 1) 66–67.

42 Garrick Hileman and Michel Rauchs, 'Global Blockchain Benchmarking Study' (Cambridge Center for Alternative Finance 2017) 20–21 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3040224> accessed 1 September 2023.

43 ibid.

44 An example is the Ethereum-blockchain, see <https://ethereum.org/en/run-a-node/> accessed on 1 September 2023.

45 Christidis and Devetsikiotis (n 40) 2293–2295.

46 Michel Rauchs and others, '2nd Global Enterprise Blockchain Benchmarking Study' (Cambridge Center for Alternative Finance 2019) 13 <https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/2nd-global-enterprise-blockchain-benchmarking-study/> accessed 1 September 2023.

47 However, this requires substantial investment in, for instance, hardware for mining or cryptocurrency in the hypothesis of a PoW-/respectively a PoS- consensus mechanism.

TYPE OF BLOCKCHAIN	Private	Public
Permissioned	ENTERPRISE BLOCKCHAINS - participation (read-privilege) is restricted and write and commit-privileges are awarded to a single node or a limited number of nodes.	PUBLIC PERMISSIONED BLOCKCHAINS - participation (read-privilege) is unrestricted but write- and commit-privileges are awarded to a single node or a limited number of nodes.
Permissionless	CONSORTIUM BLOCKCHAINS - participation (read-privilege) is restricted but write- and commit-privileges are awarded to all authorised nodes.	CRYPTOCURRENCY BLOCKCHAINS - participation (read-privilege) is unrestricted and write- and commit-privileges are awarded to all nodes.[47]

Table 1: '*Taxonomy of blockchains*' [48]

26 Finally, one has also to take into account that blockchain networks have different modes of governance: (1) centralised or decentralised and (2) on-chain or off-chain.[49]

27 Centralised governance means that only one or a limited set of actors determines the rules of operation of the blockchain network and decides on, for instance, the admission of new nodes.[50] Private blockchains are often governed centrally.[51] On the contrary, decentralised governance implicates that a variety of actors, possibly spread over the various levels of the technology stack (network – protocol – application layer), can contribute to decisions. Such governance is more typical for public blockchains.[52]

28 The distinction can also be made between on-chain and off-chain governance. The difference between the two lies in the manner in which the decision-making occurs and how these decisions are implemented. On-chain governance entails that the decision-making procedures are embedded in the blockchain protocol, i.e., the blockchain protocol itself ensures that stakeholders make decisions. With off-chain governance, the decision-making occurs elsewhere whereby stakeholders can rely on, for instance, existing forms of corporate governance such as a management board or articles of association. The decisions made must be subsequently imported into the blockchain protocol.[53] On- and off-chain governance can also be combined.[54]

II. Relevance of blockchain technology for patent registers

29 In theory, as discussed in Part 1, blockchain technology may resolve some of the challenges encountered by conventional patent registers. However, in Part 2 we then highlight the many issues and limitations that a blockchain implementation would have to deal with in order to ensure the feasibility and usefulness of transforming current patent registers into blockchain-based patent platforms.

1. Transitioning from 'reference' patent registers to blockchain-based patent platforms

30 Taking into account these technical characteristics of blockchain technology, one can conceptualise theoretically how said technology could improve the functionality of patent registers by allowing relevant stakeholders to update patent registers

48 Table 1 is based on S Nascimento and others, 'Blockchain Now And Tomorrow: Assessing Multidimensional Impacts of Distributed Ledger Technologies' (Publications Office of the European Union 2019) 14–15 <https://publications.jrc.ec.europa.eu/repository/handle/JRC117255> accessed 1 September 2023; Christidis and Devetsikiotis (n 40) 2297–2298; Hileman and Rauchs (n 42) 20–21.

49 European Commission and others (n 40) 41–45. Blockchain governance is sometimes also referred to as 'social consensus', see Rauchs and others (n 46) 14–15.

50 Rauchs and others (n 46) 14.

51 ibid 40–41.

52 Decentralised governance generally requires certain incentive structures which are not discussed in the context of this article.

53 Both systems come with (dis)advantages. For a discussion, see Nascimento and others (n 48) 17; Michael Borella, 'The Compelling Implications of Using a Blockchain to Record and Verify Patent Assignments' (*Patent Docs*) <https://www.patentdocs.org/2022/07/the-compelling-implications-of-using-a-blockchain-to-record-and-verify-patent-assignments.html> accessed 1 September 2023; European Commission and others (n 40) 43–44; Tom Lyons and Ludovic Courcelas, 'Governance of and with Blockchains' (EU Blockchain Observatory and Forum 2020) 10–13 <https://www.eublockchainforum.eu/reports/governance-and-blockchains> accessed 1 September 2023.

54 Lyons and Courcelas (n 53) 14, 18–21.

in a synchronised, transparent, and decentralised manner as well as enter into and validate patent transactions.[55] Thus, by relying on blockchains, patent registers could potentially transition from 'reference' databases to multifunctional patent platforms that may even support a transactional functionality turning a register into an online marketplace.

31 In a nutshell, one can envisage a blockchain application through which actors can establish, per jurisdiction, which patents have been applied for or granted and who has rights in those patents. Each patent (application) could have a unique hash recorded on the underlying blockchain (a so-called 'proof of existence').[56] Such hash could function simultaneously as a digital representation of respective patents as well as a central link through which all the related patent information (e.g., patent file, bibliographic information, as discussed in Section C) can be accessed (in existing patent registers or databases).[57] Furthermore, relevant patent transactions, such as licenses and assignments, could also be imported and featured on the blockchain. This could be realised by supplementing the hash with numeric identifiers representing the parties involved in transactions related to the patent and linking to the possible profile of the actor. Moreover, the application could provide additional transactional functionality (which goes beyond merely displaying transactions) using public-private key cryptography, allowing interested parties to assign or license patents and record those transactions on the blockchain.[58,59] The graphical representation of this hypothetical blockchain is provided in Figure 1.

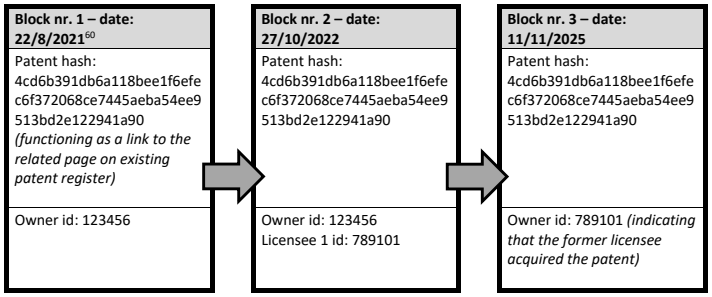


Figure 1: *'Graphical representation of the patent information in a blockchain'*

32 In such (theoretical) application, several features of blockchain technology may thus remedy certain issues or problems that the current, conventional patent registers encounter:[61]

33 **Distributed nature**: The distributed nature of blockchain technology ties in with the existing decentralised patent system. Introducing a single type of technology to be used by all patent offices could lead to more complete, uniform, and digitised patent data.[62] Moreover, by integrating them into

55 Nascimento and others (n 48) 14–20, 75; Borella (n 53); Clark (n 1) 31–34; Lois Hoyal, 'Talking about a New Revolution: Blockchain' (European Patent Office 2018) 9 <http://documents.epo.org/projects/babylon/eponet.nsf/0/FB134B001751B1FAC12583BD00317B47/$File/Talking_about_a_new_revolution_blockchain_conference_report_en.pdf> accessed 1 September 2023.

56 This hash could be incorporated into some sort of token, see Bodó, Gervais and Quintais (n 1) 314–315.

57 A hash (a 32 or 64-bit long sign combination) is the output of an encryption algorithm and is uniquely related to its input, while it is impossible to deduce the original input from the hash. Thomas Gils and Christine Frison, 'Blockchain Technology for Food Security? Resilience Potential and Risk Identification for the Multilateral System of the International Treaty on Plant Genetic Resources for Food and Agriculture', *The Transformation of Environmental Law and Governance - Risk, Innovation and Resilience* (Edward Elgar 2021) 210–211; Philip Boucher, 'How Blockchain Technology Could Change Our Lives' (European Parliamentary Research Service 2017) 10–11 <https://data.europa.eu/doi/10.2861/926645> accessed 1 September 2023.

58 Borella (n 53); Atharv Chandratre and Abhinav Pathak, 'Blockchain Based Intellectual Property Management' [2019] SSRN Electronic Journal 5–6 <https://www.ssrn.com/abstract=3800734> accessed 1 September 2023; Christidis and Devetsikiotis (n 40) 2295–2296.

59 This would require agreement by stakeholders on some form of a formal template outlining the information that should be reflected by specific assignments/licenses. Those fields could include the parties, date, the patent number(s), date, applicable fees, duration, exclusivity, choice of jurisdiction, and applicable law. A solid reference point could be current templates provided by patent offices to register licenses and patent assignments. For instance, the EPO forms 5055 and 5070, see <https://www.epo.org/applying/forms.html> accessed on 1 September 2023.

60 The date could be the patent application or grant, or even the technical import date into the blockchain, depending on the actual practical implementation of a blockchain application.

61 Christidis and Devetsikiotis (n 40) 2293–2297; Nascimento and others (n 48) 13–25; Tom Lyons, Ludovic Courcelas and Ken Timsit, 'Blockchain for Government and Public Services' (EU Blockchain Observatory and Forum 2018) 9–10, 12, 14–18 <https://www.eublockchainforum.eu/reports/blockchain-government-and-public-services> accessed 1 September 2023.

62 Lyons and Courcelas (n 53) 18.

one platform, the accessibility of national patent registers will be enhanced. More importantly, the fact that information is replicated by all the participating nodes entails that the data will persist even if a node fails (resulting in increased resilience and security).

34 **Tamper-resistant**: Due to the use of consensus mechanisms or the deliberate distribution of commit-privileges, blockchains are resilient against fraudulent transactions and avoid the possibility of double entries.[63]

35 **Transactions**: Blockchains can support a transactional functionality, allowing participating nodes to interact, transfer patents, and register such transactions on the underlying blockchain. These transactions are added to the chain automatically and in real-time, increasing the visibility and reliability of said data.[64] Blockchain enthusiasts even speculate about the possibility of automating such patent transactions relying on smart contracts (as further discussed in the following section).[65]

36 **Transparency and auditability**: Once a patent features on the blockchain, the subsequent related transactions would be shown automatically to nodes or users with a read-permission. Hence, information on subsequent owners or licensees would be disclosed efficiently, while also easing up the task of patent offices of gathering and communicating such information. Additionally, due to the use of cryptographic hashes and the 'chained' nature of the blocks, interested parties could easily retrace the origin of a patent and verify the integrity of its transactional history.[66]

37 **Lower costs and increased efficiency:** As registering patent transactions with a variety of patent offices is often not without costs (e.g., due to language, paper filing requirements, and registration fees), automating this procedure will reduce the related costs and render the registration less language-sensitive.[67] Furthermore, the use of a common data standard will improve the efficiency of patent registers worldwide. [68]

63 Nascimento and others (n 48) 24–25.

64 Christidis and Devetsikiotis (n 40) 2295–2296.

65 Hauck (n 29) 18, 20; Gürkaynak and others (n 1) 849.

66 Clark (n 1) 32; Lyons and Courcelas (n 53) 18.

67 Gorbatyuk and Kovács (n 31) 523; Gürkaynak and others (n 1) 858.

68 Lyons, Courcelas and Timsit, 'Blockchain for Government and Public Services' (n 61) 18.

38 To our knowledge, not a single patent office has attempted (to date) to integrate blockchain technology into its register. However, private entities have explored the possibility of trading patents through blockchains. One of the most prominent blockchain-based patent marketplaces currently offered is IPwe.[69] Apart from various IP analytical and managerial tools, the platform offers means to trade patents on an individual basis or contribute them to IPwe-governed pools. Whereas the project certainly is a step forward in optimising patent transactions, it has several limitations, which are further addressed in Section E.

2. Limitations of blockchain-based patent platforms

39 Although blockchain technology could, in theory, help overcome multiple challenges of existing patent registers and databases governed by patent offices, it will also bring about various issues that have to be mitigated, some of which are addressed in this section.

40 First, when designing a 'patent blockchain' one has to select its technical characteristics. As mentioned in Section D.I., blockchains can either be private or public and permissioned or permissionless. Taking into account the addressed public disclosure obligation imposed on patent applicants and enforced by patent offices, it is asserted that such blockchain should be a 'public' one (i.e., all interested parties could obtain a read-permission). At the same time, a database or platform is only valuable if the communicated information is accurate and reliable.[70] The advantage of *permissioned* blockchains is that in such networks trusted entities can be granted the competence to administer the blockchain and decide on the veracity of the data to be added. However, even if a blockchain is permissioned, it is not necessarily guaranteed that the inputted data is accurate, as the blockchain administrators may not be able to verify the lawfulness and accuracy of the inputted data in their entirety, which could lead to disputes, including patent infringements.[71] Nonetheless, it is asserted that a public permissioned blockchain seems to be the most evident type of blockchain in the current patent context,[72] as a permissionless blockchain would entail a much

69 For more information, see <https://ipwe.com/> accessed on 1 September 2023.

70 Also known as the issue of garbage in/garbage out. See e.g. De Filippi and Wright (n 14) 114.

71 Hileman and Rauchs (n 42) 18.

72 Chandratre and Pathak (n 58) 3.

	Patent offices	Patent actors	Third parties
Administration	✓	*	*
Permissions management	✓	X	X
Gatekeeping	✓	X	X
Transaction processing	✓	*	*
Transaction initiation	X	✓	X
Transaction validation	✓	✓	✓

Table 2: *'Suggested allocation of tasks'*[77]

higher level of disintermediation that would require a thorough discussion on the role of patent offices and their relationship with other stakeholders in the management of patent registers.[73] Moreover, such a blockchain would likely require a significant upgrade of the computing resources of the stakeholders who wish to be involved, reducing its practical feasibility.

41 Choosing a type of blockchain is, however, closely related to the intertwined questions of blockchain governance, the participants to the network, and the allocation of tasks.[74] Rauchs et al. (2019) provide a useful distinction between network operators and network participants with their respective, non-mutually exclusive tasks.[75] Network operators are responsible for administration (including network governance and setting of protocol rules), permissions management, and gatekeeping (admit/exclude network participants). Network participants can contribute to transaction processing (i.e., commit-permission) and transaction validation (i.e., read-permission). Transaction initiation (i.e., write permission) should also be added to the list.

42 Patent offices should be attributed an important role in accordance with their competencies under the existing legal framework. As depicted in Table 2, those tasks can be, for instance, (patent) transaction processing (including inputting patents into the network (both existing patents as well as newly granted ones)), administration, permissions management, and gatekeeping.[76] Organisations willing to enter into patent transactions ('patent actors') should, at least, be entitled to transaction initiation and validation. Other third parties (e.g., researchers or civil society) could be awarded transaction validation privileges. It remains to be reviewed which role patent actors and third parties should play in the governance/administration of a patent blockchain and to what extent they could contribute to transaction processing.

43 Due to the involvement of multiple patent offices in the envisaged network, there will be no single leader entity per se. Whether or not patent actors and third parties obtain a role in the blockchain administration will, however, determine the actual level of the decentralisation of governance. If such an initiative aims to gain support from all stakeholders, there will be no alternative but to assign them a certain role. Given the highly political nature of decisions regarding the international patent system, it can also be expected that governance will or should remain predominantly off-chain for the foreseeable future. This off-chain governance role could be awarded to the WIPO due to its administrative, neutral, and intergovernmental nature.[78]

44 Second, to increase the global visibility and tradability of patents, information provided on patent platforms should be globally available and as complete as possible. Global availability may be an issue as certain parts of the world (e.g., the "Global South") lack the digital infrastructure others have (e.g., North America, Europe and certain parts of Asia), rendering a successful global patent blockchain implementation rather difficult. Logically, this also impacts the possible initial allocation of tasks: one can imagine that certain patent offices do not dispose of the necessary computing resources required to run a full node.[79] Vice versa, certain large corporations or, for instance, universities likely do, which makes it difficult to precisely allocate the tasks for patent actors and third parties, as outlined in Table 2.[80]

45 Regarding completeness, it should be taken into

73 For a similar discussion under copyright law, see Bodó, Gervais and Quintais (n 1) 316–319.

74 Lyons and Courcelas (n 53) 17–22.

75 Rauchs and others (n 46) 24.

76 Clark (n 1) 32; Christidis and Devetsikiotis (n 40) 2295–2296.

77 '√' – direct task; 'X' – not permitted task; '*' – potentially permitted task.

78 This also follows from the choice for a permissioned blockchain network. In a permissionless network, on-chain governance is more important as no recourse can be made to any 'leading' authority and to ensure the security of the network and the balance of power. See Lyons and Courcelas (n 53) 11.

79 See footnote 8.

80 For further relevant considerations, see Lyons and Courcelas (n 53).

account that the mere availability of a 'global' blockchain network supported by patent offices will unlikely instantly incentivise patent actors to register their licenses or assignments on it. Hence, imposing an enforceable obligation on actors (backed up by negative or positive incentives) to record their transactions on the blockchain should be considered.[81] Currently, the main barriers to recording the named agreements are administrative burdens and associated costs, especially elevated due to patent territoriality. Blockchain technology could increase recordation efficiency and lower associated costs, as it permits overcoming administrative challenges posed by territoriality.

46 Third, there are many legal and regulatory hurdles that may stand in the way of a swift adoption of blockchain technology for patent registers.[82] Typical challenges include identifying applicable law, jurisdiction, enforcement, liability, data protection, issues regarding dispute resolution and blockchain governance, as well as matters relating to the transactions to be conducted (e.g., complicated patent agreements). For instance, as patents are territorial rights, the registration of the related licenses or assignments with national patent offices needs to comply with national requirements. Resolving these issues may not only require well-conceived blockchain applications that integrate these requirements into their functioning but possibly also legislative amendments.[83]

47 Another important legal issue is related to the possibility of the 'tokenisation'[84] of patents by issuing patent-specific NFTs and allowing trade in such NFTs (as done by IPwe). NFTs are distinct digital assets and should be considered separate from the real-world assets they represent (e.g., patents).[85] This means that when an NFT relating to a patent is assigned, only the NFT changes owner. The patent rights remain with the previous owner unless an additional agreement is entered into.[86] Moreover, existing formal requirements under (national) patent and contract laws will not allow for patent assignments or licenses through the transfer of an NFT.[87]

48 Fourth, an additional step in the transactional functionality could be to not just represent patents through a hash on the blockchain, as depicted in Figure 1, but incorporate them in a 'smart contract' expressing a license or assignment.[88] A smart contract functions as an autonomous actor on the blockchain network: it has its own account and will execute itself if the relevant conditions are met.[89] This automatic execution is, allegedly, one of the core benefits of smart contracts, as it entails immediate enforcement of established contractual obligations by using autonomous code.[90] However, smart contracts are deterministic and follow a strict 'if-then' logic.[91] This means that only precise, defined, and straightforward obligations can be transposed into code in an underlying smart contract and registered on a blockchain.[92] On the contrary, smart contracts are currently unable to sufficiently reflect flexible or sophisticated legal obligations conditioned on multiple factors.[93] Hence, their use appears to be difficult to reconcile with complex patent licenses and assignments, which can hardly be translated into a list of if-then statements. Moreover, there is no room for negotiation as their conditions are fixed once they are deployed on the blockchain.[94] Thus, the idea of acquiring or licensing

81 For more information, see Section 7 'Recommendations for Improving the Transparency of Patent Ownership Changes' in Gorbatyuk and Kovács (n 31) 534–538.

82 Bodó, Gervais and Quintais (n 1) 320–322, 331–335; Gürkaynak and others (n 1) 856–858; Tom Lyons, Ludovic Courcelas and Ken Timsit, 'Legal and Regulatory Framework of Blockchains and Smart Contracts' (EU Blockchain Observatory and Forum 2019) 22–25 <https://www.eublockchainforum.eu/reports/legal-and-regulatory-framework-blockchains-and-smart-contracts> accessed 1 September 2023.

83 Lyons, Courcelas and Timsit, 'Legal and Regulatory Framework of Blockchains and Smart Contracts' (n 82) 33–35.

84 Faustine Fleuret and Tom Lyons, 'Blockchain and the Future of Digital Assets' (EU Blockchain Observatory and Forum 2020) 5-7, 12 <https://www.eublockchainforum.eu/reports/blockchain-and-future-digital-assets> accessed 1 September 2023.

85 Kostopoulos and others (n 6) 4–5, 41–42.

86 Bodó, Gervais and Quintais (n 1) 314–315.

87 On top of that, trading in NFTs comes with its own risks. See Kostopoulos and others (n 6) 41–42.

88 Clark (n 1) 32–33; Gürkaynak and others (n 1) 849, 853, 857–858.

89 Christidis and Devetsikiotis (n 40) 2296–2297.

90 De Filippi and Wright (n 14) 72–88.

91 Christidis and Devetsikiotis (n 40) 2296–2297.

92 Bodó, Gervais and Quintais (n 1) 315–316.

93 De Filippi and Wright (n 14) 199–201; Lyons, Courcelas and Timsit, 'Legal and Regulatory Framework of Blockchains and Smart Contracts' (n 82) 24–25.

94 This means that smart contracts are a 'take it or leave it'

a patent with 'one click' is tempting but, at this point, arguably unrealistic. It is hard to imagine that any lawyer or representative of a legal department would advise their client to accept standard terms inbuilt into a smart contract in the form of code without any attempt nor a possibility to renegotiate. As mentioned above, what could be executed in the form of a 'smart' contract, is the formal validation of new transactions. Finally, hosting smart contracts on a blockchain network has technical consequences which can impact transaction throughput.[95]

49 Fifth, there are also a variety of relevant concerns regarding the scalability, interoperability, and sustainability of blockchain technology.[96] A first remark relating to scalability is the question of which information would/should actually be stored on the blockchain.[97] In our hypothetical example, visualised in Figure 1, we chose to only incorporate the cryptographic hash values in the blocks (which function as a link), whereas the underlying information (e.g., the actual patent file and the related bibliographic information) would be kept 'off-chain' in a regular patent register or a database.[98] In that manner, blocks would only contain the necessary amount of information (i.e., the transaction and a link to the related repository). This would keep the blockchain application more efficient and scalable, as the majority of data would be stored elsewhere. However, even in this scenario such patent blockchain will, in principle, only grow, resulting in an increasing amount of data that needs to be stored by the nodes. Hence, it can be expected that running a node in such a network for a longer time will require significant storage capacity.[99]

50 Subsequently, there is the interoperability aspect of blockchain technology. Due to the young market for blockchain technology and the variety of blockchain (network, application, service) providers, the deployed technology can still vary significantly.[100] This can be detrimental to users (e.g., vendor lock-in or lack of cross-chain communication) and necessitates the establishment of standards and interoperability requirements.[101] Another dimension of this issue is the required interoperability with existing, non-blockchain infrastructure, which may remain in operation or be gradually replaced.[102]

51 Finally, sustainability is another often discussed issue regarding blockchain technology. Indeed, the bitcoin blockchain consumes large amounts of energy due to its reliance on mining in the context of the PoW consensus mechanism.[103] This is different, however, for permissioned blockchains, which reach consensus in a different manner (and do not rely on energy-intensive consensus mechanisms). [104] Nonetheless, sustainability should remain a concern for every technology being developed nowadays.

E. Governance of blockchain-based patent marketplaces: choosing between patent offices or private entities

52 To date, none of the patent offices has attempted to introduce blockchains into their patent registers. However, the European Union Intellectual Property Office (EUIPO) has turned to blockchain to optimise its trademark and design databases. The organisation acknowledges the many benefits this technology could offer for the maintenance of trademark and design data on a global level and is gradually adding national trademark offices to its blockchain

proposition. Gürkaynak and others (n 1) 849.

95 This relates to the difference between a so-called UTXO-model or an account-based model. See Christidis and Devetsikiotis (n 40) 2295–2297.

96 Tom Lyons, Ludovic Courcelas and Ken Timsit, 'Scalability, Interoperability, and Sustainability of Blockchains' (EU Blockchain Observatory and Forum 2019) 5–21 <https://www.eublockchainforum.eu/reports/scalability-interoperability-and-sustainability-blockchains> accessed 1 September 2023.

97 The scalability issue is determined by the so-called *blockchain trilemma* in which the transaction volume and speed have to be weighed against the required level of security and the amount of decentralisation. *In casu*, by using a permissioned blockchain, the level of decentralisation is reduced which allows to preserve scalability and security. Vitalik Buterin, 'Why Sharding Is Great: Demystifying the Technical Properties' (2021) <https://vitalik.ca/general/2021/04/07/sharding.html> accessed 1 September 2023; Lyons, Courcelas and Timsit, 'Scalability, Interoperability, and Sustainability of Blockchains' (n 96) 10–11.

98 Chandratre and Pathak (n 58) 3-4, 6.

99 Gürkaynak and others (n 1) 860.

100 Rauchs and others (n 46) 21–63.

101 Hoyal (n 55) 19; Gürkaynak and others (n 1) 861.

102 Lyons and Courcelas (n 53) 21.

103 European Commission and others (n 40) 33; Lyons, Courcelas and Timsit, 'Scalability, Interoperability, and Sustainability of Blockchains' (n 96) 12–13.

104 European Commission and others (n 40) 33; Lyons, Courcelas and Timsit, 'Scalability, Interoperability, and Sustainability of Blockchains' (n 96) 12–13.

network.[105] Outside of the IP field, blockchain technology has been successfully introduced by public services managing, for instance, land registries.[106]

53 Nonetheless, blockchain-based patent marketplaces (which go beyond the functionality of blockchain-based patent platforms by offering the possibility to transact) are currently being developed by private entities, such as IPwe (introduced in Section D.II.). This dynamic triggers fundamental concerns about the privatisation of patent governance, as private entities allegedly attempt to commercialise partially publicly available patent data and appropriate certain functions of patent registers.

54 The core underlying motivation behind blockchain-based patent marketplaces established by private entities is most often profit-generation. They attempt to offer stakeholders a multifunctional platform that provides a variety of customer-oriented services on commercial terms. Facilitation of patent transactions and their registration is frequently one of the offered services. For instance, IPwe aims to become a go-to place for managing IP portfolios without relying on IP experts, such as patent attorneys, permitting to minimise associated transaction costs. Apart from the possibility to trade patents, the platform also provides its users with AI-generated IP analytics, including analysis of the value of certain IP assets or assessment of IP-related risks.[107]

55 Considering the rise of blockchain-based patent marketplaces, it is essential to review whether patent offices or private entities are in the best position to offer blockchain-based patent trade-related services. In general, powering patent registers by blockchain technology could be justified by public interests inherent in the 'quid-pro-quo' of the patent system. It aspires to further increase 'active' transparency of patent information (the disclosure function)[108] to stimulate the exchange of knowledge and technological progress. However, as explained in Section C, patent offices do not involve themselves in such business-related matters as patent trade, as their core tasks are patent examination and dissemination of patent information. The only patent trade-related obligation they currently impose on patent rightsholders is the registration of licenses and assignments to ensure transparency of rightsholders in patent registers. However, this obligation is regularly neglected due to the rather weak underlying enforcement mechanisms.[109] Even though facilitating patent transactions is not a direct obligation of patent offices, by taking on board this task patent offices, in our view, can significantly simplify patent trade.

56 To facilitate knowledge exchange and decrease associated costs of patent transactions, blockchain-based platforms or marketplaces should ideally contain complete, accessible, up-to-date, and reliable/accurate patent data. As explained in Section D.II., blockchains are particularly suited to efficiently transmit up-to-date data due to their automated and decentralised nature. The accuracy of transmitted data may not always be guaranteed, but certain shortcomings can be mitigated depending on the selected structure, functionality, and governance of the underlying blockchain. Thus, both blockchain-based marketplaces governed by public or private actors can disseminate up-to-date data. Similarly, neither can assure absolute data accuracy. Yet, blockchain-based platforms or marketplaces governed by patent offices have clear advantages over private initiatives with regard to the dissemination of complete and accessible data.

57 By increasing cross-patent register cooperation and stimulating digitisation of patent information (in line with the criteria put forward in

105 For more information, see <https://euipo.europa.eu/ohimportal/en/news/-/action/view/8662923> accessed on 1 September 2023. So far, the network has four participants: the EUIPO, the Maltese Commerce Department, Estonian Patent Office and the Lithuanian State Patent Bureau. See EUIPO, 'Blockchain at the Service of IP Owners and Consumers' (*Alicante News*, 2022) <https://euipo.europa.eu/ohimportal/en/web/guest/-/alicante-news-july-2022-blockchain-at-the-service-of-ip-owners-and-consumers?inheritRedirect=true&redirect=https%3A%2F%2Feuipo.europa.eu%2Fohimportal%2Fen%2Fweb%2Fguest%2Fsearch%3Fp_p_id%3Dcom_liferay_portal_search_web_portlet_SearchPortlet%26p_p_lifecycle%3D0%26p_p_state%3Dnormal%26p_p_mode%3Dview%26_com_liferay_portal_search_web_portlet_SearchPortlet_keywords%3D9454411> accessed 1 September 2023.

106 Lyons, Courcelas and Timsit, 'Blockchain for Government and Public Services' (n 61) 12, 28.

107 For more information, see <https://ipwe.com/your-secure-gateway-to-efficient-ip-monetization-and-risk-mitigation/> accessed on 1 September 2023.

108 "The principle of transparency is one of the key principles of property law and can be divided into "passive transparency" and "active transparency". Whereas the objective of passive transparency is to ensure that certain information is available and accessible, the objective of active transparency is to ensure that information is not only available but is also complete, accurate, reliable, and useful." Gorbatyuk and Kovács (n 31) 534; Arina Gorbatyuk, 'Rethinking Registration of Intellectual Property: The Issue of (the Lack of) Transparency of Intellectual Property Ownership', *Rethinking IT and IP law* (Intersentia 2019) 237.

109 Gorbatyuk and Kovács (n 31) 527.

Section D.II.), blockchain-based patent platforms (with or without transactional functionality) can offer a complete 'global' patent dataset to their users, as patent offices are responsible for collecting this data in the first place. On the contrary, blockchain-based patent marketplaces established by private entities (e.g., IPwe) only contain patents that patent rightsholders are interested in displaying or offering for trade. They rely on stakeholders' interest to join their commercial platform and utilise the offered services. Thus, in its scope, such marketplaces are currently closer to a 'local store' for a selected group of interested individuals (customers) than a revolutionary global patent marketplace. It is highly unlikely that private entities could develop a dataset equivalent to the one offered by patent registers unless they attempt to privatise publicly available patent information. Even if a relatively large dataset could be assembled, another quest would be to attract a large number of patent rightsholders interested in trading their patents via the offered privately governed blockchain-based marketplace. In this case, patent offices again have an advantage as many digitally advanced patent offices have already adopted digital procedures (e.g., myEPO), involving user-profiles and cybersecurity measures (e.g., passwords and electronic signatures) whose function could be extended to the blockchain network.

58 The accessibility of patent information is one of the core goals of patent disclosure obligations. It offers third parties the possibility to access collected patent information without any barriers and free of charge. Patent offices share this valuable data with third parties through their bulletins, registers, and databases on a nonpecuniary basis. Private entities, establishing patent marketplaces, are not under any legislative obligation to either give access to their dataset to any interested third party (it is also not in line with their commercial interests) or cooperate with patent offices. Thus, if patent rightsholders opt to trade their patents via privately governed blockchain-based marketplaces, there is a risk that the information on patent transactions becomes largely non-transparent. It is important to ensure that patent offices provide an appealing alternative to those private initiatives to ensure that the information on patent transactions is processed by patent offices and is accessible to all interested third parties.

59 It can be concluded that it is in the public interest to incentivise patent offices to consider developing blockchain-based platforms (and possibly marketplaces) or other innovative digital alternatives or enhancements of their existing practices. By doing so, they can prevent legal uncertainty and fragmentation of important patent information (such as up-to-date information on rightsholders), which would be the result when such marketplaces are managed by private entities. Thus, private entities could focus on offering their users patent-related business analytics but should refrain from asserting the role of patent trade intermediaries, as their interference may distort the legislatively established 'quid-pro-quo' balance of the patent system.

F. Concluding remarks

60 Incorporating blockchain technology into patent registers holds the potential to improve the efficiency of patent transactions. As opposed to other authors who argue that 'searchable archives of accepted patents [...] cannot be replaced by blockchain technology'[110], we do believe that blockchain technology could improve and advance the functionality of patent registers. To facilitate patent transactions and decrease related costs, relevant actors should ideally have access to complete, accessible, up-to-date, and accurate patent information, not only vis-à-vis the subject matter of inventions but also rightsholders. By integrating blockchain technology into their patent registers, patent offices can turn their (national or regional) patent registers into global and automatically updated platforms that could come closer to providing this 'ideal' patent data.

61 To illustrate how blockchains could facilitate patent trade, we put forward a (partial) proposal on how such a blockchain-based patent platform can be configured. In particular, patent offices could collectively govern a public permissioned blockchain to exchange and publicly disclose their patent data and related updates. Although this hypothetical blockchain may not be categorised as distributed ledger technology *sensu stricto*, we believe that it provides an insightful framework to start rethinking the current functioning and structure of patent registers.[111]

62 We claim that patent offices are best placed to set up and govern such a blockchain-based patent platform. In close cooperation, they can offer their users complete patent data and provide the technological basis for a 'global' patent market instead of 'local' patent stores currently provided by private entities. We acknowledge that this complete 'global' patent market is a long-term goal as it is conditioned on a high level of digitisation of processes of all patent offices and patent actors involved. In addition, access to a blockchain-based patent platform governed by patent offices is to be granted free of charge to any interested party in conformity with their regulatory

110 Boucher (n 57) 11.

111 Rauchs and others (n 46) 11, 20.

obligation to disseminate patent information and in line with their goals to improve the accessibility and transparency of patent data.[112]

63 Conversely, as private entities are not bound by any legal obligations to give access to their platforms or cooperate with patent offices, the 'privatisation' of blockchain-based patent platforms and marketplaces can further increase fragmentation of patent data, limit its accessibility, and diminish transparency on patent rightsholders. Consequently, patent offices should take charge of this discussion and involve other stakeholders in the patent and blockchain community to uncover possible (digital) alternatives to the existing processes and infrastructure and identify political, legal, economic, and technical challenges hindering the transition from 'reference' patent registers to a global blockchain-based patent platform.

64 **Acknowledgements**: This paper was made possible thanks to the generous funding of the Research Foundation - Flanders (postdoctoral FWO fellowship (1256621N) granted to Dr. Arina Gorbatyuk) and support of the Max Planck Institute for Innovation and Competition.

112 EPO, 'Annual Review 2020' (2021) 50 <https://www.epo.org/about-us/annual-reports-statistics/annual-report/2020/goal4.html> accessed 3 January 2023; Michelle K Lee, 'The Benefits of Transparency Across the Intellectual Property System' (2014) <https://www.uspto.gov/about-us/news-updates/benefits-transparency-across-intellectual-property-system> accessed 4 September 2023.

Exploring the Viability of AI as Judicial Replacements: a Cautionary Perspective

by **Gabriel Ernesto Melian Pérez**

Abstract: Considering the high pace of technological development, it is not futile to wonder whether AI could ever replace judges. This work analyzes this possibility and speculates on one fundamental question: Could AI effectively replace judges in all their functions? The paper proposes a cautious view: it counsels a comprehensive conception of the judicial function, where the human judge fulfills a much more complex role than just interpreting the norm and applying it to concrete cases. AI's lack of social understanding, moral agency, and rational autonomy prevents it from performing the fundamental social governance role of the judge. It does not seem that, in most cases, AI should go beyond a purely supportive role.

Keywords: Artificial Intelligence, Moral Agency, Rational Autonomy, Social Understanding, Social Governance, Judge.

Recommended citation: Gabriel Ernesto Melian Pérez, Exploring the Viability of AI as Judicial Replacements: a Cautionary Perspective, 14 (2023) JIPITEC 619 para 1.

«A legal system can be conceived without laws, but not without judges.»

FRANCESCO CARNELUTTI

A. Introduction

1 The last century saw important changes in many areas of science and technology. The advent of computers meant one of the most important changes of our time and with them the emergence of the Internet and Artificial Intelligence (AI). Humanity has entered into what some authors have called the post-industrial era[1], the society of knowledge and information.

2 We live in a world "governed" by computers. These machines have the ability to solve difficult problems, in many cases better and faster than the human brain. They are not only useful in large manufacturing companies, in the construction of gigantic buildings, or in scientific projects, but they are also useful tools for lawyers. The computer's ordering and storage capabilities have made it incredibly easy to archive and retrieve legal data, court records, case law, and legislation. Now, the Internet offers us much more, all the knowledge of the world on our desktop. All

* LL.M. Göttingen, PhD fellow , Civil Law Department, Pompeu Fabra University.

1 Daniel Bell is recognized as one of the first to use and develop the term, especially from his book "The Coming of the Post-Industrial Society" in 1973. As well as Yoneji Masuda, in "An Introduction to the Information Society", 1968.

the information that we might need in the practice of law is there for us to consult. The next step would be to organize and analyze this massive amount of data. This is where AI becomes especially helpful[2].

3 Some time ago, AI abandoned the specter of science fiction to enter our lives. It is called to play a leading role in a revolution comparable to that which generated the Internet. However, their wide capabilities have awakened a fear in humanity: a feeling of replaceability. Every day people wake up wondering whether a new technological development could make us obsolete in our jobs[3]. AI provokes such existential questions.

4 The concept of "AI as courts" has been the subject of recent controversy and discussion, as many doubt whether AI can effectively replace the role of the judge. The urging question is whether judges will survive modern technology or whether, on the contrary, AI will allow computers to resolve disputes, perhaps with greater speed, objectivity, and independence. Under this reality, this short paper will analyze whether the human judge would surrender to the technological invasion, and if so, whether this would be desirable or positive. Regarding this issue, this paper adopts a cautious position. It upholds that implementation of the AI judge could bring advantages in some aspects, but it could be problematic in others. While its implementation could quicken the process, resolving more cases in less time, AI's lack of social understanding, moral agency, and rational autonomy would prevent it from performing the fundamental social governance role of the judge. Therefore, AI could be used to assist human judges, rather than replace them.

5 The paper is structured as follows: a first section is devoted to explaining basic issues about how AI works. The second section outlines some advantages of implementing AI in the judicial process and some real cases where it is already in use. A third section summarizes the problems that the literature commonly associates with the implementation of AI in judicial processes. The fourth section will develop the hypothesis by explaining which essential characteristics or functions of the judge are impossible to reproduce by AI and why such a substitution would ultimately be neither appropriate nor desirable. The choice of topic was encouraged by an essential motivation: to determine what characteristics and qualities define judges in the process of dispensing justice and whether such characteristics can be emulated by any AI technology. In this sense, the preliminary conclusion turns out to be rather cautious.

I. Artificial Intelligence

6 In the 20th century, society became familiar with artificial intelligence mostly through art. The work of Isaac Asimov's "I Robot" is an unavoidable reference here. The stories about Robbie, Cutie, Herbie, or Stephen Byerley raise more than one ethical and philosophical question. In the field of science, Alan Turing's vision was perhaps the most influential. Turing started from the premise that humans use available information and reason to solve problems and make decisions, therefore: Why can't machines do the same? Can machines think? (Turing, 1950)[4]. Although these questions were asked more than 70 years ago, we are still debating their likely answers.

7 The earliest AI applications were in formal domains, like theorem proving, that are relatively divorced from the complexity of ordinary human experience. Progress in natural language processing, expert systems, planning, robotics, and qualitative reasoning have extended the range of human experiences and behaviors addressed by AI (Sartor & Branting, 1998). Its potential became well-known to the public in May 1997, when an extremely important event occurred: for the first time in history a machine defeated a world chess champion, the IBM Deep Blue won over the Russian Garri Kasparov[5].

2 "Legal technology", or "legal tech" encompasses a wide range of tools and platforms designed to streamline, enhance, or automate various aspects of the legal profession. They are aimed at improving the efficiency, accessibility, and affordability of legal services. Relevant examples include document automation, case management software, virtual law assistants (Chatbots), and online dispute resolution platforms.

3 For example, the Screen Actors Guild-American Federation of Television and Radio Artists (Sag-Aftra) and the Writers Guild of America (WGA) recently went on strike, warning of the threat AI poses to the jobs of Hollywood actors, writers, and production staff. "*Bargaining for our very existence': why the battle over AI is being fought in Hollywood*", The Guardian, 22/7/1023. Retrieved on 7/8/2023 from <https://www.theguardian.com/technology/2023/jul/22/sag-aftra-wga-strike-artificial-intelligence>.

4 It is important to mention that Turing's "imitation game" was challenged by Searle (1980), who developed in his *Minds, Brains, and Programs* the "Chinese Room Argument". This is used to dispute the claim that a machine can actually understand the meaning of the information it processes. In his words, "*The computer, to repeat, has a syntax but no semantics*" (Searle, 1980, p. 423), which would prevent it from truly emulating the human brain's cognitive capacity. The claims of both authors have been extensively explored and debated.

5 More recently AI has also succeeded in the go game (AlphaGo vs. Lee Sedol in 2015) and in bridge (Nook in 2022).

8 In order to approach AI, we must briefly address the concept of human intelligence with which cognitive-science-experts work. Among several definitions or conceptions of intelligence, the common element is the capacity to process information to solve problems to achieve certain/specific objectives. Basically, our brain controls the capacity to process information from the environment and from our own body, which is used to evaluate and choose future courses of action. This is where the decision making process and evaluation comes in, which consists of selecting, filtering and organizing the available information (Corvalán, 2017). The term AI is then applied when a machine imitates these "cognitive" functions such as: "perceiving", "reasoning", "learning" and "problem solving" (Russell & Norvig, 2016).

9 Haenlein and Kaplan (2019, p. 5) define artificial intelligence as "*the ability of a system to correctly interpret external data, to learn from that data and to use that knowledge to achieve specific tasks and goals through flexible adaptation*". The European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment defines IA as "*a set of scientific methods, theories and techniques whose aim is to reproduce, by a machine, the cognitive abilities of human beings. Current developments seek to have machines perform complex tasks previously carried out by humans...*".

10 It is also necessary to analyze the concept of *machine learning*, because of its importance in decision making. A common misconception is that AI and machine learning are the same thing. AI is a concept that encompasses machine learning. They pursue a single goal: the creation of devices or algorithms that omit or replace human beings by emulating their cognitive functions. Specifically, machine learning allows computer programs to learn complex tasks through experience, rather than through handcrafted computer functions. Machine learning (ML) techniques use computational algorithms on large datasets to find patterns and build models for predicting future events. Unlike statistical tools, ML focuses on accurate predictions rather than understanding the underlying phenomenon or causal relationships between variables. (Harkens *et al.*, 2020, p. 3)

11 Nowadays there are AI systems that create music, paint pictures, recognize faces and objects, detect diseases, and help protect the environment, among many other things. Artificial intelligence is currently advancing and developing at an exponential rate. Recently, the breakthrough of GPT-4 (Generative Pre-trained Transformer) model language by OpenAI caused a great impact due to its high generative capacity[6]. Therefore, one might wonder, if AI can do all this, could it also contribute to the administration of justice?

II. Harnessing AI in court

12 The judicial system in some countries is plagued by excessive costs (for individuals and society), long delays and inconsistencies leading to a growing lack of public confidence. One of the reasons for this is the large amount of information that must be collected and integrated for the legal system to function properly. The number of judges often cannot cope with all the cases that arise. AI could then be a useful tool to improve and facilitate the functioning of judicial bodies.

13 To analyze how AI could be inserted into the judicial process, it is useful to distinguish between two big possibilities: "AI in the court" and "AI as courts"[7]. When we talk about technology "in the courts", we are referring, for example, to digitalization processes. An example of this is when courts are willing to accept complaints through electronic forms, or there is an electronic notification system to remind deadlines. Another level of court digitization is the electronic record/filing system, which provides access to any case file online from anywhere. The videoconference can also be used, which offers courts the possibility of holding hearings remotely in order to expedite proceedings and ensure the safety of children, witnesses and victims. There are fewer problems associated with these proposals because they mostly involve administrative support only.

14 On the other hand, a more radical use of AI ("AI as courts") can operate in the following ways:

15 1) AI could increasingly be used as a support for judges, for example, to identify, organize and select relevant case law, detect patterns in case law or help highlight arguments presented by the parties. Judges could also follow AI suggestions or even let the AI write draft decisions. (*Direct impact on the outcome of cases*)

6 Generally, GPT 4 answers are difficult to differentiate from those of a human. It is this ability to generate natural language that has led some to wonder whether this system will make some occupations obsolete. In this paper we elaborate on this issue, focusing on the role of the judge.

7 According to Sourdin and Cornes (2018, p. 91) "*at the most basic level, technology is assisting to inform, support and advise people involved in the justice system (supportive technology)... Second, technology can replace functions and activities that were previously carried out by humans (replacement technologies) Finally, at a third level, technology can change the way that judges work and provide for very different forms of justice (disruptive technology).*"

16 2) The use of AI in court management promises to generate a wealth of valuable data on the functioning of judicial systems. Thus, AI can be used by users of the justice system to improve their processes and reduce costs through a predictive system. (*Indirect impact on the outcome of cases*)

17 For example, Morison and Harkens (2019, p. 624) discuss the Traffic Penalty Tribunal (TPT)[8] in England and Wales, which enables drivers to appeal tickets via an online platform. It is a relatively easy process, where the user enters the penalty ID together with the arguments he/she considers relevant to his/her defense. Although an automated mechanism designed to facilitate the appeals process, it is a human judge who impartially assesses the evidence and arguments to arrive at a final decision.

18 There does not seem to be much discussion about the advantages offered by digitalization processes in the legal field, where AI is used as a tool to facilitate the daily work of judges and lawyers. These are mainly the so-called ancillary activities, that include preliminary or complementary judicial tasks (e.g., jurisdictional screening, drafting routine court documents, procedural tracking). However, some countries have gone a step further and have begun to allow AI to play a more active role in the decision-making process, a more controversial issue[9].

19 The first online private court in the Netherlands was established on January 11, 2010, offering fully digitalized court proceedings, but decisions were based on human reasoning. However, since 2011, certain types of decisions, specifically e-Court judgments in debt collection proceedings, have been solely rendered as the outcome of AI without human involvement.

20 Estonia has also been at the forefront of developing "virtual judges" based on Artificial Intelligence[10]. The Estonian Ministry asked Ott Velbsberg and his team to implement artificial intelligence in smaller trials, those involving disputes of 7,000 euros or less. AI would allow for the acceleration of dozens of backlog cases that judges and court clerks cannot currently handle. Its application will work as follows: the two parties will upload their documents and information relevant to the case onto a platform, where the AI will make a decision that can be appealed by a "human" judge[11].

21 In early 2023, it made headlines that a judge in Colombia for the first time openly incorporated generative artificial intelligence into his judicial ruling. In a case involving an "acción de tutela", a constitutional remedy, the first instance judge ruled in favor of the plaintiff and, on appeal, Judge Juan Manuel Padilla upheld the decision while using ChatGPT-3 to provide additional information on the scope of the "acción de tutela". He argued that a recent Law 2213/22 allows the use of AI systems such as ChatGPT to expedite judicial decision-making.[12]

22 Chinese courts are also using AI to assist with making legal decisions. As reported by Chen and Li (2020, p. 15) "*new to the Zhejiang High People's Court is a virtual judicial assistant who specializes in financial loan disputes—Xiao Zhi. Xiao Zhi's duties extend beyond administrative tasks like scheduling. Xiao Zhi supports judges by analyzing case filings, summarizing points of contention as they are raised during trial, evaluating evidence, calculating awards, and drafting judicial documents on the fly*". Xiao Baogong Intelligent Sentencing Prediction System, another legal AI platform, is also used by judges and prosecutors in criminal law. The system has the capability to recommend penalties by analyzing vast amounts of case information and previous rulings in similar

8 <https://www.trafficpenaltytribunal.gov.uk/want-to-appeal/>

9 The use of Artificial Intelligence in decision-making has been used not only in judicial processes, but also in other relevant fields such as credit granting, subsidies and social benefits, insurance, human resources and employment, and diagnosis or treatment of diseases. Because this paper focuses on the judicial domain only, there is no space to address the ethical and legal issues of using massive amounts of data to develop automatic predictive models that impact dramatically people's lives. This is a topic that is also worth developing and researching further.

10 "*Your Honor, AI*", Harvard International Review (April 2020). Retrieved on July 31, 2023, from <https://hir.harvard.edu/your-honor-ai/>. "*Can AI Be a Fair Judge in Court? Estonia Thinks So*", Wired (25 March 2019). Retrieved on July 31, 2023, from <https://www.wired.com/story/can-ai-be-fair-judge-court-estonia-thinks-so/>.

11 However, the Estonian Ministry of Justice released a statement in 2022 explaining that this conception echoed by some media outlets is misleading: "*Estonian Ministry of Justice does not develop AI robot judge for small claims procedure nor general court procedures to replace the human judge... More precisely, Ministry of Justice is looking for opportunities for optimization and automatization of court's procedural steps in every types of procedures, including procedural decisions where possible... One of the aims is that all court cases are held digitally...*". Retrieved on July 31, 2023, from <https://www.just.ee/en/news/estonia-does-not-develop-ai-judge>.

12 "*Colombian judge says he used ChatGPT in ruling*", The Guardian (3 Feb 2023). Retrieved on August 8, 2023, from <https://www.theguardian.com/technology/2023/feb/03/colombia-judge-chatgpt-ruling>.

cases using big data analysis.[13]

23 Brazil is another country that has begun to use AI to assist in judicial processes. According to DR.IA (Laboratório de Direito e Inteligência Artificial) of the University of Brasilia: "*The Victor is an AI system applied to cases pending in the Brazilian Federal Supreme Court and seeks to facilitate the process of identifying the so-called general repercussion, contributing to increased performance and efficiency in the processing stages of extraordinary appeals in the Court*"[14]. Although it is not the Victor system that provides the final decision, its indirect impact on it seems relevant.

24 Artificial intelligence is sometimes not used to elaborate the judgment as such, however, the information it provides has a significant impact on the final decision. Take, for example the i-RATS (intelligence-led risk assessment tools) which are based on information primarily obtained from publicly-available documents. Yeung and Harkens (2023) analyze three of these tools: the London Gangs Matrix[15], the Durham 'HART' tool, and the Dutch SyRI tool. Each of these tools serves different purposes, such as reducing gang violence, improving offender rehabilitation, and efficiently identifying social welfare fraudsters. Despite their distinct technical features and objectives, all these tools generate algorithmic assessments of an individual's 'risk.' These assessments are then used by front-line decision-makers to determine appropriate actions against the individuals in question.

25 Even law firms' use of this technology is influencing how they operate, and this indirectly influences the judicial process. The increasing use of AI in the legal field, like predictive coding, predictive analytics, and machine learning, is already changing how lawyers present evidence to judges and assess client risk within law firms[16]. (Sourdin, 2018, p. 1115)

26 According to new research published in the journal PeerJ Computer Science, scientists at University College London, the University of Pennsylvania and the University of Sheffield have succeeded in developing a method that can predict the outcome of an international supranational court by analyzing trial texts using the automatic learning that is common in Artificial Intelligence. In 2016, they - only with machine learning - managed to predict the decisions of the European Court of Human Rights by 79% (Aletras, Tsarapatsanis, Preotiuc-Pietro, & Lampos, 2016). According to Nikolaos Aletras, the main author of the research, "*Artificial Intelligence cannot replace judges or lawyers, but it is useful in identifying certain patterns that will obtain certain results. This tool could be very valuable in finding out which cases may violate the European Convention on Human Rights*"[17].

27 It is clear that judges and the current judicial system are not perfect. By using AI judges, we could exclude public pressure as a decisive factor in decision-making as these systems do not take the expectations of the press or the public into consideration. We could also rule out the problem of bribery. The use of algorithms, in principle, leads to improvements in efficiency, speed, predictability and security. However, does this mean that judges should be replaced by technology in order to gain efficiency and speed? Arguably not, or at least, this is not the solution that this paper argues for. This is partly because there are so many factors that impact on judicial decision-making, as it will be discussed later on. Then, it is time to analyze the phenomenon of AI as courts and its potential handicaps, moral and ethical implications.

III. Problems arising from the implementation of the AI judge

28 The first problem that arises when we think about replacing human judges is, "*as some commentators*

13 "*How China's AI is automating the legal system*", DW (20 Jan 2023), Retrieved on August 8, 2023, from <https://www.dw.com/en/how-chinas-ai-is-automating-the-legal-system/a-64465988>.

14 <http://dria.unb.br/teste-top/projeto-victor-stf-unb>.

15 "*Although not originally intended, the Matrix is also allegedly used in evidence to support the prosecution of gang-related offences*" (Yeung and Harkens, 2023, p. 3). So, although it was actually designed for use by the police, it has also been also used in court proceedings.

16 There are legal technology companies that specialize in designing services for lawyers, providing comprehensive access to judicial information and case law. With the use of these electronic tools, law firms want to reduce legal uncertainty and unpredictability of court decisions. At this point, it would be appropriate to introduce a disclaimer. The criticism intended in this paper focuses on the direct impact of artificial intelligence on judicial work. Algorithms are known to be used by lawyers and paralegals for the analysis of documents during litigation and the prediction of case outcomes. While these algorithms can influence the outcome to some extent, their main application is to assist lawyers rather than to directly influence the judicial process. So, they are not the subject of the discussion here. Note that in the following, we will not refer to this category of artificial intelligence, but rather to that which is used as a direct substitute for the judicial function.

17 "*AI predicts outcomes of human rights trials*", UCL News (24 Oct 2016). Retrieved on 31/7/2023 from <https://www.ucl.ac.uk/news/2016/oct/ai-predicts-outcomes-human-rights-trials>.

have pointed out, the question of how to accurately translate the law into codes, commands and functions that a computer program can understand and apply. Legal language is nuanced and often requires contextual understandings" (Sourdin, 2018, p. 1127). The clearer and more concise a legal rule is (the fewer exceptions it admits and the fewer vague terms it uses), the easier would be for AI systems to apply it. This could have controversial long-term consequences on the design of the laws since the rules would be developed with the objective of being interpreted by an AI and not by a human. Therefore, it is likely that the rules in the future would have a particular structure with the easy interpretation by the AI in mind. According to Sourdin (2018, p. 1128) *"such amendments may result in unfair or arbitrary decisions due to the lack of individualized justice and discretion, and a lack of nuance in the law".*

29 As it was previously mentioned, there are some countries that have already implemented in one way or another the use of AI judges. In principle, this has been authorized in cases that have the characteristic of being less controversial to automate: non-rivals and non-complex cases. The supporters usually argue that an automated system to solve cases of this kind, can help to decongest the judicial bodies and offer faster, more impartial, and reliable responses. Non-rival cases are those where the parties are in full agreement on the desired outcome. They may even collaborate with each other and with the judge to achieve that outcome. Think, for example, of divorce cases where both parties agree on the terms of the separation. However, the more complex a case is, the more difficult it is for the AI to solve. This refers, first, to the complexity that is directly related to the specific aspects of the case such as the number of witnesses, documentary evidence, and the number of parties. But it also refers to the complexity of the legal matter itself. Certainly, it is not the same when, within the same divorce case, there are one or more children, and the judge must decide who gets custody. The human dimension plays a more important role in this case[18].

30 There are some issues associated with AI that are still problematic and may also be pertinent to include in the discussion. One significant concern about AI judges is their dependence on a power source, making them vulnerable during power outages. Another critical risk is their susceptibility to hacking. If they are hacked, it could lead to severe consequences, potentially undermining citizens' privacy, and the integrity of the judicial process. It is usually argued that conventional judicial litigation is costly and that these technologies could lower costs. Although this seems like a good argument in principle, the development, programming, and maintenance of robot judges would also likely entail substantial costs. Moreover, not everything should be measured in terms of money since the environmental impact of their energy consumption might also be overlooked (Dhar, 2020; Van Wynsberghe, 2021). The latter deserves further study.

31 There is also the problem of non-existent input data. These AI programs work with datasets full of judicial precedents on which they base their decisions. What would happen if a totally new case was brought before the AI and no precedent existed? Obviously, the AI should not produce any results, unlike a human judge who is obliged to settle the case even if there is no precedent. To make matters worse, generative artificial intelligences such as the GPT 3 Chat almost never produce an "I don't know" answer. Usually, in the absence of enough data to produce a meaningful answer, the AI ends up giving false, fictitious, or incoherent answers.

32 Another of the limitations traditionally attributed to AI is its inability to understand contextual elements. In an effort to remedy this, it is fed large amounts of data, which often turns out to be personal data. However, this is also controversial since privacy laws and data protection laws impose limitations on the collection and processing of "personal data". This could be deemed disproportionate and a violation of the right to privacy under Article 8(1) of the European Convention on Human Rights (ECHR)[19].

1. I. AI biases. The case of COMPAS

33 It is generally claimed that AI is desirable over humans because one of the advantages of these mechanisms, theoretically, is the absence of emotions or personal biases. After all, the AI does not care about people's money or status, it judges everyone equally. It is neutral, fair, and objective. However, as Fahimi and Lücking (2021) rightly point out this is just a common myth. The fact is that "*as part of society, AI is deeply rooted in it and as such not separable from structures of discrimination. Due to this socio-technical embeddedness, AI cannot make discrimination disappear by itself*". Several authors have remarked that AI tools can reproduce existing societal biases and ultimately ends up perpetuating

18 Further discussion of this issue will be provided in section E.

19 General Data Protection Regulation (GDPR) effective from 2018 in the European Union includes a provision granting individuals the right not to be subjected to decisions based entirely on automated processing, such as profiling if such decisions have legal consequences (Article 22(1)). This suggests an awareness of the potential risks and limitations associated with complete reliance on algorithmic decision-making.

structural discrimination[20] (Flores, Bechtel and Lowenkamp, 2016; Chander and Krishnamurthy, 2018; Noble, 2018; Sourdin, 2018; Yapo and Weiss, 2018; Wachter, Mittelstadt and Russell, 2021; Angwin *et al.*, 2022).

34 In United States, AI has been implemented to support judges in estimating the likelihood of recidivism and the risk of evasion when deciding whether to grant bail. Although it leaves the decision up to the human judge, AI still has a strong impact on the outcome of the case. One of the most notorious and discussed cases is the Correctional Offender Management Profiling for Alternative Sanctions, or COMPAS[21]. It was designed to help make evidence-based decisions through assessment (based on 137 questions answered by the offender during an interview, and information obtained from criminal records) and ultimately reduce recidivism and increase public safety (Angwin *et al.*, 2022). By assessing the criminal history and criminological factors such as socio-economic status and stability, family history, employment, etc., the algorithm provides a report that includes a risk score calculated on a scale of 1 to 10. A risk average then appears which evaluates whether someone can be released on bail, sent to prison, or receive another punishment. When the person is already incarcerated, the algorithm also determines whether they deserve the benefit of parole.

35 With COMPAS, the judges only get a result, but they don't know how exactly the AI reached that conclusion. This is known as "the black box problem". A black box, by definition, is a system whose inputs and outputs are known, but the operation of that system is unknown (Deeks, 2019). It is usually difficult to access the code of these systems because they are legally protected by trade secret. This is the case of COMPAS, which works through a proprietary algorithm. This lack of transparency in a judicial process is, to say the least, objectionable[22].

36 This tool has already been legally assessed by the Wisconsin Supreme Court in *Loomis v. Wisconsin*[23]. The court determined that the use of COMPAS was not contrary to the right to due process, as alleged by the defendant[24], who had been sentenced to 6 years based on the results shown by this algorithm. Despite denying the appeal, Justice Bradley remarked that judges should proceed with caution when using such risk assessments. The judge stated that *"[i]t is very important to remember that risk scores are not intended to determine the severity of the sentence or whether an offender is incarcerated"* and that studies *"have raised questions about whether [COMPAS scores] disproportionately classify minority offenders as having a higher risk of recidivism"*[25]. Therefore, the court finds that judges must also explain the factors, other than the evaluation that support the decision made.

37 This case highlights the importance of careful data selection and algorithm design to minimize such biases. Biases may arise if data is collected or sampled in a way that over- or under-represents certain groups, skewing the AI system's performance. AI systems learn patterns from the data they are trained on, and if the data contains human biases, the AI system may also reflect those biases in its decisions. It is important to have access to and monitor the code and dataset of these algorithms, as there is a risk that creators will incorporate, intentionally or unintentionally, biases, prejudices or other elements in the same programming that somehow "contaminate" the outcome[26].

38 As indicated by Yeung and Harkens (2023), technical developers typically consider contextual factors as irrelevant "noise" due to a "contextual detachment mindset". They are trained to abstract prediction models from legal and constitutional considerations.

20 The core of AI technology lies in the data that it relies on, if data presents any inconsistency or bias, this will be reflected in the outcome. Noble's (2018) highlights how search engines and platforms, through their recommendations system, can (re)produce and perpetuate societal biases, including racism. Failure to recognize this issue could be dangerous. As is shown in the COMPAS case, algorithms used in the administration of justice are not free from this problem either.

21 Developed by a private company called Equivant (formerly Northpointe).

22 "*Most notably, many such tools are limited in their capacity to enable full and precise accounts of both the factors producing their calculative output and the weighting of relevant characteristics derived from training data. This hinders the ability to provide functional explanations concerning how an output has been generated*" (Harkens *et al.*, 2020, p. 25). In view of its legal relevance, this issue will be further addressed in section E.

23 881 N.W.2d 749 (2016).

24 Mr. Loomis appealed arguing that the basis of his sanction was an undisclosed algorithm, making it impossible to assess and thus violating due process.

25 The judge here may be referring to the well-known case study on AI bias, conducted by Propublica (Angwin *et al.*, 2016), which revealed that although the software was designed to maximize overall accuracy, it exhibited a significant bias. Specifically, it had twice the false positive rate for African Americans compared to Caucasians.

26 The new Artificial Intelligence Act in Europe would incorporate certain obligations in this regard, requiring companies developing these technologies to ensure that there is no bias in the AI training process.

However, the authors argue that algorithmic tool developers and authorities overseeing their implementation often fail to recognize or understand the constitutional and legal implications of these technical choices. In other words, the disconnect between technical development and legal implications may lead to unforeseen problems and biases in algorithmic systems.

39 Modern risk assessment tools rely on algorithms trained with historical crime data, potentially leading to the replication of biases and past mistakes. Machine-learning algorithms use statistics to identify patterns in the data, which might be associated with crime but not necessarily causations (O'Hara, 2020, p. 4). Using statistical correlations from historical data can be misleading and doesn't guarantee accurate predictions.

40 As it has become clear, the implementation of artificial intelligence in court proceedings has important implications that impact the guarantees of due process and other fundamental rights of citizens. The literature has addressed each of these issues to a greater or lesser extent, and some have even attempted to provide solutions. Although it must be recognized that the mentioned issues are sensitive and have a considerable legal relevance, this paper still argues that they may have a solution in the medium or long term due to technological progress itself, which will allow the development of better IAs. However, even if this technology reaches such a state, there are still essential elements of the judicial function that the most advanced technology will hardly be able to emulate. In the next section we will discuss what are those inherent characteristics of the judicial function that make the human judge irreplaceable.

IV. Moral agency, rational autonomy, and the social dimension of the judicial function

41 When someone thinks of the judicial function, the first thing that comes to mind is case management and resolving disputes. But the judge's role goes far beyond this[27]. Judicial commentary helps shape society's functioning, and judges also play an educational role, guiding litigants and lawyers and contributing to civic education (Sourdin and Cornes, 2018). Advocates of replacing judges with AI overlook the broader contributions judges make to society, including matters of compliance and acceptance of the rule of law, which go beyond mere adjudication (Sourdin, 2018). In the words of Sartor and Branting (1998, p. 105):

> *"Judicial decision-making is an area of daunting complexity, where highly sophisticated legal expertise merges with cognitive and emotional competence. Many of the central concepts in the judicial application of the law – such as "justice", "reasonable care", and "intent" – are deeply enmeshed in the fabric of human life. Judicial decision-making requires assessing the credibility of witnesses, evaluating the probative weight of evidence, interpreting the meaning and intended effect of legal statutes and other normative authorities and, especially in criminal cases, balancing mercy with justice. The hazards of replacing judicial discretion with a rigid computer model can hardly be overestimated".*

42 The aim of this section will be to analyze these distinctive features of the judicial service in order to assess the extent to which the human element is central or relevant to its practice.[28]

1. Two interdependent functions

43 What does a judge do? Well, the most simplistic view would say that the ideal prototype of courts is where an independent adjudicator applies the law to the facts, leading to a decisive ruling declaring one party legally right and the other legally wrong. However, most people today challenge this reductionist and formalistic approach[29]. Fiss (1979), for example, considers that the resolution of cases is not the main purpose of judges[30]. According to this

27 This paper assumes a comprehensive conception of the role of the judge. Although we recognize that there is no global and unique conception of what a judge should be, it is not the main purpose of this paper to discuss it. So, for the sake of argument, the particular social and proactive role of the judge discussed under this heading is a point I take for granted.

28 Please note that, although this section is divided into sub-sections for a better understanding of the arguments, all these ideas are closely related to each other.

29 *"Too often portrayed as mere private dispute resolvers, the public good performed by courts as vital institutions of governance is commonly sidelined. There is, in such an environment, an increasingly pressing need to explain what it is that courts actually do; to articulate precisely the function of a judge".* (McIntyre, 2020, p. 1). The European Networks of Councils for the Judiciary (ENCJ WORKING GROUP) in its Judicial Ethics Report of 2009-2010 recognized that **"***in our European societies, the judge's role has evolved: it is no longer confined to being "the mouthpiece of the law"; the judge is also, to a certain extent, a creator of law, which requires responsibilities and ethical rules consistent with this evolution*".

30 "*I doubt whether dispute resolution is an adequate description of the social function of courts. To my mind courts exist to give*

influential author "*adjudication is the social process by which judges give meaning to our public values*" (Fiss, 1979, p. 2). That is why courts bring about significant changes, essentially reconstructing social reality[31]. The structural reform, of which the judge must be a promoter, focuses on the broader aspects of social life and the role of large organizations, like courts, in shaping those conditions. To support his point, Fiss considers that paradigmatic cases such as *Brown v. Board of Education*[32], did not really focused on settling a dispute between individuals, but rather to give meaning to certain public values[33].

44 Fiss's argument is meritorious; however, he errs in part in giving more weight to one function over the other. The social function of the judge is best expressed by McIntyre (2020, p. 1) when he recognizes that the essence of the judiciary is "*the unique way in which the two aspects of dispute resolution and social governance are woven together into a coherent single function*". The merit of this argument lies in acknowledging the dialectical relationship between both functions.

45 Judges cannot administer justice effectively unless they possess an understanding of the social and cultural factors that may significantly influence individuals' behavior in specific situations[34]. Promoting greater awareness of the judiciary about local communities will increase confidence in the justice system in general[35]. By actively engaging in the community, judges will gain valuable insights into how their decisions affect people's lives, leading to better-informed and more impactful judgments (Ifill, 2000; Gargallo, 2007; Kamil, 2009). This is relevant not only for AI, but also for human judges themselves. It is not desirable to assign judges to dispense justice in communities or environments with which they are unfamiliar. Even if it is possible to explain to such a person the characteristics of the place, it is difficult for that person to really understand the context. If replacing human judges with other humans in certain communities can be problematic because of unfamiliarity with the context, it would be even worse if it were an AI.

46 Therefore, judges are deeply influenced by social dynamics, which are complex and context dependent. The law, like all social phenomena, is loaded with values and principles present in society and which vary over time. A technology like AI may struggle to capture these complexities fully and accurately. AI lacks the capacity to replicate the inherently social dimension of delivering justice, and attempting to do so would involve compromising or distorting essential social relations and interactions. Since legal processes are deeply rooted in the social context, that is, human interactions and dynamics, no matter how advanced an AI is, it will never be able to capture the intrinsically social nature of law (Morison and Harkens, 2019)[36]. This socially active dimension of the judge contributes to making the law more dynamic, thus avoiding situations of legal stagnation[37].

2. Lack of moral agency and rational autonomy

47 This section departs from the premise that moral agency is an innate quality of the human being and essential to exercise the judicial function[38], while

meaning to our public values, not to resolve disputes" (Fiss, 1979, p. 29)

31 Also (Ciacchi, 2014, p. 125): "*I understand judicial governance as societal policy-making through adjudication at both the national and the supranational level*".

32 347 U.S. 483 (1954). In a unanimous decision, the Supreme Court ruled that racial segregation in public schools was unconstitutional and violated the Equal Protection Clause (Fourteenth Amendment). The Court overturned the "separate but equal" doctrine established in *Plessy v. Ferguson* (163 U.S. 537 (1896)), declaring that racial segregation in public education was inherently unequal and therefore unconstitutional.

33 Specifically racial equality and non-discrimination.

34 "*Judges do not simply apply general legal provisions to specific cases in a vacuum, disconnected from political and social life; instead, they make decisions that have normative and distributional consequences—in fact, they are empowered to do exactly that. The most pressing of these implications is that judicial decision-making should not be viewed in isolation, as if it were divorced from ongoing social or political trends. Judges make choices about how to think about and decide cases, choices that may be influenced by political, institutional, and social context.*" (Taylor, 2023, pp. 288–289)

35 This contributes to the legitimacy of the judicial system itself and of the law in general, an issue that will be addressed below.

36 Schmid (2008) is another author who considers that adjudication is always shaped by the broader social context, including political, economic, and social factors that influence the minds of judges and their decisions. Schmid sees this influence as necessary and not undesirable because it allows the law to adapt to the changing social environment effectively.

37 Potential legal stagnation is discussed further in section E.V.

38 "*... the judicial decision is a legal one, and in all cases that legal*

AI lacks this element. Moral agency involves the ability to reflect on one's actions and understand their moral implications. For judges, this means considering how their decisions impact the parties involved and society as a whole. It also requires understanding and respecting social and cultural norms, treating others with dignity and respect, and acknowledging and upholding the rights and autonomy of individuals.

48 In short, judges cannot simply apply the law without first interpreting it, and this interpretation is subject to the ideological and moral preconceptions of the interpreter. Therefore, to exercise the function of judging it is considered necessary to have certain personal attributes, ideology, and morals (such as fairness, justice, and compassion)[39]. According to the ENCJ working group[40], the judge "*in his assessment of facts and decisions he finds a measure between empathy, compassion, kindness, discipline and severity*[41]*, so that his application of law is perceived as legitimate and fair... This quality implies not only real open-mindedness and receptiveness but also the ability to call into question oneself*". The AI is simply incapable of replicating this, just because it does not even have a "sense of self".

49 This is not to say that the judge is a person who is driven by his passions and feelings. It should be kept in mind that the human judge also has rational autonomy. For Tasioulas (2023), "rational autonomy" refers to the ability of human beings to detach themselves from their desires, social pressures, and established behaviors to objectively assess the pros and cons of a situation. It involves making a well-considered judgment on the right course of action based on this assessment and then choosing to follow that judgment in a specific case. The possession of rational autonomy is seen as a crucial aspect of human dignity.

50 Related to this, Fortes (2020, p. 462) also raises a crucial point: "*one important lesson for our speculative reflection on the development of judicial robots is that contemporary artificial intelligence may not produce its decisions with prudence, which seems an essential quality for adjudication*". What he and Gargallo (2007, p. 121)[42] call prudence, is nothing more than the exercise of moral agency and rational autonomy in a given situation, which allows the human being to weigh the different alternatives available to him and analyze the potential implications of his decision. By contrast, AI is not able to consider the potential ramifications or long-term implications of a particular verdict on the life of individuals.

51 Gargallo (2007, p. 130) also points out that judging is not simply applying a legal rule to facts through mechanical deductive reasoning. In the process of judging, a reasonable logic is used that is based on knowledge of the law, the legal institutions involved and the general values and principles of law. The judge takes into account the consequences of his decision when determining the facts and qualifying them legally. In essence, the judgment involves a complex process of consideration and reasoning beyond a simple logical syllogism[43].

52 Moral agency is particularly relevant to the more challenging areas of the legal universe. How does an AI understand[44] such subjective legal concepts/principles like good faith, degrading treatment, human dignity, autonomy, hate crime, best interests of the child, etc.? How could it reach a nuanced opinion on issues such as abortion, clash of fundamental rights, death penalty or legal paradoxes?[45] This makes AI hardly applicable to complex areas such as criminal, constitutional, or family law.

53 Everything depends on our position on the judiciary. If we desire laboratory judges who resolve disputes

decision is inextricably tied to a moral one, either explicitly or implicitly." (Mancini and Rosenfeld, 2010, p. 16)

39 "*Judicial responsiveness requires judges to act from the perspective of conscious legal rationality and also with intuition, empathy and compassion.*" (Sourdin and Cornes, 2018, p. 87). See also (Nava, 2008).

40 See 29.

41 Gargallo (2007, p. 117) refers to these qualities as "judicial virtues".

42 In fact, Gargallo (2007, p. 129) identifies prudence as the most important asset of the judge: "*There are many virtues that we can appreciate in a good judge (good judgment, perspicacity, prudence, farsightedness, a sense of justice, humanity, compassion, courage, temperance...), although the one that best serves the proper function of the judge and informs all the others is prudence. We could say that it is the most characteristic virtue of the 'good judge'*".

43 "*One may consider that the decision-making procedure is so complex, variable, uncertain, fuzzy and value-laden, that it could never be reduced to logical models*". (Taruffo, 1998, p. 314)

44 AI processes large amounts of data, but processing is not the same as understanding (See 4 [Turing vs. Searle]). As a society we need judges to understand and be aware of the significance of their work.

45 Another important concept, but one that is not particularly easy to apply, is that of the purposes of the sanction, a topic that has been discussed in law for hundreds of years. When the AI imposes a sanction, would it really be aware of the purpose of the sanction it is imposing? Could it reason why it is imposing such a sanction and not another?

in a "logical" and amoral basis, AI might be a good option. Now, if we want judges who are socially aware, empathic, proactive, and dynamic, AI will probably never meet that expectation. It is even difficult to develop the AI into a being with moral convictions, ethics and an inventory of the values mentioned here, since we do not even know exactly how this phenomenon works in the mind of the human being himself. Sourdin and Cornes (2018, p. 112) explain that in the pursuit of this, a paradox interferes: "*... such personal inputs, emanating from human judges', and society's unconscious, are by definition not consciously knowable and therefore not translatable into code*". Therefore, *decoding* the human mind and its moral agency would be a precondition for subsequently providing moral agency to other entities.

3. III. A role model

54 When the human judge is replaced by an AI, more than a mere administrator of justice or public official is lost. This section attempts to highlight the social role of the judge as a pillar of the community and as a role model[46].

55 The role model epitomized by judges is legally relevant because, pragmatically, moral sanctions operate more effectively when they come from someone who is valued as legitimate or deserving of respect (Seña, 2001). Throughout history, judges have been attributed a special ethical status and have been required to behave morally in their private lives, which seems to be relevant for the proper performance of their jurisdictional function. Seña (2001, p. 380) quotes the following words of Piero Calamandrei: "*so high in our estimation is the mission of the judge and so necessary is confidence in him, that human weaknesses which are unnoticed or forgiven in any other order of public officials, seem inconceivable in a judge.... Judges are like those who belong to a religious order. Each of them has to be an example of virtue, if they do not want believers to lose faith*"[47]. What for religious leaders is the loss of faith, judges would be the loss of legitimacy. It is argued that the judge must play this role model in order to generate confidence in those affected by his decisions and thus contribute to the stability of the legal system. The judge must also consider that his decisions have an impact not only on the subject concerned, but also on the rest of citizens.

56 Aspen (1993) and Joy (2000) have studied this topic and argue quite logically that judges are seen as role models, primarily because they are expected to set an example through their conduct. They cannot expect others to adhere to standards of behavior they do not follow themselves. When judges demonstrate proper behavior and uphold their role model status, they inspire the public to follow suit, fostering high expectations of behavior and building trust and confidence in the judiciary (Martineau, 1981). This also relates to the aforementioned connection between the judge and the community[48]. Roche (2020, p. 2244), drawing on (Ifill, 2000) states: "*Judges should model all the qualities required of them by their codes of conduct to nurture those same qualities in the community they serve. However, judges who do not share the same values with their communities cannot be good role models for their communities*".

57 This also relates to what was mentioned in the previous section on moral agency and rational autonomy. According to the ENCJ WORKING GROUP a judge should understands that their professional conduct, private life, and behavior in society significantly impact the perception of justice and public confidence. Building trust in the justice system goes beyond being an independent, impartial, honest, competent, and diligent judge. It also involves displaying personal qualities such as wisdom, loyalty, humanity, courage, seriousness, and prudence, as well as the ability to work diligently, listen effectively, and communicate clearly. The exercise of these moral attributes is what makes it possible for the judge to become a role model for his or her community.

58 Sourdin and Cornes (2018, p. 97) also remind us that "*apart from their critical adjudicative role, judges also play an educative role, informing litigants and lawyers about approaches to be taken and contributing to civic education at a broader level*". The importance of this facet of the judge is often overlooked. Roche (2020, p. 2220), however, thinks judges are fundamentally teachers. Judges act as teachers when they exercise judicial power and uphold high standards of behavior. Their teaching role is vital for connecting judges to society, improving judicial efficiency, fostering a positive perception of judges, and ensuring access to justice.

46 However, it is important to clarify that the purpose here is not to glorify the figure of the human judge or to endow him or her with a halo of infallibility. "*The challenge however, will be for judges to use their role model status realistically without expectation of perfection, and for the public to have realistic expectations of judges, which understands that perfection is unattainable*." (Roche, 2020, p. 2247)

47 Public confidence in the judiciary also seems to depend on the conduct of judges, which results in a higher demand on their behavior compared to an ordinary citizen. (Riley, 1992; Seña, 2001)

48 Section E.I.

4. IV. Legitimacy

59 Tasioulas (2023, p. 1) quotes in one of his papers a famous passage from The Laws of Plato[49] that is highly illustrative of some of the issues discussed here[50]. In this dialogue, Plato intends to illustrate the qualitative difference between a "free doctor", one who is trained and can explain the treatment to his patient, and a "slave doctor", who cannot explain what he is doing and instead works by trial and error. In this case, Cleinias opts for the free doctor precisely because he is better able to provide his diagnosis through reasoning, dialogue and understanding. Judicial explicability[51] works in a similar way with the citizenry. There is a close relationship between the rationality of the decision, explicability, and legitimacy. In his book, McIntyre (2019, p. 152) articulates this point sharply:

> "That judicial decision must be rational, in the sense that is justifiable, as the judge must engage in the argumentative enterprise of persuading others that the chosen alternative is preferable. Persuasive decisions promote effective dispute-resolution, by giving disputants good reasons to accept even outcomes they disagree with. Similarly, justification affects social governance, as the normative impact of a resolution will vary with the persuasiveness of the reasoning."

60 Judges must be aware of the impact their decisions have on the judiciary's ability to fulfill its social role. The effectiveness of their judgments relies on the overall social legitimacy of the courts. Thus, judges hold a responsibility in upholding the necessary public confidence in the judicial system (McIntyre, 2019). Maintaining the public's trust and confidence in the justice system is essential because when people believe in its integrity, they are more likely to accept and comply with the decisions made (Crootof, 2019). Legitimacy can be achieved, inter alia, through the judge's adherence to certain moral values, transparency, dialogue and explainability, all of which we have already seen that AI lacks.

61 When analyzing the feasibility of an AI judge, Volokh (2018, p. 1137) states that we should "*Consider the Output, Not the Method*". Statements such as these should be taken with caution. It could be problematic to assume such a premise/principle. In the judicial process, what is important is not only the outcome, but also the process itself[52]. Going back to Plato's dialogue, both the "slave doctor" and the "free doctor" can reach the same outcome. The issue is which method is more desirable? Cleinias understands that the free doctor is better, because the patient does not feel alienated in the process. The patient here is not only a passive subject, but also an active participant in this bidirectional dynamic. Ultimately, there is value in the dialogue between two rational moral agents. On the other hand, the slave doctor represents an algorithm, dispensing the treatment, but failing to provide the patient with the rationale behind the outcome. The patient is more likely to follow the instruction in this case by means of imposition, not assimilation.

62 Tasioulas (2023, pp. 10–12) argues that for AI to fully respect the rational autonomy of human beings, it must possess rational autonomy itself. Without this capacity, AI lacks the ability to judge humans without infringing on their dignity and due process guarantees. The use of AI tools as substitutes for human judges undermines the rule of law's goal of securing respect for rational autonomy, explainability, and accountability. Meaning, people might not value the persuasiveness of opinions rendered by artificial intelligence because they believe that human decision-making is the only legitimate form of judicial decision-making. They may hold this view due to a belief in human dignity, which requires their claims to be heard by fellow

49 Plato, *The Laws*, ed M Schofield (Cambridge, Cambridge University Press, 2016) 163-64 (720b-e)

50 "*ATHENIAN – And you realise, don't you, that the people who fall sick in our cities may be slaves or free-born? And that it is the slave-doctors who for the most part treat the slaves, either dashing round the city or sitting in their surgeries? None of these doctors gives any explanation of the particular disease of any particular slave – or listens to one; all they do is prescribe the treatment as they see fit, on the basis of trial and error ...*

The free-born doctor spends most of his time treating and keeping an eye on the diseases of the free-born. He investigates the origin of the disease, in the light of his study of the natural order, taking the patient himself and his friends into partnership. This allows him both to learn from those who are sick, and at the same time to teach the invalid himself, to the best of his ability; and he prescribes no treatment without first getting the patient's consent. Only then, and all the time using his powers of persuasion to keep the patient cooperative, does he attempt to complete the task of bringing him back to health. Is a doctor who heals in this way a better doctor? Or the other way? Likewise a trainer who trains in this way? He has one single ability. Should he get it to complete its exercise by this dual method, or in the simple way – the less good of the two, and the one which makes the patient more hostile? CLEINIAS – The dual approach, my friend, is by far the better."

51 AI explainability or explicability is a process that allows individuals affected by a machine learning decision, with legal or significant consequences, to request an explanation for that decision. Additionally, it grants the parties the right to access, to the extent possible and reasonable, the data used and information generated by the AI model.

52 The legal process is a crucial element in the administration of justice. It is not for nothing that the procedural law field exists.

humans. That is, the legitimacy of the justice system could be compromised due to potential public reluctance in embracing judgments delivered by no human entities[53].

63 In a nutshell, transparency, reasonability and explainability of judicial decisions are elements that guarantee due process and legitimacy. According to the ENCJ WORKING GROUP, a judge should "*give reasons for his decision so that everyone involved can understand the logic on which the judge based his decision*"[54]. For instance, consider the problem raised by Loomis appeal mentioned in section D.I. Because the COMPAS operated as a "Black Box" system, one can know the result, but not exactly how it was reached, that is, the system lacks explainability[55]. How can the right to appeal even be guaranteed if the affected party is incapable of understanding the reasoning by which he/she was affected[56]? Therefore, Gargallo (2007, p. 132) is right when he states that "*the provision of a rationale is a guarantee against prejudice and arbitrariness, and facilitates jurisdictional control through appeals, which contributes to the strengthening of legal certainty*".

64 There is another issue. Because an algorithm has no moral agency or rational autonomy, it cannot be held responsible for its decisions. Rational moral agents make decisions and are held accountable for them. So, AI also raises a problem concerning liability and accountability[57].

5. Risk of legal stagnation

65 Judges have the difficult task of balancing legal stability and responsiveness to social change. On one hand, reforming the law to align with social values can make it more just and adaptable. Maintaining rigid laws can lead to inconsistency and lack of coherence. The constant interaction with society enables judges to tailor their decisions to real-life situations and achieve a normative coherence. On the other hand, this flexibility comes at the cost of certainty and predictability, which can challenge the overall legitimacy and acceptability of the legal system and judicial governance. Striking a careful balance between stability/ predictability[58] and the need for just flexibility becomes crucial for effective judicial governance.

66 In this sense, the drawback of AI is its reliance on

53 Following this reasoning, one could even hypothesize whether, in the not-too-distant future, being judged by a human judge would be recognized as a fundamental human right. See (Górski, 2023). This is an interesting question that is left open for further discussion in further papers.

54 See 29.

55 According to O'Hara (2020) excellent article on the nature and purpose of explanations, the main objective of an explanation is to help the audience understand a phenomenon. Simply presenting information without additional explanatory context doesn't fully meet the needs of the subject. The subject needs to question the decision's logic. She also stresses that the purpose of explanations should be to guide future conduct, helping subjects to understand how their past behavior, as represented in the data, led them to make a particular decision and how they can change their behavior accordingly. Thus, she concludes that "*in order to contest a decision, the data subject must understand it. To facilitate this... we should take 'explanation' in its performative sense, not in the sense of a product or text... It does not seem plausible that the output of XAI* (explainable IA) *could function as an explanation*" (O'Hara, 2020, p. 5).

56 See GDPR recital 71 (on the right of the affected party to be given an explanation of the decision taken in order to be able to challenge it).

57 This issue has become increasingly debated since the rise of generative AI. Let's imagine that the AI judge makes a mistake, who would be liable? If we consider the literature on liability for unlawful acts resulting from AI (Giuffrida, 2019; Wendehorst, 2020), the discussions center on the following responsible parties: the one who programmed the IA, the one who selected and trained the dataset, or the one who introduced the prompts. Specialists are skeptical about the proposal that AI itself should be considered responsible (See, e.g. the Open Letter to the European Commission Artificial Intelligence and Robotics (2018)). There are several ethical and legal reasons for adopting this position, starting from the potential consequences of recognizing AI as a legal entity. In addition, one cannot ignore the fact that, as explained, AI lacks the rational autonomy to be held responsible ("*Conventional wisdom holds that punishing AI is incongruous with basic criminal law principles such as the capacity for culpability and the requirement of a guilty mind*" (Abbott and Sarch, 2019, p. 323)). People usually tend to look for a human being to be held accountable for AI actions (See Expert Group on Liability and New Technologies – New Technologies Formation (EG-NTF), Report on Liability for Artificial Intelligence and other emerging digital technologies (2019), Key Finding no 8). The fact that one tends to look for a wrongdoer other than the AI (being the developer or user) evidences people's skepticism of the fact of recognizing AI agency. So, in any case, before introducing a robot judge, should be considered the idea of the AI having legal personhood to be legally accountable for its actions, with all that this implies.

58 "*The judge is required to embrace the virtuous tension between the pursuit of clarity, predictability and order on one hand, and responsive and just flexibility and change on the other. In doing so, the judge injects a necessary vitality and responsive dynamic to the law.*" (McIntyre, 2020, p. 37)

past data. As a result, they often end up reproducing patterns and perpetuating the biases, choices, and arguments with which they were trained. Judicial robots would likely have difficulties making decisions that go against existing precedent. This design would make it difficult for them to adapt to dynamic social environments. Thus, while they perform well in terms of consistency and predictability, they are not so satisfactory in terms of flexibility and adaptability required for judicial governance (Crootof, 2019; McIntyre, 2020). It is unlikely that algorithms would have been capable of reaching groundbreaking and counter-hegemonic decisions such as *Brown v. Board of Education*. Most likely, this system will end up indefinitely reproducing the *status quo* and establishing a model of "legal recycling".

67 An effective administration of justice requires judges who have the ability to adapt and recalibrate the legal machinery. AI is unfortunately limited to working on the same mistakes that were once made and contains few sophisticated social tools to overcome those mistakes and keep pace with society. Therefore, the implementation of the AI judge would not contribute to the efficacy of the norm itself. Every judicial application of legal rules directly impacts upon that particular law, strengthening, maintaining, or reforming it. The process of actively altering the law through judicial decisions ensures that it remains well adapted to its social purposes and reflects concrete social values. When a judicial decision is publicly declared, it clarifies the "contour" of the norm, reducing uncertainty and facilitating settlements. Through the application of the law in resolving disputes, judges reaffirm the public value of legal rules, making them active normative constraints within society. By adapting legal norms to the current social context, judicial decisions revitalize the law, making it more dynamic, responsive, and effective in guiding social behavior (Dickson, 2000; McIntyre, 2019, p. 59).

6. Public functions outsourced to private entities

68 Lately, private companies have been increasingly exercising control over communications, media and public discourse. As Balkin (2018) rightly points out, freedom of expression is no longer a dual relationship (State-citizen), but a triangular one (State-citizen-platform). Over time, we all have witnessed how functions or powers, that were traditionally public, are being privatized. The change to AI judges would be another symptom of this phenomenon.

69 Justice administration has historically been one of the classic public powers, within the classical theory of the tripartition of powers. The potential dangers of involving private sector technical developers in state functions are (i) market dominance, (ii) undue influence over public policy, (iii) lack of accountability, (iv) loss of control, and (v) erosion of public trust[59] (Krent, 2010; Morison and Harkens, 2019, p. 631; Calo and Citron, 2020; Grote and Di Nucci, 2020). If private companies are developing these AIs, how can we prevent them from influencing the outcome? How can we know for sure that there is no undue influence, if we cannot access the code? This is an extremely important issue and one that has deep ethical implications. Allowing them to design datasets and algorithms gives them influence over decisions that can impact fundamental human rights, including the right to freedom (Deeks, 2019). Proper regulations and ethical guidelines are essential to mitigate these risks and ensure a balanced approach to private sector involvement[60].

B. CONCLUSION

70 The judicial system faces various challenges, including excessive costs for both individuals and society, prolonged delays in case resolution, and inconsistencies in judgments. Additionally, the limited number of judges often leads to difficulties in handling the increasing caseloads. These issues have resulted in a decline in public confidence in the system. This makes the idea of deploying artificial intelligence increasingly appealing. However, McIntyre (2019) emphasizes the need for reflection on the essential functions of courts, their significance, and whether they still hold value before completely abandoning them in favor of new approaches. That was the aim of this paper.

71 The contribution made by the digitalization of judicial processes to speed up decisions and save costs is undeniable. Then, should judges disappear? Not in our opinion, at least not at the moment. We will never know how far technological development can go. In any case, let us remember that the judge is not only the person in charge of imparting justice, but he/she is also a role model and reference to society. Moral agency is an attribute of the judicial agency that contributes to the social governance function of judges. Many judges also play a role in an educational sense by contributing to civic education on a broader level. Discretionary decisions must take into account the values of the community, society, the personal conditions of the parties and any other

59 In general, the principle of independence (specifically its judicial discretion dimension) would be compromised, as judicial decisions could be subject to the undue influence of private interests.

60 In Europe, the IA Act could mitigate these concerns.

circumstances that may be relevant (Sourdin, 2018). If jurists fail to advocate for this kind of judges, their decline is unavoidable. This could lead to the emergence of a new system, which may fulfill some aspects of the judicial role but leave others unaddressed (McIntyre, 2019, p. 297).

72 This paper does not encourage the elimination of AI from courts. The author concludes that, although judges and other legal operators should not be displaced by these computer programs, the use of the latter could indeed optimize the exercise of judicial work in the future. AI programs could be cautiously used to assist human judges, rather than replace them.

JIPITEC

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

www.jipitec.eu