MASARYK UNIVERSITY JOURNAL OF LAW AND TECHNOLOGY

VOLUME 18 | NUMBER 1 | SUMMER 2024 | ISSN 1802-5943

PEER REVIEWED

CONTENTS:

www.mujlt.law.muni.cz

Masaryk University Journal of Law and Technology
issued by Institute of Law and Technology
Faculty of Law, Masaryk University
www.mujlt.law.muni.cz

Official Partner (Czech Republic)
ROWAN LEGAL, advokátní kancelář s.r.o. (https://rowan.legal)
Na Pankráci 127, 14000 Praha 4

Subscriptions, Enquiries, Permissions
Institute of Law and Technology, Faculty of Law, MU (cyber.law.muni.cz)

listed in HeinOnline (www.heinonline.org)
listed in Scopus (www.scopus.com)
reg. no. MK ČR E 17653

MASARYK UNIVERSITY JOURNAL OF
LAW AND TECHNOLOGY

VOLUME **18** | NUMBER **1** | SUMMER **2024**

LIST OF ARTICLES

LIST OF COMMENTS

DOI 10.5817/MUJLT2024-1-1

ALTERNATIVE LEGAL BASES FOR PROCESSING HEALTH DATA FOR SCIENTIFIC RESEARCH PURPOSES

by

ROXANNE MEILAK BORG * MIREILLE MARTINE CARUANA †

The processing of health data for scientific research purposes requires a legal basis under Article 6 and a justification under Article 9 (2) GDPR by way of an exception to the general prohibition in Art. 9(1) of the processing of special category data. Consent tends to be highly advocated for in this regard, in both literature and practice. However, the GDPR permits an alternative option: processing for scientific research purposes based on Union or Member State law which provides for suitable and specific safeguarding measures. This paper undertakes an in-depth examination of the 'research exception' in Art. 9 (2) (j) GDPR permitting the processing of health data for scientific research purposes, thoroughly considering its elements and its implications. It refers to examples of Member State implementing legislation and the proposed European Health Data Space Regulation for illustration purposes and argues that if implemented faithfully, Art. 9 (2) (j) strikes a better balance between the interests of the various stakeholders than consent, which is overall burdensome and may hinder research. Finally, in light of the uneven implementation of the GDPR's research exception by the Member States which creates considerable legal uncertainties and results in barriers to the free flow of research data across the EU, this paper calls for a harmonised implementing Union law in this regard.

* Roxanne Meilak Borg LL.B. (Melit.), LL.D. (Melit.), M.A. (Melit.), is a Research Assistant at the Department of Media, Communications and Technology Law within the Faculty of Laws and former Data Protection Officer of the University of Malta. For correspondence: roxanne.meilak@um.edu.mt.

† Mireille M Caruana, B.A., LL.D. (Melit.), LL.M. (Lond.), Ph.D. (Bristol), is Senior Lecturer and Head of the Department of Media, Communications and Technology Law within the Faculty of Laws at the University of Malta. For correspondence: mireille.caruana@um.edu.mt

KEY WORDS

Health Data, Scientific Research Purposes, General Data Protection Regulation (GDPR), European Health Data Space (EHDS) Regulation.

1. INTRODUCTION

The impact of scientific research on health data is far-reaching: it may result in better individual diagnosis and treatment and may lead to better management of future diseases and improved healthcare services. Within the EU, research on health data constitutes a processing operation under the General Data Protection Regulation ("GDPR")[1] and must conform with such Regulation as well as with any additional national data protection laws Member States may have in place. The GDPR appears to take the rights and interests of the relevant stakeholders – including the research community – into account. It incorporates the term "processing for scientific research purposes" in Recitals and substantive provisions[2] and affirms that "scientific research" should be understood broadly to include "for example technological development and demonstration, fundamental research, applied research and privately funded research."[3]

As a data processing operation, scientific research on health data requires a legal basis under Art. 6 GDPR and, since it involves data that are sensitive in nature and fall under a special category listed in Art. 9 (1) - which also prohibits the processing of such data - it must be justified under an Art. 9 (2) provision. Art. 6 does not provide a specific legal basis for data processing for scientific research, but Art. 9 (2) (j) includes the so-called "research exception" - an exception to the general prohibition of the processing of special category data where the processing is for scientific research purposes.

Currently, however, there is no widespread application of Art. 9 (2) (j). It is consent - included as both a legal basis in Art. 6[4] and a possible exception in Art. 9 (2)[5] - that tends to be not only advocated for in academic literature, but also, the preferred option in practice.[6] This could

---

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General DataProtection Regulation). Official Journal oftheEuropean Union (2016/L-119/1) 4 May. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

2 Ibid., Recitals 33,156-57,159; Arts. 5 (1) (b) and (e), 9 (2) (j), 89.

3 Ibid., Recital 156.

4 Ibid., Art. 6 (1) (a).

5 Ibid., Art. 9 (2) (a).

6 See Dove, E. S. and Chen, J. (2020) Should consent for data processing be privileged in health research? A comparative analysis. *International Data Privacy Law*, 10 (2), p. 119; Hallinan, D. (2020) Broad consent under the GDPR: an optimistic perspective on a bright future. *Life*

be because it appears to afford data subjects greater control over their data,[7] or because in practice research participants are generally still required to give their consent for ethical purposes.[8] Be it as it may, consent as a legal basis is overall burdensome, does not necessarily result in the most comprehensive protection for research participants, and restricts researchers' flexibility, thereby hindering research.

This paper undertakes an in-depth examination of the Art. 9 (2) research exception in order to assess its legal and practical suitability as an alternative to consent. Thus, it aims to answer the following research question: Should we move away from consent in the context of data-driven research, and focus instead on effectively operationalising the Art. 9 (2) research exemption?

The paper begins by contemplating various reasons why consent is unsuitable as a legal basis and/or Art. 9 (2) exception for the processing of health data for scientific research purposes. It then considers the elements of Art. 9 (2) (j), focusing on its interplay with Article 89 (1) GDPR and the requirement of adopting "suitable and specific" safeguarding measures. It draws on the experience of selected EU MS to exemplify State practice in this respect, referring to provisions of Austrian, Belgian, Estonian, Finnish, German, Irish and Polish laws in light of such countries' geographical distribution and different legislative approaches, as well of the laws of the authors' home country of Malta. As Chapter 4 shows, the relevant national laws are disparate, and the implementation of safeguards within national legal frameworks fragmented. The views and practices of national DPAs are not considered in this review.

Next, the paper engages in a brief analysis of two specific pieces of legislation in light of the Art. 9 (2) (j) requirements. It identifies the Irish

Sciences, Society and Policy, 16 (1), p. 6; Manis, M. (2017) The processing of personal data in the context of scientific research. The new regime under the EU-GDPR. *BioLaw Journal - Rivista di BioDiritto*, 3, p. 337; Quinn, P. (2021) Research under the GDPR – a level playing field for public and private sector research? *Life Sciences, Society and Policy*, 17 (4), pp. 6, 8, 29.

7 See Comandè, G. and Schneider, G. (2022) Differential Data Protection Regimes in Data-Driven Research: Why the GDPR is More Research-Friendly Than You Think. *German Law Journal*, 23, pp. 573-574.

8 In terms, for instance, of the: World Medical Association, *Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Subjects*, June 1964. Available from: `https://www.wma.net/policies-post/wma-declaration-of-helsinki-ethical-principles-for-medical-research-involving-human-subjects/` [Accessed 29 December 2023]; and the World Medical Association, *Declaration of Taipei on Ethical Considerations Regarding Health Databases and Biobanks*, October 2022. Available from `https://www.wma.net/policies-post/wma-declaration-of-taipei-on-ethical-considerations-regarding-health-databases-and-biobanks/` [Accessed 29 December 2023].

Health Research Regulation ("HRR")[9] as a solid example of a comprehensive national law setting out such requirements (despite its shortcoming, in the authors' view, of reintroducing consent as a mandatory requirement), and considers the proposed European Health Data Space ("EHDS") Regulation[10] in view of its status as a topical and upcoming EU-wide law.

This paper does not purport to discuss appropriate alternative legal bases to consent under Art. 6 GDPR for the concerned processing; nonetheless, a brief discussion in this respect is warranted since it would be senseless to opt for an alternative exception under Art. 9 (2) without concurrently opting for an alternative legal basis under Art. 6. Scientific research is often carried out by public or publicly-funded entities; although Art. 6 does not include a specific legal basis for "scientific research purposes," it does provide one for public authorities/organisations. Thus, this paper briefly considers the relevance and interplay of such provision (Art. 6 (1) (e)) with and for Art. 9 (2) (j), as well as for research that is carried out by private entities in the public interest, at the end of Chapter 6.

The analysis shows that the GDPR offers the normative flexibility to accommodate solutions to any potential hindrance to research posed by data protection legislation, even if disparate national laws currently fall short of fully implementing the research exception. The paper argues that with proper implementation, the GDPR's research exception could strike a better balance between the various interests involved while also enabling the free flow of research data across the EU, resulting in the establishment of a true European research area. It thus calls for a shift towards a widespread application of Art. 9 (2) (j), in particular through a harmonised EU law implementing this provision.

2. UNSUITABILITY OF CONSENT AS A LEGAL BASIS

Consent is one of the most well-known, and advocated for,[11] possible legal bases under Art. 6 and exceptions under Art. 9 for data processing for scientific research purposes,[12] despite repeated assertions by EU data protection authorities that basing such data processing on consent may not

[9] Promulgated under the Irish Data Protection Act 2018 (No. 7 of 2018). Available from https://www.irishstatutebook.ie/eli/2018/si/314/made/en/pdf [Accessed 29 December 2023].

[10] Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, (COM/2022/197 final) 3 May. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex\%3A52022PC0197 [Accessed 29 December 2023].

[11] Dove, E. S. and Chen, J. (2020), *op. cit.*

[12] Quinn, P. (2021) Research under the GDPR – a level playing field for public and private sector research? *Life Sciences, Society and Policy*, 17 (4), pp. 6, 8.

be advisable.[13] In addition, there are many reasons why it is not a *suitable* option.

2.1. BURDENSOME TO OBTAIN; CAN BE WITHDRAWN

The GDPR sets a high threshold for consent as a legal basis for data processing. It is burdensome, in fact, to obtain consent in a manner that fulfils all the GDPR's requirements, since the GDPR requires consent to be "freely given", "specific", "informed" and an "unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."[14] Furthermore, data subjects must be given the opportunity to withdraw their consent at any point,[15] and once withdrawn, all processing based on such consent must be halted.

2.2. DIFFICULT TO IMPLEMENT IN CERTAIN CIRCUMSTANCES

It is harder to fulfil the GDPR's consent requirements where data to be used for research are obtained from third parties and not directly from research participants, as for instance in the case of a researcher wishing to carry out research on patient data originally collected and held by a medical institution for healthcare purposes. In such a scenario, it is impractical and perhaps even impossible for the researcher to seek each patient's consent in a manner that complies with the GDPR.

Consent is also problematic where data are collected and stored, usually in bio- or similar "data" banks, for generic and/or future research purposes. The requirement of specificity is not met here because the research purposes are often unknown at the time of data collection. Biobanking refers to the establishment of a research database consisting of genetic samples and extracted genetic data which is of increasing importance for innovative data-driven research, and, as has been argued, requires more flexible consent

[13] See European Data Protection Supervisor, A Preliminary Opinion on data protection and scientific research, Adopted on 6 January 2020. Available from: https://edps.europa.eu/data-protection/our-work/publications/opinions/preliminary-opinion-data-protection-and-scientific_en [Accessed 29 December 2023], p. 20; and EDPB, Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (art.70.1.b)), Adopted on 23 January 2019. Available from: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-32019-concerning-questions-and-answers_en [Accessed 29 December 2023].

[14] Ibid., Art. 4 (11).

[15] Ibid., Art. 7 (3).

options.[16] The notion of "open" or "broad" consent - whereby research participants give general consent to their data being used in future research - is particularly advocated for in this regard. The GDPR attempted to take such scenarios into consideration[17] and some MS have even chosen to reflect the concept of broad consent in their national laws: for instance, the notion is incorporated in Austria's Research Organisation Act[18] and Ireland's HRR.[19] Still, EU data protection authorities have asserted that such consent is not tantamount to, or even likely to fall under, the GDPR notion of consent,[20] so its applicability to the present context remains uncertain.

2.3. IMBALANCE BETWEEN THE PARTIES INVOLVED

Consent is not a valid legal basis where there is an imbalance between the controller and the data subjects, as such dynamics would likely negate the element of freely-given consent.[21] Public authorities are generally precluded from relying on consent as a legal basis[22] and employers are also discouraged from basing the processing of their employees' data on consent, since employees would likely be constrained or feel pressured to consent for fear of detrimental effects at work.[23] In the same way, individuals receiving medical treatment might feel "obliged" to consent to their health data being used for research purposes if they believed that declining could negatively affect their treatment or medical care. In fact, the Clinical Trials Regulation ("CTR")[24] already imposes an obligation on clinical trials investigators to

[16] Hallinan, D. and Friedewald, M. (2015) Open consent, biobanking and data protection law: can open consent be "informed" under the forthcoming data protection regulation? *Life Sciences, Society and Policy*, 11 (1), p. 3.

[17] By virtue of Recital 23. See also Hallinan, D. (2020) Broad consent under the GDPR: an optimistic perspective on a bright future. *Life Sciences, Society and Policy*, 16 (1).

[18] See Art. 2 (d) (3). Available from `https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen\&Gesetzesnummer=10009514` {Accessed 29 December 2023].

[19] HRR, *op. cit.* Reg. 3 (1) (e).

[20] See Art. 29 DP WP, Guidelines on consent under Regulation 2016/679, Revised and Adopted on 10 April 2018 (17/EN, WP 259 rev.01) Available from: `https://ec.europa.eu/newsroom/article29/items/623051/en` [Accessed 29 December 2023]; and European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/678, Adopted on 4 May 2020 (Version 1.1) Available from: `https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en` [Accessed 29 December 2023].

[21] Ibid., p. 6.

[22] Recital 43 GDPR.

[23] Art. 29 DP WP, *op. cit.*, p. 6.

[24] Regulation (EU) No 536 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC. *Official Journal of the European Union* (2014/L-158/1) 27 May. Available from: `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex\%3A32014R0536` [Accessed 29 December 2023].

carefully assess participants" circumstances to ensure that their consent is freely given and they are not inappropriately influenced to take part.[25] Thus it is likely that consent for the processing of health data for scientific research purposes would also not fulfil the "freely-given" criterion.

2.4. CONFLATION WITH ETHICAL CONSENT

Finally, it is important to recall that consent as a GDPR legal basis for data processing is not the same as "informed consent" for ethical purposes as envisaged by international instruments such as the WMA Helsinki Declaration.[26] "Ethical" consent is sought from individuals to ensure they are willing to participate in the concerned research, as a matter of respecting the individual's human dignity and self-determination.[27] In contrast, consent for the processing of data for scientific research purposes is a possible and non-exclusive legal basis provided for by the GDPR.

Ethical consent should not be confused or conflated with GDPR consent, and as a general rule, can and should not be done away with. On the other hand, there is no legal requirement to base data processing for scientific research on consent, particularly since the GDPR provides alternative options under both Arts. 6 and 9. Thus, where a controller opts for consent for data processing, consent as a legal basis for processing and that requested for ethical purposes overlap and may prove confusing for research participants.[28] While this does not in itself render GDPR consent unsuitable as a legal basis, it adds to the complexity of collecting such consent in a manner that complies with the GDPR, particularly in terms of ensuring that such consent is truly properly "informed."

3. RESEARCH EXCEPTION UNDER ARTICLE 9

3.1. ART. 9 (2) (J)

Art. 9 (1) GDPR prohibits the processing of data classified as "special category" unless an exception is provided in Art. 9 (2); Art. 9 (2) (j) sets out

[25] EDPB, Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (art.70.1.b)), Adopted on 23 January 2019. Available from: `https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-32019-concerning-questions-and-answers_en` [Accessed 29 December 2023].

[26] WMA, *op. cit.* For discussion on the main components of ethical consent see United Nations General Assembly, Right of everyone to the enjoyment of the highest attainable standard of physical and mental health, Adopted on 10 August 2009. Available from: `https://www.refworld.org/pdfid/4aa762e30.pdf`[Accessed 29 December 2023].

[27] WMA, *op. cit.*

[28] Dove, E. S. and Chen, J. (2020) Should consent for data processing be privileged in health research? A comparative analysis. *International Data Privacy Law*, 10 (2), p. 128.

a specific exception for the processing of special category data for research purposes, stating that the prohibition set forth in para. (1) shall not apply:

> *... where processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 (1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.*

Art. 9 (2) (j) is long-winded and convoluted[29] and sets out conditions that need to be fulfilled where it is to be relied on as a justification for the processing of special category data. It requires the concerned processing to be (i) necessary for scientific research purposes; (ii) in accordance with Art. 89 (1); and (iii) based on Union or MS law.

There is no guidance elsewhere in the GDPR or at EU level on how this provision should be interpreted or implemented. Linguistically, it is somewhat unclear whether it is the concerned processing or the requisite Union or Member State law that must be proportionate, respect the essence of the right to data protection and provide for suitable and specific safeguarding measures.[30] Kuner, Bygrave and Docksey[31] and Comandè and Schneider[32] take the former view. The authors of the present contribution favour the interpretation that the requisite Union or MS law should authorise the data processing for scientific research purposes and set out the scope of these purposes in a manner that is proportionate and respectful of data protection rights. Such a law would thus not only explicitly identify "suitable and specific" safeguarding measures for the concerned processing, but also provide a broader context for the concerned processing. Notably, there is currently no EU law implementing Art. 9 (2) (j).

3.2. ARTICLE 89(1)

Art. 89 (1), cross-referred to in Art. 9 (2) (j), requires processing for scientific research purposes to be:

---

[29] Ducato, R. (2020) Data protection, scientific research and the role of information. *Computer Law & Security Review*, 37, p. 5.

[30] The Italian version of Art. 9(2)(j) GDPR could be said to support the first interpretation; the English version could be read in both ways, and the French and Maltese versions appear to leave no doubt that the second interpretation is the correct one. The examination of other language versions is limited to the languages known to the authors. Ideally, all the other language versions would also be examined in order to reach a reliable conclusion and perhaps gain more insight into the legislator's intention.

[31] Kuner, C., Bygrave L. A., Docksey, C. and Drechsler, L. (*eds.) The EU General Data Protection Regulation (GDPR), A Commentary.* New York: Oxford University Press, p. 381.

[32] See (n 6) p. 580.

> *...subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. These safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.*

By way of context, Art. 89 (1) applies to the processing of *all* personal data (not just special category data) for scientific research purposes. It is a substantive provision within the GDPR, which as a Regulation is directly applicable in the Member States. As such, Art. 89 (1) does not require implementation into, nor indeed need to be reflected within, national laws. There is nonetheless some debate regarding whether the "appropriate safeguards" it calls for should be listed in national law, and whether the provision imposes an obligation on Member States in this regard or whether it is researchers as controllers who must implement safeguarding measures.[33] Furthermore, there is no guidance in the GDPR or otherwise at EU level about what the "appropriate safeguards" should be.[34]

3.3. THE INTERPLAY BETWEEN ART. 9 (2) (J) AND ART. 89 (1)

The reference to Art. 89 (1) and its corresponding obligations in Art. 9 (2) (j) appears to complicate matters, since both provisions set out a respective requirement pertaining to safeguarding measures. Furthermore, whilst it is clear that the "suitable and specific measures" required by Art. 9 (2) (j) must be provided for in Union or MS law, it remains unclear whether Art. 89 (1) "appropriate safeguards" should also be listed in law. This dissonance was even acknowledged during the GDPR's legislative process, in the form of an observation to such effect put forth by the Belgian delegation,[35] which appears to have not been taken into consideration since the relevant text remained unchanged.

---

[33] Milieu Consulting SRL, Study on the appropriate safeguards under article 89 (1) GDPR for the processing of personal data for scientific research, Adopted in August 2021 (EDPS/2019/02-08) Available from: `https://edpb.europa.eu/our-work-tools/our-documents/legal-study-external-provider/legal-study-appropriate-safeguards-under_en` [Accessed 29 December 2023] p. 9.

[34] See Kuner et al. *op. cit.*

[35] See Council of the European Union, Preparation of the Council position on the evaluation and review of the General Data Protection Regulation (GDPR) - Comments from Member States, 9 October 2019 (12756/1/19, REV 1) Available from: `https://data.consilium.europa.eu/doc/document/ST-12756-2019-REV-1/en/pdf` [Accessed 29 December 2023] p. 4.

Nonetheless, despite any possible confusion, and although they may appear at face value as an undue repetition, the obligations set forth in Arts. 9 (2) (j) and 89 (1) are distinct and likely apply cumulatively where Art. 9 (2) (j) is relied on for the processing of special category data for research purposes.[36]

It is not hard to understand the legislator's line of reasoning in respect of the obligation to have "suitable and specific" safeguarding measures for the processing referred to in Art. 9 (2) (j). Such an obligation laid out in law offers "added" protection to data subjects' rights and interests, particularly since the processing is not based on their consent. It also reflects the general practice of affording greater protection to special category data processed for research purposes.[37] On the other hand, one could question why there is mention of Art. 89 (1) in Art. 9 (2) (j) at all, if the former already separately establishes an overarching obligation in respect of all data processing for research purposes. A possible explanation could be that the reference to Art. 89 (1) is intended here as a reminder of the importance of adequately protecting the concerned data subjects. The cumulative application of Art. 89 (1), then, may be considered as a safety net of sorts, that provides a two-tier level of protection irrespective of what Member States choose to enact in any law setting out the "suitable and specific measures" required by Art. 9 (2) (j). However, this explanation still does not clarify what either set of measures should or could entail; nor the difference, if any, in practice, between them; nor indeed exactly what they are intended to protect, since they refer respectively to "the fundamental rights and the interests of the data subject'[38] and "the rights and freedoms of the data subject."[39]

4. IDENTIFYING SAFEGUARDING MEASURES

4.1. APPROPRIATE SAFEGUARDS

The terms "suitable and specific measures" set out in Art. 9 (2) (j) and "appropriate safeguards" set out in Art. 89 (1) are both legacy terms inherited from the GDPR's predecessor, the Data Protection Directive. Neither term is defined in the GDPR; nor as stated above, is the difference between them. Furthermore, to date no comprehensive guidelines with specific examples of such measures have been proffered,[40] even though the Art. 29 WP called for a definition for the term "safeguards" in as early as 2011, advocating for the provision of *examples* of such, and itself mentioning data security, specific

[36] See Ducato (2020), *op. cit.*, p. 5; Comandè, G. and Schneider, G. (2022), *op. cit.*, p. 580.
[37] Milieu Consulting SRL, *op. cit.*, p. 51.
[38] GDPR, Art. 9 (2) (j).
[39] GDPR, Art. 89 (1).
[40] EDPS (2020), *op. cit.*, p. 5.

notification and permit requirements in this regard.[41] Art. 89 (1) also proffers some, albeit extremely limited, insight into what "appropriate safeguards" could be, since it requires "technical and organisational measures" that "ensure respect for the principle of data minimisation" and identifies by way of a non-exhaustive example the specific measure of pseudonymisation. However, guidance at EU level is limited to the above two instances, and the task of identifying and implementing appropriate safeguarding measures is left in the hands of the Member States and/or the controllers and processors engaged in the processing.

Academic literature has attempted to shed light on the matter. Some authors suggest that to choose and implement appropriate safeguards, inspiration should be drawn from principles already enshrined in the GDPR, such as proportionality, data security and data minimisation.[42] Other authors recommend looking to international instruments, including ones governing ethics, for further direction. Staunton et al[43] considered texts such as the Council of Europe Convention for the protection of individuals with regards to the automatic processing of individual data[44] and the UNESCO Universal Declaration on Bioethics and Human Rights[45] to identify possible safeguards that could also fulfil the requirements of Art. 89 (1), ultimately recommending six possible standards: "consent that is appropriately governed; independent review and oversight; accountable processes; clear and transparent policies; adoption of security measures; and training and education of all those involved in the use and re-use of personal data in research."[46]

An analysis of existing "appropriate safeguards" in selected EEA States identified commonly implemented measures including pseudonymisation and anonymisation, risk assessments, data protection impact assessments ("DPIAs"), rules regarding access to and the physical handling of data, oversight by ethics committees and involvement of national data protection

[41] Art. 29 DP WP, Advice paper on special categories of data ("sensitive data"), Adopted on 20 April 2011 (Ref. Ares(2011)444105) Available from: https://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf [Accessed 29 December 2023] p. 11.

[42] See Kuner et al (2021), *op. cit.*, p. 381.

[43] Staunton et al. (2022) Appropriate Safeguards and Article 89 of the GDPR: Considerations for Biobank, Databank and Genetic Research. *Frontiers in Genetics*, 13, p. 9.

[44] Of 28 January 1981 (ETS 108) Available from: https://www.refworld.org/docid/3dde1005a.html [Accessed 29 December 2023].

[45] Of 19 October 2005. Available from: https://en.unesco.org/about-us/legal-affairs/universal-declaration-bioethics-and-human-rights [Accessed 29 December 2023].

[46] Staunton et al (2022), *op. cit.*, p. 9.

authorities.[47] Further insight into appropriate safeguarding measures is provided by the proposed EHDS Regulation, which refers to "establishing the safeguards for processing, in terms of lawful purposes, trusted governance for providing access to health data (through health data access bodies) and processing in a secure environment, as well as modalities for data processing, set out in the data permit."[48]

The status quo in Member States has however been described as a "patchwork of safeguards."[49] Although common measures may be applied across the EU, this is not done in a homogenous manner, particularly since there is currently no obligation of uniformity at EU level.

4.2. MEMBER STATE APPROACHES

Member States have thus tended to take unique and fragmented approaches towards adopting and implementing safeguards within their national legal frameworks. This section exemplifies how measures such as anonymisation and pseudonymisation and DPIAs, that are commonly acknowledged and resorted to as safeguards for data processing for research purposes, are implemented differently in different Member States.

4.2.1 Anonymisation and pseudonymisation

Anonymisation and pseudonymisation are both long-established safeguarding measures in the field of research, with pseudonymisation affirmed as "one of the safeguards most relevant to health sector research."[50] They are generally prevalent in data protection legislation, and have even been incorporated in the proposed EHDS Regulation.[51] Often, the use of anonymised data for research purposes is presented as the preferred default position, and the use of pseudonymised data permitted where it is not possible to achieve the purposes of the processing with anonymous data.

A case in point, the Belgian Data Protection Act[52] dictates as a general rule that anonymous data must be used for research purposes. The controller is nonetheless permitted to use pseudonymised data "if it is

[47] Milieu Consulting SRL, *op. cit.*

[48] EHDS, *op. cit.*, Recital 37.

[49] Milieu Consulting SRL, *op. cit.*, p. 5.

[50] DG Food and Health Safety (2021) *Assessment of the EU Member States' rules on health data in the light of GDPR*. Luxembourg: Publications Office of the European Union. Available from: https://health.ec.europa.eu/publications/assessment-eu-member-states-rules-health-data-light-gdpr_en [Accessed 29 December 2023] p. 61.

[51] EHDS, *op. cit.*, Art. 44.

[52] Adopted on 30 July 2018. Available from: https://www.dataprotectionauthority.be/publications/act-of-30-july-2018.pdf [Accessed 29 December 2023].

not possible to achieve the research by processing anonymous data" and "non-pseudonymised data" "if it is not possible to achieve the research or statistical purpose by processing pseudonymised data."[53] Belgian law also identifies specific circumstances under which data processed for research purposes must be anonymised or pseudonymised.[54] For instance, data to be used for research must be anonymised or pseudonymised once they have been collected from the data subjects;[55] when they shall be used for further processing[56] and when they shall be shared with one or more additional controllers for further processing.[57]

The Maltese DPA takes a similar, albeit less rigid, stance. Mirroring Art. 89 (1) GDPR, it imposes pseudonymisation as an overarching obligation in respect of data processing for research purposes, but requires that where such purposes "can be fulfilled by processing which does not permit, or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner."[58] The Irish DPA sets out an obligation for "suitable and specific measures [to be] taken to safeguard the fundamental rights and freedoms of data subjects' where data are to be processed for research purposes.[59] It does not require the use of pseudonymised data in research; it merely lists this as a possible "suitable and safeguarding measure."[60] It too provides that processing shall be fulfilled in a manner which does not permit, or no longer permits, identification of data subjects if it is still possible to achieve the purposes in this manner.[61]

This waterfall system has also been reflected in the proposed EHDS Regulation. Art. 44, governing the sharing of electronic health data, follows the principles of data minimisation and purpose limitation. As a first step it permits the relevant authority (the "health data access body"), to provide requested health data "in an anonymised format;"[62] where "the purpose of the data user's processing cannot be achieved with anonymised data" such data may be provided in "pseudonymised format."[63]

---

53 Ibid., Art. 197.
54 Ibid., Arts. 198-204.
55 Ibid., Art. 198.
56 Ibid., Art. 199.
57 Ibid., Art. 201.
58 Data Protection Act, Chapter 586, Laws of Malta. Available from: `https://legislation.mt/Legislation` [Accessed 29 December 2023] Art. 6 (4).
59 Data Protection Act 2018, Act Number 7 of 2018. Available from: `https://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html` [Accessed 29 December 2023] Art. 42.
60 Ibid., Art. 36 (1) (iv).
61 Ibid., Art. 42 (3).
62 EHDS (2023), Art. 44 (2).
63 Ibid., Art. 44 (3).

Some MS laws furthermore require pseudonymised data to be anonymised as soon as the research allows and/or once the purposes of the processing have been fulfilled.[64] Notably, however, not all MS laws require data to be used for research to be anonymised. For instance, Estonian law merely establishes an obligation to process data for scientific purposes "in a pseudonymised format"[65] and the Finnish Data Protection Act calls for pseudonymisation of data only where the processing of special category data is concerned.[66]

4.2.2 DPIAs

The GDPR explicitly mandates a DPIA in cases where the processing is likely to result in a high risk to the rights and freedoms of natural persons.[67] It identifies general circumstances where DPIAs are mandatory, such as in the case of "processing on a large scale of special categories of data"[68] but fails to provide concrete examples of such scenarios, leaving it to the relevant controllers to determine whether or not a DPIA is mandatory in respect of their particular processing operations. Further guidance in this regard has been proffered by the Art. 29 WP;[69] nonetheless, apart from establishing that the "storage for archiving purposes of pseudonymised personal data concerning vulnerable data subjects of research projects or clinical trials" requires a DPIA,[70] these guidelines do not specifically address scientific research or research on health data.

[64] See in this regard: Austrian Data Protection Act. Available from: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen\&Gesetzesnummer=10001597\&FassungVom=2018-05-25 [Accessed 29 December 2023] Section 7 (5); Irish HRR (2018), *op. cit.*, Reg. 3 (1) (c) (vii); German BDSG. Available from: https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html [Accessed 29 December 2023] Section 27 (3); Malta Subsidiary Legislation 528.10. Available from https://legislation.mt/Legislation [Accessed 29 December 2023] Reg. 4; Polish Act on Higher Education and Science. Available from: https://www.gov.pl/attachment/d6975935-4b24-4be3-96f1-09c51589958a [Accessed 29 December 2023] Art. 469b (4).

[65] Author's translation. Data Protection Act. Available from: https://www.riigiteataja.ee/en/eli/523012019001/consolide[Accessed 29 December 2023] Section 6 (1).

[66] (1050/2018) Available from: https://www.finlex.fi/en/laki/kaannokset/2018/en20181050.pdf [Accessed 29 December 2023] Section 6.

[67] Ibid., Art. 35.

[68] Ibid., Art. 35 (3) (b).

[69] Art. 29 DP WP, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, Revised and Adopted on 4 October 2017 (17/EN, WP 248 rev.01) Available from: https://ec.europa.eu/newsroom/article29/items/611236/en [Accessed 29 December 2023] pp. 9-12.

[70] Ibid., p. 11.

Despite both the overarching obligation for all controllers and processors to conduct a DPIA where this is mandated under Art. 35 GDPR, and the fact that scientific research is not highlighted as requiring a DPIA by the relevant authorities, some of the Member States whose laws were reviewed for this article chose to include a specific obligation, in their national laws, to conduct such an assessment in respect of processing activities for the purpose of scientific research; particularly where this is conducted on special category data.

Belgium, Finland and Ireland all require a DPIA where health data are to be processed for research purposes. Belgian law mandates a DPIA for the processing of all special category data for scientific purposes unless there is a code of conduct in place;[71] Finland mandates a DPIA where special categories of data are to be processed for research purposes if data subjects' rights are to be derogated from in terms of the same law.[72] In the latter case, the DPIA must be sent to the Data Protection Ombudsman before processing begins. Ireland requires an assessment to be made in respect of the concerned health research, and where such an assessment indicates a "high risk to the rights and freedoms of individuals', requires a DPIA.[73]

Thus, while Member States have incorporated the same notions and measures discussed above into their national data protection legislative frameworks, they have done so to different extents, in relation to different categories of data and in respect of different circumstances.

5. WAY FORWARD

5.1. LAWS IMPLEMENTING ART. 9 (2) (J)

The measures considered in the previous section likely not only qualify as "appropriate safeguards" within the meaning of Art. 89 (1), but also fulfil the requirements of "suitable and specific measures" required by Art. 9 (2) (j) if and when they are provided for in a law that sets out the scope and purposes of processing of special category data for research purposes. The suitability of any such measures in the context of Art. 9 (2) (j) will depend more on their being tailormade to the specific research context (e.g. research carried out in the context of a bio- or other "data" bank) than on their inclusion in any pre-established set of measures. Therefore, the focus of any discussion on Art. 9 (2) (j) should be the specific law it calls for. In order to elucidate this point, it is helpful to consider two pertinent pieces of legislation in light

[71] See EHDS (2022), Sections 191, 187.
[72] See Estonian Data Portection Act, *op. cit.*, Section 31.
[73] HRR, *op. cit.*, Reg. 3 (1) (c) (i) and (ii).

of the Art. 9 (2) (j) requirements: the Irish HRR[74] and the proposed EHDS Regulation.[75]

5.1.1 Irish Health Research Regulations

The Irish HRR govern the processing of personal data for "the purposes of health research," requiring controllers who are processing data for such purposes to take a number of "suitable and specific measures to safeguard the fundamental rights and freedoms of the data subject."[76] Notably, this law not only spells out a list of safeguarding measures, but also sets out the scope of its application by defining the concept of "health research.".[77]

The HRR thus establish safeguarding measures for a specific context, in relation to particular processing operations and defined purposes. Although the wording of Reg. 3 (1) is not exactly the same as that of Art. 9 (2) (j),[78] and the HRR do not specifically state that they are intended to implement Art. 9 (2) (j), the structure of the law and the rules it sets out may be said to correspond to the Art. 9 (2) (j) criteria. Nonetheless, it is not without its limitations: while in theory the HRR present an opportunity for controllers to opt for a legal basis other than consent for data processing for health research purposes, they re-introduce the GDPR notion of "explicit consent" as an obligatory safeguard.[79] Thus, in practice, controllers still need to seek data subjects' consent for their research activities. Moreover, it appears that the HRR will apply irrespective of the Art. 9 (2) exception chosen by controllers for the relevant processing.

5.1.2 EHDS Regulation

The proposed EHDS Regulation aspires towards a European "space" for electronic health data and mechanisms by which such data may be requested for various specific purposes, including for scientific research. It thus aims to make electronic health data more readily-available across the EU and to establish a "governance framework" for the access and use of such data for predetermined purposes.[80] In fact, in its substantive provisions, the EHDS sets out the relevant categories of data, the purposes for which they may

[74] HRR, *op. cit.*
[75] EHDS, *op. cit.*
[76] HRR, *op. cit.*, Reg. 3 (1).
[77] Ibid., Reg. 3 (2).
[78] The former speaks of safeguarding the "fundamental rights and freedoms of the data subject" and the latter of safeguarding the "fundamental rights and *interests* of the data subject."
[79] HRR, *op. cit.*, Reg. 3 (1) (e).
[80] EHDS (2022), *op. cit.*, Art. 1 (1).

be processed, and requisite safeguards.[81] In contrast with the HRR, it also explicitly states that it is intended to form a legal basis "in accordance with Art. 9 (2) (g) (h) (i) and (j) GDPR," albeit in a non-binding recital.

It remains unclear, however, which purposes listed under Art. 34 specifically correspond to Art. 9 (2) (j). Furthermore, controllers intending to access electronic health data in pseudonymised format under the EHDS must themselves determine an appropriate legal basis under Art. 6 GDPR and reflect this in their request for a data permit.[82] However, there is no parallel requirement to reflect the exception availed of under Art. 9 (2) in a data permit request. The proposed Regulation has in fact been criticized for its lack of clarity by both the EDPB and the EDPS,[83] and it remains to be seen how it will be applied in practice if adopted in its current form.

5.2. CODES OF CONDUCT

Against a background of divergent MS laws and practices pertaining to data processing for scientific research purposes, a harmonised EU law implementing Art. 9(2)(j) is not currently envisaged. As discussed, the EHDS itself does not deliver sufficient clarity regarding the use of health data for scientific research purposes. Furthermore, national laws implementing Art. 9 (2) (j) may provide legal certainty for entities operating solely within a concerned Member State's territory, but do little to encourage or enable seamless data flows across the EU and the ERA.

The GDPR presents a possible solution to this too, by permitting the drawing up of Codes of Conduct which may then be approved by the relevant supervisory authority or EDPB.[84] Such Codes are perceived as useful tools for lawful collaboration and data sharing across the EU.[85] Nevertheless, developing such a Code intended to bridge existing gaps between Member States is neither a straightforward nor a fast process.[86] Various Codes relating to health research have been proposed following the entry into force of

[81] Ibid., Arts. 33 and 34.

[82] Ibid., Art. 45 (4).

[83] EDPB and EDPS, Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space, Adopted on 12 July 2022. Available from: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032022-proposal_en [Accessed 29 December 2023] p. 23 paras. 87-90.

[84] Art. 40.

[85] EDPS, p. 25. See also: Krekora-Zajac, D., Marciniak, B. and Pawlikowski, J. (2021) Recommendations for Creating Codes of Conduct for Processing Personal Data in Biobanking Based on GDPR art.40. *Frontiers in Genetics*, 12, p. 2.

[86] Krekora-Zajac, D., Marciniak, B. and Pawlikowski, J. (2021) Recommendations for Creating Codes of Conduct for Processing Personal Data in Biobanking Based on GDPR art.40. *Frontiers in Genetics*, 12, p. 3.

the GDPR, but thus far, these are either a work in progress,[87] have not been formally approved,[88] or are still awaiting approval from the relevant authority.[89]

5.3. LEGAL BASIS UNDER ART. 6 GDPR

It is an established principle that controllers who have identified an exception under Art. 9 (2) for the processing of prohibited special category data, must still also have a legal basis under Art. 6 for the concerned processing.[90] It is not the aim of this paper to discuss all possibilities under Art. 6, however, the authors note that the most appropriate legal basis under this provision will differ depending on the type of entity that is carrying out the research - whether it is a public or private organisation - and the nature or purpose of the research.

Scientific research is often carried out by public or publicly-funded organisations and in the public interest. Thus, such entities could on the basis of their public nature rely on the widely-accepted legal basis for public authorities in the first limb of Art. 6 (1) (e), which permits data processing "for the performance of a task carried out in the public interest," in lieu of consent. The authors believe that a private entity could also - in principle - rely on this provision if and when the concerned research is in the public interest. Private entities would naturally need to justify why they are opting for this provision as opposed to Art. 6 (1) (f) and demonstrate the inherent public interest in

[87] BBMRI-ERIC's "Code of Conduct for Health Research." Further information available from: https://code-of-conduct-for-health-research.eu/ [Accessed 28 December 2023].

[88] Coreon's Code of Conduct for Health Research. Available from: https://www.coreon.org/wp-content/uploads/2023/06/Code-of-Conduct-for-Health-Research-2022.pdf [Accessed 29 December 2023].

[89] EUCROF's Code of Conduct for Service Providers in Clinical Research. Further information available from: https://www.eucrof.eu/images/21_03_22_20210306_EUCROF_Code_-_Introduction_Note.pdf [Accessed 29 December 2023]; EFPIA's Code of Conduct on Clinical Trials and Pharmacovigilance. Further information available from: https://www.efpia.eu/news-events/the-efpia-view/statements-press-releases/efpia-statement-on-a-gdpr-code-of-conduct/ [Accessed 28 December 2023].

[90] See: Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, Adopted on 9 April 2014 (844/14/EN, WP 217) Available from: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm [Accessed 29 December 2023] pp. 15-16; Donnelly, M. and MacDonaugh, M. (2019) Health, Consent and the GDPR Exemption *European Journal of Health Law,* 26, p. 101; Comandè, G. and Schneider, G. (20212) Differential Data Protection Regimes in Data-Driven Research: Why the GDPR is More Research-Friendly Than You Think. *German Law Journal,* 23, p. 570; and Case C-667/21 *Krankenversicherung Nordrhein* [2023] ECLI:EU:C:2023:1022.

their research activities, and may thus find it more challenging to apply this basis in practice.[91]

In any case, and most importantly to the present discussion, Art. 6 (1) (e) also requires a corresponding national law that governs the relevant processing. The authors postulate that the law required by Art. 9 (2) (j) could thus serve a "double" purpose and strive to also fulfil the requirements set out in Art. 6 (1) (e). This would make it straightforward for controllers to opt for Arts. 9 (2) (j) and 6 (1) (e) when processing data for scientific research purposes.

6. CONCLUSION

Consent tends to be the most resorted to legal basis and/or exception for the processing of special category data for scientific research purposes. As this paper has shown, this is potentially problematic for researchers due to the strict consent requirements under the GDPR. Furthermore, it does not necessarily result in effective protection for concerned data subjects. The GDPR itself permits an alternative option by virtue of Art. 9 (2) (j), which requires in particular that the processing be based on a Union or national law providing for adequate protection for data subjects' fundamental rights and interests. Thus, this provision not only alleviates researchers of the burden of having to base their processing on the legal basis of consent but, if correctly implemented, also ensures that data subjects' rights and interests are more adequately and effectively protected than if the processing were to be based on their consent.

Art. 9 (2) (j) refers to Art. 89 (1), establishing a two-tier requirement of safeguarding measures; those required by Art. 9 (2) (j) itself, termed "suitable and specific measures" and the Art. 89 (1) "appropriate safeguards." While there is no guidance on the difference, if any, between these two sets of measures, it is likely that in practice each set will comprise similar or even identical measures. However, those set out in Art. 89 (1) apply to the processing of all personal data (not just special category data), while the suitable and specific measures required by Art. 9 (2) (j) should be incorporated in the requisite law that also sets out the context, scope and purposes of the processing.

Since there is currently no EU law implementing Art. 9 (2) (j), Member States have taken a fragmented approach, and although there are many safeguarding measures commonly applied across the EU, these are implemented differently in each Member State. Laws implementing Art. 9 (2) (j) are thus specific to the country in which they have been adopted.

[91] Quinn (2021), *op. cit.*, p. 9.

Even in the proposed EHDS Regulation, which purports to be a legal basis in accordance with Articles 9 (2) (g) - (j) GDPR for the secondary use of health data and to establish safeguards for processing, there is remaining uncertainty as to when and how it would be applicable, in practice, in respect of data processing for scientific research purposes.

National laws are helpful to provide legal certainty for entities operating within a Member State. However, they do little to facilitate data sharing as is necessary to establish and maintain a European research area free of internal barriers to the flow of research data. Codes of Conduct may aid with bridging existing differences between different Member State laws and practices. Such Codes represent a more attainable option in the immediate future than a harmonised EU law; however, although several have been proposed since the GDPR's entry into force, none have been formally adopted yet. Further research is required to explore how the law may be applied vis-a-vis upcoming technological infrastructures such as those proposed in the EHDS, how Codes of Conduct may serve to bridge the gaps in this regard and the added value AI/machine learning brings to the research health sector.

As already envisaged in the EHDS initiative, a harmonised EU law implementing Art. 9 (2) (j) is what is needed to strike a fair balance between the various stakeholder interests in the field of health research, as well as to contribute towards the free movement of personal data for research purposes within the EU.

LIST OF REFERENCES

[1] Article 29 Data Protection Working Party, Advice paper on special categories of data ("sensitive data"), Adopted on 20 April 2011 (Ref. Ares(2011)444105) Available from: https://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf [Accessed 29 December 2023]

[2] Article 29 Data Protection Working Party, Guidelines on consent under Regulation 2016/679, Revised and Adopted on 10 April 2018 (17/EN, WP 259 rev.01) Available from: https://ec.europa.eu/newsroom/article29/items/623051/en [Accessed 29 December 2023]

[3] Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, Revised and Adopted on 4 October 2017 (17/EN, WP 248 rev.01) Available from:

https://ec.europa.eu/newsroom/article29/items/611236/en [Accessed 29 December 2023]

[4] Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, Adopted on 9 April 2014 (844/14/EN, WP 217) Available from: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm [Accessed 29 December 2023].

[5] Austrian Data Protection Act. Available from: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen\&Gesetzesnummer=10001597\&FassungVom=2018-05-25 [Accessed 29 December 2023].

[6] BBMRI-ERIC, Code of Conduct for Health Research. Further information available from: https://code-of-conduct-for-health-research.eu/ [Accessed 28 December 2023].

[7] Belgian GDPR Implementing Act. Available from: https://www.dataprotectionauthority.be/publications/act-of-30-july-2018.pdf [Accessed 29 December 2023].

[8] Comandè, G. and Schneider, G. (2022) Differential Data Protection Regimes in Data-Driven Research: Why the GDPR is More Research-Friendly Than You Think. *German Law Journal*, 23.

[9] Council of Europe Convention for the protection of personal data Of 28 January 1981 (ETS 108) Available from: https://www.refworld.org/docid/3dde1005a.html [Accessed 29 December 2023].Coreon"s Code of Conduct for Health Research. Available from: https://www.coreon.org/wp-content/uploads/2023/06/Code-of-Conduct-for-Health-Research-2022.pdf [Accessed 29 December 2023].

[10] Council of the European Union, Preparation of the Council position on the evaluation and review of the General Data Protection Regulation (GDPR) - Comments from Member States, 9 October 2019 (12756/1/19, REV 1) Available from: https://data.consilium.europa.eu/doc/document/ST-12756-2019-REV-1/en/pdf [Accessed 29 December 2023]

[11] DG Food and Health Safety (2021) *Assessment of the EU Member States" rules on health data in the light of GDPR.* Luxembourg: Publications Office of the European Union. Available from: https://health.ec.europa.eu/publications/assessment-eu-member-states-rules-health-data-light-gdpr_en [Accessed 29 December 2023]

[12] Donnelly, M. and MacDonaugh, M. (2019) Health, Consent and the GDPR Exemption *European Journal of Health Law,* 26

[13] Dove, E. S. and Chen, J. (2020) Should consent for data processing be privileged in health research? A comparative analysis. *International Data Privacy Law* 10 (2).

[14] Ducato, R. (2020) Data protection, scientific research and the role of information. *Computer Law & Security Review*, 37

[15] EFPIA"s Code of Conduct on Clinical Trials and Pharmacovigilance. Further information available from: https://www.efpia.eu/news-events/the-efpia-view/statements-press-releases/efpia-statement-on-a-gdpr-code-of-conduct/ [Accessed 28 December 2023].

[16] Estonian Data Protection Act. Available from: https://www.riigiteataja.ee/en/eli/523012019001/consolide[Accessed 29 December 2023]

[17] EUCROF Code of Conduct for Service Providers in Clinical Research. Further information available from: https://www.eucrof.eu/images/21_03_22_20210306_EUCROF_Code_-_Introduction_Note.pdf [Accessed 29 December 2023]

[18] European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/678, Adopted on 4 May 2020 (Version 1.1) Available from: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en [Accessed 29 December 2023].

[19] EDPB, Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (art.70.1.b)), Adopted on 23 January 2019. Available from: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-32019-concerning-questions-and-answers_en [Accessed 29 December 2023].

[20] EDPB and EDPS, Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space, Adopted on 12 July 2022. Available from: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032022-proposal_en [Accessed 29 December 2023] p. 23 paras. 87-90.

[21] European Data Protection Supervisor, A Preliminary Opinion on data protection and scientific research, Adopted on 6 January 2020. Available from: https://edps.europa.eu/data-protection/our-work/publications/opinions/preliminary-opinion-data-protection-and-scientific_en [Accessed 29 December 2023]

[22] Finnish Data Protection Act (1050/2018) Available from: https://www.finlex.fi/en/laki/kaannokset/2018/en20181050.pdf[Accessed 29 December 2023]

[23] German BDSG. Available from: https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html [Accessed 29 December 2023]

[24] Hallinan, D. (2020) Broad consent under the GDPR: an optimistic perspective on a bright future. *Life Sciences, Society and Policy*, 16 (1).

[25] Hallinan, D. and Friedewald, M. (2015) Open consent, biobanking and data protection law: can open consent be "informed" under the forthcoming data protection regulation? *Life Sciences, Society and Policy*, 11 (1).

[26] ICO. (2023) *Public Task.* [online] Cheshire:ICO. Available from: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/public-task/ [Accessed 29 December 2023].

[27] Irish Data Protection Act 2018. Act Number 7 of 2018. Available from: https://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html [Accessed 29 December 2023]

[28] Irish Health Research Regulations. Available from: https://www.irishstatutebook.ie/eli/2018/si/314/made/en/pdf[Accessed 29 December 2023].

[29] Krekora-Zajac, D., Marciniak, B. and Pawlikowski, J. (2021) Recommendations for Creating Codes of Conduct for Processing Personal Data in Biobanking Based on GDPR art.40. *Frontiers in Genetics,* 12

[30] Kuner, C., Bygrave L. A., Docksey, C. and Drechsler, L. (*eds.) The EU General Data Protection Regulation (GDPR), A Commentary.* New York: Oxford University Press

[31] Malta Subsidiary Legislation 528.10. Available from https://legislation.mt/Legislation [Accessed 29 December 2023]

[32] Manis, M. (2017) The processing of personal data in the context of scientific research. The new regime under the EU-GDPR. *BioLaw Journal - Rivista di BioDiritto*, 3.

[33] Milieu Consulting SRL, Study on the appropriate safeguards under article 89 (1) GDPR for the processing of personal data for scientific research, Adopted in August 2021 (EDPS/2019/02-08) Available from: https://edpb.europa.eu/our-work-tools/our-documents/legal-study-external-provider/legal-study-appropriate-safeguards-under_en [Accessed 29 December 2023]

[34] Polish Act on Higher Education and Science. Available from: https://www.gov.pl/attachment/d6975935-4b24-4be3-96f1-09c51589958a [Accessed 29 December 2023]

[35] Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, (COM/2022/197 final) 3 May. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex?3A52022PC0197 [Accessed 29 December 2023].

[36] Quinn, P. (2021) Research under the GDPR – a level playing field for public and private sector research? *Life Sciences, Society and Policy*, 17 (4).

[37] Regulation (EU) No 536 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC. *Official Journal of the European Union* (2014/L-158/1) 27 May. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex\%3A32014R0536 [Accessed 29 December 2023].

[38] Staunton et al (2022) Appropriate Safeguards and Article 89 of the GDPR: Considerations for Biobank, Databank and Genetic Research. *Frontiers in Genetics*, 13.

[39] UNESCO Universal Declaration on Bioethics and Human Rights Of 19 October 2005. Available from: https://en.unesco.org/about-us/legal-affairs/universal-declaration-bioethics-and-human-rights [Accessed 29 December 2023]

[40] United Nations General Assembly, Right of everyone to the enjoyment of the highest attainable standard of physical and mental health, Adopted on 10 August 2009. Available from: https://www.refworld.org/pdfid/4aa762e30.pdf [Accessed 29 December 2023].

[41] World Medical Association, *Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Subjects*, June 1964. Available from: https://www.wma.net/policies-post/wma-declaration-of-helsinki-ethical-principles-for-medical-research-involving-human-subjects/ [Accessed 29 December 2023]

[42] World Medical Association, *Declaration of Taipei on Ethical Considerations Regarding Health Databases and Biobanks,* October 2022. Available from https://www.wma.net/policies-post/wma-declaration-of-taipei-on-ethical-considerations-regarding-health-databases-and-biobanks/ [Accessed 29 December 2023].

DOI 10.5817/MUJLT2024-1-2

HUMOUR AND INTELLECTUAL PROPERTY LAW: TRADEMARK PARODY PERSPECTIVE IN THE CZECH REPUBLIC

by

MICHAL JEŽEK *

This article discusses the issue of humour in the context of intellectual property law, with a focus on parody in trademark law. Parody is a form of humorous expression that is generally protected by freedom of expression. Although copyright law has a statutory exception for caricature, parody, and pastiche, no such exception exists in trademark law. Therefore, parody must be treated differently in this area of law. The article first introduces the legal position of parody and discusses the assessment of parody in both copyright and trademark law in the EU and Czech law. Then it examines the peculiarities of the trademark law approach and with the help of German landmark cases, highlights the possibilities for the treatment of trademark parody in the Czech Republic. The outcomes may apply to closely related laws throughout the EU territory.

KEY WORDS

Humour, Parody, Copyright, Trademark, Freedom of Expression

* PhD student, Department of International and European Law, Faculty of Law, Masaryk University, Brno, Czech Republic, 2024, Michal.Jezek@law.muni.cz, ORCID: 0009-0006-1343-7916. The author would like to express his gratitude to JUDr. Radim Charvát, Ph.D., LL.M. and doc. JUDr. Pavel Koukal, Ph.D. for their comments on earlier drafts of this article. The author would also like to thank both anonymous reviewers for their constructive and valuable feedback.

1. INTRODUCTION

Generally (and historically[1]), parody is a form of artistic expression that is usually associated with the imitation of a particular work, person or style.[2] For a parody to be successful (i.e. to amuse the recipient), there must be a connection between the parodic creation and the original work.[3] The legal definition of parody was introduced by the Court of Justice of the EU ("CJEU") in the landmark copyright parody case *Deckmyn*[4] (see Chapter 3 below for details of the case).

Concerning both Czech and EU law, the issue of parody was introduced by the Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society[5] („InfoSoc Directive") which introduced an optional statutory exception to copyright for caricature, parody and pastiche in its Art. 5(3)(k). The Czech Republic adopted this provision in 2017.[6,7] This statutory exception means that the copyrighted work may be used for caricature, parody or pastiche without the author's consent. However, other elements must be fulfilled when applying this exception and using another person's work.[8]

---

1 Cf. Dentith, S. (2000) *Parody*. London: Routledge, p. 45-46.

2 Cf. OED (2023) *Oxford English Dictionary,* s.v. "parody (n.2), sense 1.a," [online] Available from: https://doi.org/10.1093/OED/4390633272 [Accessed 14 December 2023].

3 Cf. e.g. *Cliffs Notes, Inc. v. Bantam Doubleday Dell Publishing Group, Inc*. (1989) United States Court of Appeals, Second Circuit, 886 F.2d 490, paragraph 494; or Fletcher, A. L. (2010). The Product with the Parody Trademark: What's Wrong with Chewy Vuiton. *The Trademark Reporter*, 100 (5), p. 1094, citing *Louis Vuitton Malletier S.A. v. Haute Diggity Dog, LLC*, United States Court of Appeals, Fourth Circuit, 507 F.3d 252.

4 Judgement of 3 September 2014, Johan Deckmyn, Vrijheidsfonds VZW v. Helena Vandersteen, C-201/13, EU:C:2014:2132.

5 Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society. *Official Journal of the European Union* (L 167) 22 June 2001. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex\%3A32001L0029 [Accessed 3 October 2022].

6 Sec. 38g of *Act on Copyright and Rights Related to Copyright 2000*, No. 121/2000 Coll. The Czech Republic. Prague: Collection of Laws. In Czech ("Czech Copyright Act"). In 2017, this provision dealt only with the exception for caricature and parody. The exception for pastiche was added in the latest amendment to the Czech Copyright Act, Act No. 429/2022 Coll., which entered into force on 5 January 2023.

7 As Telec and Tůma pointed out, before the introduction of the exception into the Czech Copyright Act, it was possible for the courts to cover the issues of caricature or parody by a simple balancing test of the conflicting fundamental rights. This means that caricature and parody were already an inherent limitation of copyright by that time. See Telec, I. and Tůma, P. (2019) Komentář k § 38g. In: Ivo Telec, Pavel Tůma (eds.). *Autorský zákon: Komentář*. Praha: C. H. Beck, p. 470.

8 According to Sec. 29 Czech Copyright Act, the use should not be contrary to the normal exploitation of the work, and it should not unreasonably prejudice the legitimate interests of the author. This provision represents the Czech version of the three-step test.

Although parody is typical for artistic works, it can also be created in the context of trademarks or designs[9]. In the case of trademark parody, there is a risk of trademark infringement.[10] If the parody is successful, there should be no likelihood of confusion. This is because the parody creates an association with the famous mark while at the same time satirizing it (because of its imitation feature).[11] There is no point in creating a parody if no one gets the joke. Therefore, a trademark parody would always target well-known trademarks[12] or trademarks with reputation[13]. "Enjoy Cocaine" instead of "Enjoy Coke"[14] or "Chewy Vuiton" instead of "Louis Vuitton"[15] are just a few examples of trademark parodies.

Trademark parody can take two forms. First, when a parodic sign is applied for registration as a trademark (the issue of parody is therefore addressed during the registration process). Second, the parodic sign is simply used without registration, either for commercial purposes (such as creating parodic merchandise[16]) or non-commercial purposes (e.g. by opening

[9] Although parody in design law is not the primary focus of this article, it is important to note that the current initiative for EU design law reform is trying to introduce the "critique and parody" exception, see Commission Proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 6/2002 on Community designs and repealing Commission Regulation (EC) No 2246/2002. 28 November 2022. Available from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:666:FIN [Accessed 11 May 2024]. For further discussion on this issue see also Jacques, S. and Derclay, E. (2024). The Parody Exception in EU Design Law: A Catalyst for Creative Evolution, Innovation and Cultural Discourse. *European Intellectual Property Review*, 46 (5), p. 285-298.

[10] Myers, G. (1996) Trademark Parody: Lessons from the Copyright Decision in Campbell v. Acuff-Rose. *Law and Contemporary Problems*, 59 (2), p. 181-182.

[11] Cf. Machnicka, A. A. (2016) Louis Vuitton does not laugh at its bags´ parody. *Journal of Intellectual Property Law & Practice*, 11 (5), p. 325.

[12] Art. 6bis of the *Paris Convention for the Protection of Industrial Property*, 20 March 1883, as amended on 28 September 1979. Available from: https://www.wipo.int/wipolex/en/text/287556[Accessed 7 December 2023], and Sec. 2(d) of the *Act on Trademarks and the Amendments to Act No. 6/2002 Coll. on Courts, Judges, Lay Judges and State Court Administration and on the Amendments to Certain Other Acts (Act on Courts and Judges) 2003*, No. 441/2003 Coll. The Czech Republic. Prague: Collection of Laws. In Czech ("Czech Trademark Act").

[13] Art. 5(3) Directive (EU) 2015/2436 of the European Parliament and of the Council of 16 December 2015 to approximate the laws of the Member States relating to trade marks. *Official Journal of the European Union* (L 336/1) 23 December 2015. Available from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015L2436 („Trademark Directive") [Accessed 7 December 2023] and Sec. 7(1)(c) of the Czech Trademark Act.

[14] *Coca-Cola Company v. Gemini Rising* (1972) District Court for the Eastern District of New York, 346 F. Supp. 1183.

[15] *Louis Vuitton Malletier v. Haute Diggity Dog* (2007) Court of Appeals for the Fourth Circuit, 507 F.3d 252.

[16] Cf., e.g. T-Shirts with "PrayStation" sign and depiction of original "PlayStation" trademark, cf. Knedlo Zelo Wear (2024) *Main Page* [online]. Available from https://www.knedlozelowear.cz/ [Accessed 14 April 2024].

the public discussion over topics of societal interest[17]). Both situations can be decided under trademark law; however, the freedom of expression should be part of the appreciation in each of the mentioned examples.

There are only a few cases concerning humour in Czech case law, and (almost) none of them deals with trademark parodies. However, there are examples of parodies (products and signs that meet the basic elements of parody) on the Czech market that can be mentioned in this regard. One of them is the *IbalGIN* case. The "IbalGIN" pink gin, until recently produced by the Fruko-Schulz company, was being sold in bottles with signs similar to the "Ibalgin" trademark[18]. The original "Ibalgin" trademark is known for the famous Czech pain reliever produced by the SANOFI company (formerly Zentiva). Although the *IbalGIN* case is discussed in this paper as an illustrative case, it was brought to the court and recently settled (see Chapter 6 below for more details).[19]

Concerning the structure of this article, first, the issue of parody in the context of freedom of expression is explained, including landmark cases of the European Court of Human Rights ("ECHR"). Secondly, it discusses the scope of the legal approach to parody in copyright and trademark law in both the EU and Czech legal systems. Although the approaches are treated separately, the significant impact of the harmonisation of EU law is emphasised. The coverage of both copyright and trademark law is justified by the premise that trademark parody might borrow the basic assessment features from the determination of copyright parody.[20]

Since there is minimum case law on trademark parody from either the CJEU or the Czech courts and the treatment of trademark parody differs from country to country[21], an analysis of German case law is provided for further assessment of how trademark parody could be treated. The German legal system is relatively close (and not only geographically or historically)[22]

[17] See., e.g. Greenpeace's parody on the "ESSO" trademark, cf. *Greenpeace v Esso* (2008) The French Court of Cassation No. 06-10961.

[18] See Úřad průmyslového vlastnictví (2022) *Trademark registration No. 476663* [online]. Available from: `https://isdv.upv.cz/obr/ozvyprej/663/O-476663.pdf` [Accessed 1 October 2022].

[19] In the following text, "IbalGIN" stands for the "parodic version" whereas "Ibalgin" signifies the original trademark.

[20] E.g., since there is a legal definition of parody introduced by the CJEU for copyright infringement matters, it would not be appropriate to introduce a specific definition for the issue of trademark parody.

[21] Cf. reports of selected states and groups in AIPPI (2002) *Yearbook 2002/I* [online]. Available from: `https://aippi.soutron.net/Portal/Default/en-GB/RecordView/Index/2995` [Accessed 8 January 2024], p. 291-521.

[22] For the proximity of copyright see, e.g., Koukal, P. (2019) *Autorské právo, public domain a lidská práva*. Brno: Masarykova univerzita, p. 73-38; trademark law, on the other hand, is substantially harmonized by the EU law, cf. eg. Sec. 14 of the *Act on the Protection of Trade*

to the Czech law, so the German judicature could be a useful inspiration for the treatment of trademark parody in the Czech Republic, especially, under the influence of the noticeable EU harmonisation of trademark law. The results of the analysed cases are applied to the illustrative case of *IbalGIN*.

This article concludes that a parodic trademark might be protected by freedom of expression; however, it must make at least a minimal statement (comment, criticism, etc.) about the original trademark or society (i.e., it shall raise public debate); otherwise, it would be considered as a purely commercial activity that unfairly takes advantage of the original trademark's reputation. If the above criteria are met, freedom of expression should be considered as a decisive factor in both the parodic trademark registration procedure and its simple factual use.

The relevance of the topic is even of more importance by the fact that the CJEU received a request for a preliminary ruling on the issue of political parody in the *IKEA-PLAN* case[23] (see Section 3.2.1 below for more details). In addition, the Czech courts recently decided the first copyright parody case in the Czech jurisprudence (see Section 4.1 below), and the recent progress in the *IbalGIN* case (including the trademark/RCD invalidity proceedings and the preliminary injunction proceedings) emphasises the topicality of the parody issue in the Czech intellectual property law, same as in the EU territory.

2. FREEDOM OF EXPRESSION IN THE CONTEXT OF PARODY

On the one hand, intellectual property rights can be characterized as an exception to the general freedom to act[24], on the other hand, freedom of expression represents an exception to general intellectual property rights.[25] Freedom of expression is one of the most precious political rights that is protected in all democratic societies. In the context of parodying intellectual

Marks and other Signs 1994, MarkenG. The Federal Republic of Germany. Berlin: Federal Gazzete. In German, which is comparable to Art. 10 of the Trademark Directive and Sec. 8 of the Czech Trademark Act.

[23] Request for a preliminary ruling of 8 May 2023, C-298/23. *Official Journal of the European Union* (C-286/21) 4 August 2023. Available from: `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62023CN0298` [Accessed 7 December 2023].

[24] Cf. e.g. Art. 2(3) of the *Charter of Fundamental Rights and Freedoms* 1993, No. 2/1993 Coll. The Czech Republic. Prague: Collection of Laws. In Czech ("Czech Charter"): "Anyone may do what is not prohibited by law, and no one may be compelled to do what the law does not require".

[25] Cf. Koukal, P. (2019) *Autorské právo, public domain a lidská práva*, op. cit., p. 447-448.

property, freedom of expression is usually on one side of the scale when balancing the rights and interests of the parties involved.[26]

As regards the determination of freedom of expression in intellectual property law, such cases are usually decided based on the expression's nature – whether it is political, artistic or commercial.[27] The more the expression is in the public interest, the less its commercial nature plays a decisive role.[28] The artistic expression might be considered both political and commercial, depending on the context and the intention of the performer.[29] Therefore, the commercialisation of use under the freedom of expression is more problematic[30] and requires a wider scope of assessment from the perspective of political/public debate.

The general (European) scope of the protection of freedom of expression is granted by Art. 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms[31] ("Convention") and Art. 11 of the Charter of Fundamental Rights of the EU[32] ("EU Charter"). All thoughts and opinions may be freely expressed in any form. What matters is the aim and purpose of the expression.[33] Consequently, the expression of an opinion can be part of any artistic work, even if it is rude or shocking.[34] According to the provisions cited, freedom of expression can be restricted by law if the restriction is a "measure necessary in a democratic society" and "pursues any of the legitimate objectives".

The ECHR has already addressed the issue of freedom of expression under Art. 10 of the Convention and intellectual property rights. In

[26] Geiger, Ch. and Izyumenko, E. (2014) Copyright on the Human Rights' Trial: Redefining the Boundaries of Exclusivity Through Freedom of Expression. *International Review of Intellectual Property and Competition Law*, 45 (3), p. 317-318.

[27] Bartoň, M. and Hejč, D. (2021) Čl. 17 [Svoboda projevu a právo na informace]. In: Faisal Husseini et al. (eds). *Listina základní práv a svobod*. Praha: C. H. Beck, p. 540.

[28] Op. cit., p. 543.

[29] Op. cit., p. 541.

[30] Pontes, L. M. (2015) Trademark and Freedom of Speech: A comparison between the U.S. and the EU System in the Awakening of Johan Deckmyn v. Helena Vandersteen. In: *Ninth WIPO Advanced Intellectual Property Research Forum: Towards a Flexible Application of Intellectual Property Law - A Closer Look at Internal and External Balancing Tools*, World Intellectual Property Organization, p. 15.

[31] *Convention for the Protection of Human Rights and Fundamental Freedoms*, 4 November 1950. Available from: `https://www.echr.coe.int/documents/d/echr/convention\_ENG` [Accessed 27 November 2023].

[32] *Charter of Fundamental Rights of the EU*, 18 December 2000 (2000/C 364/01). Available from: `https://www.europarl.europa.eu/charter/pdf/text\_en.pdf` [Accessed 27 November 2023].

[33] Bartoň, M. and Hejč, D. (2021) Čl. 17 [Svoboda projevu a právo na informace]. In: Faisal Husseini et al. (eds). *Listina základní práv a svobod*. Praha: C. H. Beck, p. 516.

[34] Kosař, D. (2012) Čl. 10 [Svoboda projevu]. In: Jiří Kmec et al (eds.). *Evropská úmluva o lidských právech. Komentář*. Praha: C. H. Beck, p. 1007.

the *Ashby Donald* case[35], the ECHR held that Art. 10 of the Convention covered the situation of posting photographs online and thus making an expression via the Internet[36]. In assessing whether the imposed restriction on freedom of expression is necessary for a democratic society, the ECHR stated that the Convention leaves almost no room for restrictions on political speech, whereas, in the area of commerce, states are afforded a wide margin of discretion.[37] Therefore, the work or activity that generates debate on the issue of "public interest" is afforded greater protection than the (purely) commercial one.

In the *Pirate Bay* case[38], the ECHR held that even the sharing of copyrighted material for profits is covered by Art. 10 of the Convention.[39] In the context of both decisions, the ECHR maintains that the nature of the information and the interest at stake represent the key margin of appreciation.[40] The ECHR's findings suggest that parodies are protected under Art. 10 of the Convention and the assessment of their admissibility should be based on the statement of creative intent, whether or not the parody comments on a matter of public interest. Moreover, as stated in the *Goucha v. Portugal* case[41], satire and parody are given a wider margin of appreciation in the context of freedom of expression and both of them naturally aim to provoke and agitate[42].

Generally, the CJEU is in the position to interpret the EU law in accordance with the Convention and its interpretation by the ECHR.[43] Concerning freedom of expression, Advocate General Collins stated in his opinion that both Art. 10 of the Convention and Art. 11 of the EU Charter have the same „meaning and scope".[44]

---

35 *Ashby Donald and others v. France* (2013). No. 36769/08, ECHR.

36 Op. cit, paragraph 34.

37 Op. cit., paragraph 39.

38 *Neij and Kolmisoppi v. Sweden* (2013). No. 40397/12, ECHR.

39 Ibid.

40 For further discussion concerning both cases see e.g. Myška, M. (2013), Ashby Donald v pirátské zátoce: svoboda projevu a vymáhání autorského práva v aktuální judikatuře ESLP. *Revue pro právo a technologie*, 4 (8), pp. 37–41. Available from: `https://journals.muni.cz/revue/article/view/5005` [Accessed 4 November 2023].

41 *Sousa Goucha v. Portugal* (2016). No. 70434/12, ECHR.

42 Op. cit., paragraph 50.

43 Cf. e.g. Judgement of 22 October 2020, Silver Plastics GmbH & Co. KG and Johannes Reifenhäuser Holding GmbH & Co. KG v. European Commission, C-702/19 P, EU:C:2020:857, paragraph 25.

44 Opinion of Advocate General Collins, delivered on 15th June 2023, case C-451/22, RTL Nederland BV, RTL Nieuws BV. *European Court Reports*. Available from: `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62022CC0451` [Accessed 27 November 2023], paragraph 49.

Regarding trademark parody, Advocate General Bobek emphasised that it does "play a role in trademark law".[45] This role of freedom of expression in EU trademark law is reflected in several aspects. First, Art. 51(1) of the EU Charter obliges all official EU institutions to respect the protected rights within the limits of their respective powers. As mentioned above, freedom of expression is protected by Art. 11 the EU Charter. Secondly, Regulation 2017/1001[46] and its Recital 21 ensures that the rules are applied with respect to fundamental rights, in particular, freedom of expression.[47] Finally, in its case law, the EUIPO recognizes that the freedom of expression "must be duly taken into account" when assessing the (in)validity of a trademark.[48]

In his opinion, Advocate General Bobek suggested that "the weight to be given to freedom of expression in the area of trade mark law may be somewhat different, perhaps slightly lighter, in the overall balancing of the rights and interests present"[49] than in the area covered by copyright law (art, culture, literature). The relevant question is how much less weight and under what circumstances freedom of expression might be accorded in trademark parody cases.

As Helfer and Austin point out, "[a]lthough [...] parody is often offensive, it is nevertheless 'deserving of substantial freedom both as entertainment and as a form of social and literary criticism' [...] Denying parodists the opportunity to poke fun at symbols and names which have become woven into the fabric of our daily life, would constitute a serious curtailment of a protected form of expression."[50] Therefore, it may be concluded that whereas parody exception plays the role of an internal limitation

[45] Opinion of Advocate General Bobek, delivered on 2nd July 2019, case C-240/18 P, Constantin Film Produktion GmbH v European Union Intellectual Property Office (EUIPO). *European Court Reports*. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62018CC0240 [Accessed 27 November 2023], paragraph 47.

[46] Regulation (EU) 2017/1001 of the European Parliament and of the Council of 14 June 2017 on the European Union trade mark. *Official Journal of the European Union* (L 154) 16 June. Available from: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32017R1001 [Accessed on 27 November 2023].

[47] Op. cit., paragraph 21 of the recital.

[48] See, for instance, OHIM the Boards of Appeal decision of 2 September 2015, case R 519/2015-4, paragraph 16 (citing OHIM the Boards of Appeal decision of 6 July 2006, case R 495/2005-G, paragraphs 15-17).

[49] Opinion of Advocate General Bobek, delivered on 2nd July 2019, case C-240/18 P, Constantin Film Produktion GmbH v European Union Intellectual Property Office (EUIPO). *European Court Reports*. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62018CC0240 [Accessed 27 November 2023], paragraph 56.

[50] Helfer, L., R. and Austin, G. W. (2011) *Human Rights and Intellectual Property: Mapping the Global Interface*. New York: Cambridge University Press, p. 293.

to the author's rights, freedom of expression shall be understood as an external limitation to the trademark owner's rights.[51]

Apart from the general European scope of protection, in Czech law, freedom of expression is based on Art. 17 of the Czech Charter, which is part of the Czech constitutional order. All the above-mentioned provisions of the Convention, the EU Charter and the Czech Charter shall be duly applied to protect freedom of expression in the Czech case law.

3. EU LAW APPROACH TO PARODY

3.1. PARODY AND COPYRIGHT IN THE EU LAW

The EU copyright law is not fully harmonised or unified. Some Member States of the EU do have open exceptions like the US *fair use* doctrine, e.g. Belgium[52]. However, partial harmonisation of EU copyright law was achieved by the InfoSoc Directive, which, among others, introduced a statutory exception for parody. Although Member States are not obliged to adopt this exception into their copyright laws, the European Parliament recommended that they do so.[53] The Czech Republic has adopted this limitation into the Czech Copyright Act by amending Act No. 102/2017 Coll.

The landmark copyright parody case considered by the CJEU is *Deckmyn*[54]. The merit of the case lies in the calendar created by J. Deckmyn (from Vlaams Belang political party) which shows the Mayor of Gent throwing gold coins to people wearing veils and people of colour. The image was allegedly similar to the cover of the comic book "Suske en Wiske" (created by W. Vandersteen). J. Deckmyn based his defence on political caricature and parody. The Belgian court referred the preliminary question to the CJEU in seeking the definition of parody under EU law.

---

[51] Concerning the trademark law and its external limit see, e.g. Żelechowski, Ł. (2018) Invoking freedom of expression and freedom of competition in trade mark infringement disputes: legal mechanisms for striking a balance. *ERA Forum*, 19, p. 133. Available from: https://link.springer.com/article/10.1007/s12027-018-0498-3 [Accessed 13 April 2024].

[52] Hernandez, I. et al. (2020) *Comparative Advertising and Parodies: Treatment Through a Fair Use Approach Under Trademark and Copyright Law in Selected Jurisdictions* [online]. Available from: https://www.inta.org/wp-content/uploads/public-files/advocacy/testimony-submissions/Comparative-Advertising-and-Parodies-Survey-4.20.20.pdf [Accessed 3 October 2022], p. 5.

[53] European Parliament resolution of 9 July 2015 on the implementation of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society. *Official Journal of the European Union* (C 265/121) 11 August 2017. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52015IP0273 [Accessed 3 October 2022].

[54] Judgement of 3 September 2014, Johan Deckmyn, Vrijheidsfonds VZW v. Helena Vandersteen, C-201/13, EU:C:2014:2132.

The CJEU stated that parody is an autonomous term of the EU law, and therefore only the CJEU can define what parody is.[55] This interpretation is applied uniformly throughout the EU. According to the CJEU, "the essential characteristics of parody are, first, to evoke an existing work while being noticeably different from it, and, secondly, to constitute an expression of hum[o]r or mockery."[56] Moreover, the concept of parody is not subject to any further conditions.[57]

Furthermore, according to the CJEU, conflicting rights and interests must be weighed to strike a fair balance between the copyright holder, on the one hand, and freedom of expression, on the other, and therefore all the relevant circumstances of the case must be taken into account.[58] However, Nordemann and Kraetzig point out that this requirement makes it difficult to implement the definition of parody, as it can "create legal uncertainty and potentially restrict the freedom of expression"[59]. Rigorous application of the principle of non-discrimination, which must always be considered as relevant circumstance, could be hazardous for controversial parodies.[60]

3.2. TRADEMARK PARODY IN THE EU LAW

Two possible outcomes of the EU copyright approach to parody might be applied to the EU trademark law. First, concerning the autonomous definition of parody under the *Deckmyn* case, it does not seem very useful to redefine parody for trademark law purposes, so the assessment of parody should be the same. Second, the necessity of protecting the freedom of expression and its balancing with property rights should be the same in trademark law too.

There is no exception for parody in the harmonisation of the EU trademark law. In the context of parody, the trademark with reputation comes into play. As there is a need to protect the reputation of a trademark, the dilution and confusion principles apply to the assessment of trademark infringement. The harmonising Trademark Directive in its Art. 5(3)(a) states that a trademark shall not be registered or shall be declared invalid if it is identical

[55] Op. cit., paragraph 15.
[56] Op. cit., paragraph 20.
[57] Op. cit., paragraph 21.
[58] Op. cit., paragraphs 27-28.
[59] Nordemann, J. B. and Kraetzig, V. (2016) *The German Bundesgerichtshof changes its concept of parody following CJEU Deckmyn v. Vrijheidsfonds/ Vandersteen.* [blog entry] 3 November. Kluwer Copyright Blog. Available from: `http://copyrightblog.kluweriplaw.com/2016/11/03/the-german-bundesgerichtshof-changes-its-concept-of-parody-following-cjeu-deckmyn-v-vrijheidsfonds-vandersteen/` [Accessed 3 October 2022].
[60] Ibid.

or similar to an earlier trademark (reputed in Member State[61]) "and the use of the later trade mark without due cause would take unfair advantage of, or be detrimental to, the distinctive character or the repute of the earlier trade mark". Furthermore, Art. 10(2)(c) of the Trademark Directive states that the owner of a trademark with reputation is entitled to prohibit any non-consensual use of the sign in the course of trade, irrespective of the goods or services concerned, of the sign which "takes unfair advantage of or is detrimental to, the distinctive character or the repute of the trade mark".

Trademarks with reputation are therefore protected against dilution, tarnishment and taking unfair advantage.[62] [63] In his opinion of the cited judgment, Advocate General Jacobs interpreted all these concepts.[64] First, Jacobs stated that "[t]he essence of dilution [...] is that the blurring of the distinctiveness of the mark means that it is no longer capable of arousing immediate association with the goods for which it is registered and used."[65] Secondly, there is the element of detriment to the reputation of a trademark – tarnishment. According to Jacobs, this is the situation where "the goods for which the infringing sign is used appeal to the public's senses in such a way that the trademark's power of attraction is affected."[66]

Finally, there is the possibility of trademark infringement caused by taking unfair advantage of the distinctive character or reputation of the mark. This is the case of free-riding or an attempt to trade upon the reputation of the earlier mark.[67] The concept of free-riding "covers, in particular, cases where, by reason of a transfer of the image of the mark or of the characteristics which it projects to the goods identified by the identical or similar sign, there

[61] The CJEU prefers quantitative scope, see Judgement of 14 September 1999, General Motors Corporation v. Yplon SA, C-375/97, EU:C:1999:408, paragraph 31: „a registered trade mark must be known by a significant part of the public concerned by the products or services which it covers"; whereas the Czech Supreme Administrative Court prefers qualitative scope, see e. g. *Dermacour Laboratories s.r.o. v. Úřad průmyslového vlastnictví* (2018) Supreme Administrative Court 6 As 71/2018, paragraph 42: „the public, as a result of its use, is familiar with the mark and associates it with the good qualities it expects from the goods or services so marked and places its trust in it" [author's own transalation].

[62] Judgment of 23 October 2003, Adidas-Salomon AG and Adidas Benelux BV v. Fitnessworld Trading Ltd., C-408/01, EU:C:2003:582, paragraph 37.

[63] For the basics of the concepts, its origin and comparison between EU and the US see, e.g. Luepke, M. H. H. (2008) Taking Unfair Advantage or Diluting a Famous Mark - a 20/20 Perspective on the Blurred Differences Between U.S. and E.U. Dilution Law. *Trademark Reporter*, 98(3), pp. 789-833.

[64] Opinion of Advocate General Jacobs, delivered on 10th July 2003, case C-408/01, Adidas-Salomon AG and Adidas Benelux BV v. Fitnessworld Trading Ltd. *European Court Reports* (I-12537) 10 July 2003. Available from: `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX\%3A62001CC0408` [Accessed 7 October 2022].

[65] Op. cit., paragraph 37.

[66] Op. cit., paragraph 38.

[67] Op. cit., paragraph 39.

is clear exploitation on the coat-tails of the mark with a reputation."[68] To obtain protection, the proprietor must prove that there exists a risk of such infringement. The link between the earlier and the later mark should be established.[69]

It is not required to prove the existence of a likelihood of confusion to assess whether a trademark with a reputation has been infringed.[70] However, if the likelihood of confusion is established, it supports the finding of a link created between the signs in the minds of consumers.[71] Without the link, the dilution infringement of a trademark with reputation cannot be stated.[72]

The concept of confusion principle is based on a global appreciation of the visual, aural or conceptual similarity of the conflicting marks (the overall impression and its distinctive and dominant components). As the CJEU stated, "the more distinctive the earlier mark, the greater will be the likelihood of confusion".[73] However, when considering a parody of a reputed trademark, the assessment might be sufficiently based on stating the likelihood of association, i.e. a situation where the consumer is not confused as to the source but makes a psychological association between the conflicting marks, especially when different categories of goods or services are concerned.[74]

The CJEU (the General Court, respectively) in the *Polo/Lauren*[75] case partially dealt with an alleged trademark parody. The dispute between the Polo/Lauren company and OHIM (now EUIPO) dealt with an application for registering an allegedly parodic trademark of Fresh Side company. The original Polo/Lauren trademark depicts a polo player on a horse. The

[68] Judgement of 18 June 2009, L´Oreal SA v. Bellure NV, C-487/07, EU:C:2009:378, paragraph 41.

[69] Charvát points out that trademark protection against "free-riding" (the taking of an unfair advantage) in the absence of confusion and economic harm to the trademark owner's rights is debatable and rather redundant. In Charvát's view, this is reflected in the US law where the provision prohibiting "free-riding" of the reputation was excluded in 2006 by the Trademark Revision Dilution Act. See Charvát, R (2012). Ochranná známka s dobrým jménem dle práva Evropské unie a České republiky. *Právní rozhledy*, 20(22), p. 787.

[70] Judgement of 11 November 1997, Sabel v. PUMA, C-251/95, EU:C:1997:528, paragraph 20.

[71] Judgement of 27 November 2008, Intel Corporation Inc. v. CPM United Kingdom Ltd, C-252/07, EU:C:2008:655, paragraph 30.

[72] Op. cit., paragraph 31.

[73] Judgement of 11 November 1997, Sabel v. PUMA, C-251/95, EU:C:1997:528, paragraph 22-24.

[74] Cf. e.g. Judgement of 14 September 1999, General Motors Corporation v. Yplon SA, C-375/97, EU:C:1999:408, paragraph 23; or Judgement of 27 November 2008, Intel Corporation Inc. v. CPM United Kingdom Ltd, C-252/07, EU:C:2008:655, paragraph 30.

[75] Judgment of 18 September 2014, The Polo/Lauren Company, LP v. OHIM, T-265/13, EU:T:2014:779.

"parodic" trademark depicts a polo player on a bicycle.[76] OHIM rejected Polo/Lauren's opposition to the application and the OHIM Board of Appeal sustained this verdict. However, the CJEU annulled the OHIM's decision on the basis of the earlier trademark with reputation protection and on the grounds of a finding of similarity between the signs.[77] Therefore, both the doctrine of dilution and the doctrine of confusion were applied in mutual combination. In the following proceeding, OHIM found that the alleged parody was taking advantage of the original's reputation for economic purposes.[78] As OHIM stated, "[t]his is not about stopping parody, but it cannot be right to grant protection to a sign that gains cachet by mocking the reputation of another. When the reputation of a brand is involved, trade mark law has no sense of humour."[79] Thus, the OHIM confirmed that parody itself does not constitute a ground for the exclusion of trademark infringement.[80] However, the EU is still awaiting a pure trademark parody case in front of the CJEU that would lead to a clear conclusion of trademark parody treatment.

3.2.1 IKEA-PLAN – *Deckmyn* of a trademark parody?

On 8 May 2023, the Dutch Business Court in Brussels (*Nederlandstalige Ondernemingsrechtbank*) referred to the CJEU a request for a preliminary ruling in the case of political parody on the "IKEA" trademark.[81] There are three referred questions[82], which might be simply put as:

1) Whether freedom of expression constitutes a "due cause" for using a well-known trademark?

2) What are the criteria taken into account when assessing the balance of fundamental rights in question?

3) Can the national court take into account the list of criteria, e.g. "the extent to which the expression has a commercial character

[76] Op. cit., paragraphs 2 and 6.
[77] Op. cit., paragraphs 32, 33 and 39.
[78] OHIM the Boards of Appeal decision of 7 July 2015, case R 353/2015-5, paragraph 60.
[79] Ibid.
[80] Sitko, J. (2018) Parodia w kontekście naruszenia prawa do zarejestrowanego znaku towarowego (analiza prawnoporównawcza). In: Janusz Barta, Jakub Chwalba, Ryszard Markiewicz, Piotr Wasilewski (eds.) *Qui bene dubitat, bene sciet. Księga jubileuszowa dedykowana Profesor Ewie Nowińskiej*. Warsaw: Wolters Kluwer Polska, p. 687.
[81] Request for a preliminary ruling of 8 May 2023, C-298/23. *Official Journal of the European Union* (C-286/21) 4 August 2023. Available from: `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62023CN0298` [Accessed 27 November 2023].
[82] For the exact wording of the questions see Ibid.

or purpose" or "the extent to which the expression has a public interest, is socially relevant or opens a debate" etc.?

The subject-matter of the case is based on a political campaign (by the same party as in the *Deckmyn* case) using the blue and yellow logo for "IKEA-PLAN" concerning the reform of migration policy in Belgium.[83] While IKEA assumes trademark infringement, the political party claims parody as "due cause" for using the "IKEA" trademark.[84]

In this case, the CJEU has the opportunity to comment fully on the issue of freedom of expression in the context of trademark parody, possibly setting the boundaries of when and how this fundamental right will be curtailed. The significance of this case will no doubt be compared to the *Deckmyn* case and its implication for parody in (EU) copyright law. The importance of the case is emphasized by the fact that the International Trademark Association ("INTA") has submitted an amicus brief to the CJEU in this particular case.[85] INTA's intervention in the case is that the CJEU should not extend the interpretation of "due cause" by "allowing 'parody' as a general fair use defense in trademark infringement cases".[86] In this sense, INTA believes that the "due cause" principle is designed to avoid unnecessary damage to the trademark by the infringer and that "freedom of expression does not automatically secure non-infringement".[87] The CJEU does not have to and formally cannot consider INTA's submission. However, it will be interesting to see whether some of the ideas/arguments put forward by INTA will feature in the CJEU's decision.

4. THE CZECH LAW APPROACH TO PARODY

4.1. COPYRIGHT

The Czech Republic, as a Member State of the EU, has adopted a statutory exception for caricature and parody from the InfoSoc Directive into Sec. 38g of the Czech Copyright Act. To qualify for the use of the exception, all

[83] See Rosati, E. (2023) *What role for freedom of expression under EU trade mark law? An "IKEA-PLAN" prompts a CJEU referral.* [blog entry] 9 July. The IPKat. Available from: `https://ipkitten.blogspot.com/2023/07/what-role-for-freedom-of-expression.html` [Accessed 27 November 2023]; as Rosati points out, IKEA stands for „Immigratie Kan Echt Anders", meaning „Immigration can really change".

[84] Ibid.

[85] Parotta, N. and Lubberger, A. *INTA Attempts to File Amicus Brief with CJEU in Preliminary Ruling Case.* [online]. International Trademark Association. Available from: `https://www.inta.org/news-and-press/inta-news/inta-attempts-to-file-amicus-brief-with-cjeu-in-preliminary-ruling-case-involving-ikea/` [Accessed 10 May 2024].

[86] Ibid.

[87] Ibid.

elements of the three-step test must be met.[88] According to Czech scholars, this provision helps to strike a balance of interests between the rights and freedom of expression.[89] However, after five years of the effectiveness of the provision, so far only one parody case has been decided under the parody exception.

The case concerns a conflict between Greenpeace Czech Republic and Czech Energy Group[90] ("ČEZ"). Greenpeace transformed the three advertising videos of ČEZ by inserting new footage (images of forest fires and deforestation, dead bodies, exhausted coal mines) accusing ČEZ of causing climate change. All three transformed videos were posted by Greenpeace on its Facebook page.[91] The Prague Municipal Court found that neither of the characteristics nor the three-step test had been met.[92] The High Court in Prague reversed the judgment of the Municipal Court.[93]

First, the High Court held that in this case, it is a parody according to *Deckmyn's* definition because the transformed videos evoked the original by adding horrifying images, thus creating irony.[94] Furthermore, it also met the three-step test (the spots were still used as videos and the reversal of the meaning of the original advertisement to the public is the essence of parody).[95] In addition, the Greenpeace spots do not conflict with a normal exploitation of the original work and do not unreasonably prejudice the legitimate interests of ČEZ, since it must be clear to any user that the new spots are part of an "ecological battle" in which ČEZ is in the "opposing" position.[96]

---

[88] Three-step test is regulated in Sec. 29 Czech Copyright Act. The elements of the test deal with limitations and exceptions to exclusive rights in 1) certain special cases which 2) do not conflict with a normal exploitation of the work and 3) do not unreasonably prejudice the legitimate interests of the right holder.

[89] Telec, I. and Tůma, P. (2019) Komentář k § 38g. In: Ivo Telec, Pavel Tůma (eds.). *Autorský zákon: Komentář*. Praha: C. H. Beck, p. 470.

[90] The Czech Republic holds major assets of the group.

[91] Three video spots were dealt in different proceedings but at the same court and judge. See *ČEZ a. s. v. Greenpeace Česká republika, z.s.* (2020) Municipal Court Prague 32 C 2/2019 [not published]; *ČEZ a. s. v. Greenpeace Česká republika, z.s.* (2020) Municipal Court Prague 32 C 7/2019 [not published]; *ČEZ a. s. v. Greenpeace Česká republika, z.s.* (2020) Municipal Court Prague 32 C 1/2020 [not published]. Therefore, the findings in all cases are the same. Against all the decisions, an appeal was brought.

[92] *ČEZ a. s. v. Greenpeace Česká republika, z.s.* (2020) Municipal Court Prague 32 C 7/2019.

[93] See *ČEZ a. s. v. Greenpeace Česká republika, z.s.* (2022) High Court Prague 3 Co 54/2021 [not published]; *ČEZ a. s. v. Greenpeace Česká republika, z.s.* (2022) High Court Prague 3 Co 55/2021 [not published]; *ČEZ a. s. v. Greenpeace Česká republika, z.s.* (2022) High Court Prague 3 Co 56/2021 [not published].

[94] *ČEZ a. s. v. Greenpeace Česká republika, z.s.* (2022) High Court Prague 3 Co 54/2021 [not published].

[95] Ibid.

[96] Ibid.

An extraordinary appeal was made against all these decisions.[97] The Supreme Court had to deal with the question of law, whether an audiovisual work might be used for parody. The Supreme Court first stated that there is no reason why a parody of an audiovisual work should not be allowed. Regarding the requirement of "normal exploitation of the original work", the Supreme Court confirmed that in this case, the insertion of new footage was the essence of the parodic use by creating critical/ironic comments. The Supreme Court also held that it is irrelevant whether the parody was successful. The decisive matter is the artistic intent of the creator. It was also emphasized that individuals or organizations involved in public debate must be able to withstand a higher level of criticism.[98,99] The findings of the Supreme Court were upheld by the Czech Constitutional Court,[100] which, among others, stated that humour (satire, parody, irony) is part of daily life and a crucial part of democratic society.[101]

4.2. TRADEMARKS

There is no statutory exception for parody in Czech trademark law. As in the case of copyright, the EU harmonisation is also applied in the Czech trademark law. Therefore, both the doctrine of dilution and the doctrine of confusion are included in the Czech Trademark Act. Pursuant to Sec. 8(2)(c) of the Czech Trademark Act, the use of a similar or confusing mark is prohibited if the earlier mark has a certain reputation in the Czech Republic, regardless of the categories of goods and services, if such use may be detrimental to the distinctive character or reputation of the mark or would take unfair advantage of it. In addition, Sec. 8(2)(b) Czech Trademark Act prohibits the use of a mark that creates a likelihood of confusion with an earlier mark.

The key element in determining trademark parody is the aspect of the trademark's reputation and its recognition by the relevant section of

[97] See *ČEZ a. s. v. Greenpeace Česká republika, z.s.* (2023) Supreme Court 23 Cdo 2178/2022; *ČEZ a. s. v. Greenpeace Česká republika, z.s.* (2023) Supreme Court 23 Cdo 2403/2022; *ČEZ a. s. v. Greenpeace Česká republika, z.s.* (2023) Supreme Court 23 Cdo 2627/2022. The former is a decision on the merits, and the rest of the decisions dismiss the extraordinary appeal.

[98] Cf. *ČEZ a. s. v. Greenpeace Česká republika, z.s.* (2023) Supreme Court 23 Cdo 2178/2022.

[99] For the translated version of the the decision *ČEZ a. s. v. Greenpeace Česká republika, z.s.* (2023) Supreme Court 23 Cdo 2178/2022 see Koukal, P. and Ježek, M. (2024) Parody of Audio-Visual Works. *GRUR International*, 73(2), pp. 172-179.

[100] *ČEZ a. s. v. Greenpeace Česká republika, z.s.* (2024) Constitutional Court I. ÚS 2956/23; *ČEZ a. s. v. Greenpeace Česká republika, z.s.* (2024) Constitutional Court I. ÚS 2957/23; *ČEZ a. s. v. Greenpeace Česká republika, z.s.* (2024) Constitutional Court IV. ÚS 2979/23.

[101] *ČEZ a. s. v. Greenpeace Česká republika, z.s.* (2024) Constitutional Court I. ÚS 2956/23, paragraph 30.

the public. The degree of such recognition and reputation may outweigh the differences in goods and services.[102] The most famous marks, e.g. "Coca-Cola" or "Adidas", transcend the boundaries of their relevant markets and would be recognized by almost every person on the planet. In the absence of a precise provision on parody, the determination of whether a trademark parody is permissible relies on the dilution or confusion tests and, in general, on a balancing of the interests and rights of the owners and the parodists (in terms of freedom of expression).[103]

The Industrial Property Office of the Czech Republic[104] has not dealt with parody in any trademark registration procedure[105]. A similar conclusion can be drawn from Czech case law. The only case that could be considered to cover the issue of trademark parody was the case of the "LEGO" figures and trademarks used for the political campaign.[106]

The Czech Piracy Party[107] used "LEGO" figures in one of its pre-election videos. The Czech Constitutional Court's decision contains some interesting remarks. First, the "LEGO" trademark has a certain reputation as it is known to the public. Second, the pre-election video was found humorous.[108] Finally, the Constitutional Court found that although the "LEGO" trademark was used as a part of political expression and criticism of intellectual property as a part of the political program, but to the court's view, this message could have been conveyed in a way that did not infringe on the owner's rights.[109]

This result aligns with the general requirement of balancing the contested fundamental rights. The decision states that even satirical political expression might be in contrary to the trademark owner's rights. The finding is relatively strict. From the general context of the video, it cannot be assumed that

[102] Peřinová, E. (2020) Komentář k § 7. In: Peřinová, E. et al. (eds). *Zákon o ochranných známkách: Praktický komentář*. Praha, Wolters Kluwer, p. 55-56.

[103] For further perspective of how trademark parody cases are treated in the EU, see also Ramalho, A. (2009). Parody in Trademarks and Copyright: Has Humour Gone Too Far. *Cambridge Student Law Review*, 5(1), 58-74. For the US perspective, cf. e.g. Simon, D. A. (2013). The Confusion Trap: Rethinking Parody in Trademark Law. *Washington Law Review*, 88(3), pp. 1021-1102; Gerhardt, D. R. (2007). The 2006 Trademark Dilution Revision Act Rolls out Luxury Claim and Parody Exemption. *North Carolina Journal of Law and Technology*, 8(2), pp. 205-230.

[104] Registration authority for industrial property rights in the Czech Republic.

[105] Response of the Industrial Property Office of the Czech Republic of 3. 12. 2021, No. 2021/D21113596/11/ÚPV.

[106] *Česká pirátská strana v. LEGO Juris A/S* (2017) Czech Constitutional Court I. ÚS 2166/16.

[107] Piráti (2022) *Program České pirátské strany: Právní problémy duševního vlastnictví* [online]. Available from: `https://wiki.pirati.cz/kci/dusevko` [Accessed 11 November 2022]; to point out, the Czech Piracy Party program, among others, calls for cancelling the copyright law.

[108] *Česká pirátská strana v. LEGO Juris A/S* (2017) Czech Constitutional Court I. ÚS 2166/16.

[109] Ibid.

consumers would be confused about the support of the LEGO company to the Czech Piracy Party (which constantly fights against intellectual property rights in general). Furthermore, the video does not cause harm to the reputation or to the distinctive character of the "LEGO" trademark. It is also notable that the political advertisement is not so much commercial as a typical business advertisement since it is not aimed at economic gain. The author is of the view that in this case, the Constitutional Court might have considered the rights in question in greater depth, including whether and to what extent the LEGO company's rights had or might have been infringed.

5. LESSONS LEARNED FROM GERMANY

In Germany, the issue of trademark parody is repeatedly being discussed and there is currently a settled case law dealing with this issue. Due to the proximity of the legal systems, the findings of the German courts might be helpful for the assessment in the Czech Republic.

5.1. CASE LAW

In the very first case on this issue, the Federal Court of Justice (*Bundesgerichtshof*) ruled that the use of a well-known trademark in a humorous way to present a product can exclude the unfair advantage of distinctive character based on freedom of art.[110] The case was about the purple postcard "Muh", which used and allegedly infringed Milka's "Lila" colour trademark. The card was printed with a poem written by "Rainer Maria Milka" and the poem stated, "It is calm above the tree tops, somewhere a cow is bellowing. Moo!".[111]

The Court confirmed that a creative design is the essence of artistic activity, and since freedom of art protects artistic expression, the parody postcard falls within its scope of protection because of its humorous and satirical depiction of cows.[112] If it cannot be assumed that the parodic use is disparaging of the original trademark and that the parodist is pursuing exclusively commercial purposes, the protection of artistic freedom prevails over property rights.[113]

In the *eiPott* case[114], the German manufacturer sold egg cups under the name "eiPott". The Hamburg Court of Appeal (*Oberlandesgericht Hamburg*) held that the name was artificially created and that "pott" (*pot*) was not

[110] *Lila-Postkarte* (2005) Federal Court of Justice I ZR 159/02.
[111] Cf. Senftleben, M. Adapting EU Trademark Law to New Technologies - Back to Basics? In: Geiger, C. (ed.) *Constructing European Intellectual Property: Achievements and New Perspectives.* Cheltenham: Edward Elgar Publishing, p. 148.
[112] *Lila-Postkarte* (2005) Federal Court of Justice I ZR 159/02, paragraph 29.
[113] Op. cit., paragraph 35.
[114] *eiPott* (2010) Hamburg Appeal Court 5 W 84/2010.

commonly used for egg cups in Germany. Therefore, the public will not understand the term (in a descriptive way) and so it creates an indication as trademarks do. The pronunciation of "eiPott" is similar to Apple's "iPOD".[115] This similarity creates a humorous connotation between the two marks.

Based on the distinctiveness of the original trademark, the similarity of goods (the mark "iPOD" is designated also used for "appliances in the kitchen"), and the phonetical similarity, the court found the likelihood of confusion.[116] The court also noted that in some exceptional cases, the use of a reputed or well-known trademark for one's product could be justified under freedom of art (citing, e.g. *Lila-Postkarte* case).[117] However, as the Court has stated, in such a case, the mark must combine other elements which allude to the trademark owner. This "creative surplus" (*kreativer Überschuss*) will then overlap the reputation in the overall impression.[118] [119]

In the *Springender Pudel* (*Jumping Poodle*) case[120], the Federal Court of Justice held that the jumping poodle was a successful parody of the "PUMA" trademark, but that freedom of art could not take precedence over the property right.[121] The court concluded that the parodic trademark should not be registered because it benefits from the commercial and advertising efforts of "PUMA" and its existence would not be inconceivable without the existence of such a highly distinctive earlier trademark. In addition, "jumping poodle" could be protected by copyright law.[122] The difference from the *Lila-Postkarte* case is that "jumping poodle" was used for the same category of goods and sought to be protected as a registered trademark.[123]

In addition, the "jumping poodle" makes no comment or criticism of the original trademark. There is recognizable commercial interest in targeting consumers who are attracted by a humorous reference to the

[115] Op. cit., paragraphs 10 and 14.
[116] Op. cit., paragraph 15.
[117] Op. cit., paragraphs 22-23.
[118] Op. cit., paragraph 25.
[119] The case cited is very similar to *IbalGIN*. In both cases, the phonetic similarity is the only humorous message. Both marks borrow part of the original's design, in the case of the *eiPott* it was bitten egg, and in the case of the *IbalGIN* pink and blue color and font of the text. In neither case, there is any further reference or comment made to the original.
[120] *Springender Pudel* (2015) Federal Court of Justice I ZR 59/13; for the discussion of the case cf. e.g. Clark, B. (2015) *Dogged Pursuit of a trade mark parody: PUMA v PUDEL in the Bundesgerichtshof.* [blog entry] 21 April. The IPKat. Available from: `https://ipkitten.blogspot.com/2015/04/dogged-pursuit-of-trade-mark-parody.html` [Accessed 7 December 2023].
[121] *Springender Pudel* (2015) Federal Court of Justice I ZR 59/13, paragraphs 59-60.
[122] Ibid.
[123] Op. cit., paragraph 60.

well-known trademark, without which the business might not be successful. Therefore, freedom of expression cannot prevail over property rights.[124]

The Federal Patent Court took a similar view in the recent *British Hairways* case[125]. Based on the dissimilarity of services, the likelihood of confusion with the "British Airways" trademark was not found, however, the taking of unfair advantage was stated.[126] According to the Court, such a use of the original trademark constitutes a parody protected by freedom of art, nevertheless, it does not justify the unfair use of the former mark. Simultaneously, the latter mark does not make any comment or criticism of the original that could be considered as freedom of expression.[127] Therefore, the cancellation of the "British Hairways" trademark was ordered.[128]

5.2. OUTCOMES

As Pemsel pointed out, German case law provides the perspective that "it is easier to attack the registration of a parody successfully than the use of it", although the impact of use is more serious than that of registration.[129] In both, *Springender Pudel* and *British Hairways*, the owners of the original trademark sought to cancel the registration of a sign that took unfair advantage, but, the action did not seek to prohibit the unregistered use.

The overall outcomes of the cited case law might be described in the following overview.

1) A parodic trademark is protected under freedom of art/freedom of expression if

    a. it meets the definition of parody (creates an association in the mind of the consumer and is humorous/satirical; copyright assessment permissible);
    b. it makes a statement about the original trademark (adds something extra – comment, criticism, allusion) or society (i.e. provokes public debate) and
    c. it does not disparage the original trademark or is not solely for commercial gain.

[124] Op. cit., paragraphs 62-63.
[125] *British Hairways* (2022) Federal Patent Court of Germany 30 W (pat) 15/19.
[126] Ibid.
[127] Ibid.
[128] Ibid.
[129] Pemsel, M. (2023) *British Hairways did not take off – as a trade mark.* [blog entry] 4 July. The IPKat Available from: `https://ipkitten.blogspot.com/2023/07/british-hairways-did-not-take-off-as.html` [Accessed 28 November 2023].

2) A parodic trademark is not protected under freedom of art/freedom of expression if

   a. it meets the definition of parody (creates an association in the mind of the consumer and is humorous/satiric; copyright assessment admissible), but, at the same time,
   b. it does not make a statement about the original trademark or society (i.e. provokes public debate) and
   c. it disparages the original trademark or is solely for commercial gain and (takes unfair advantage of the distinctive character); and
   d. (applies for the registration)[130].

Since a parody must imitate the original, the assessment of the likelihood of confusion is not very useful for trademark parodies. On the other hand, the likelihood of association is sufficient to determine whether a parody is successful, i.e. whether it creates a link in the minds of the recipients. It seems clear that parody as a humorous expression will be considered during the assessment of dilution, particularly in the determination of unfair advantage. Furthermore, whether a parodic trademark makes a statement about the original trademark or society is the key element for the whole consideration. Playing with words and letters might be humorous, but if there is no further message, it would mostly be seen as a simple attempt to profit from the fun and the original trademark owner's expenses.

As Helfer and Austin point out, "defending an unlicensed use on parody grounds requires targeting the product or company identified by the mark rather than using the mark only to gain attention".[131] Luepke adds that if the parody or criticism is reasonable rather than disparaging, freedom of expression would prevail.[132]

The German scholars and experts concluded that the decision in trademark parody cases does not generally focus on the assessment

[130] The final requirement would not be questioned in every trademark parody case, however, as the German courts state, the trademark owner does not have to endure the registration of a parodic sign which might be protected under copyright, cf. *Springender Pudel* (2015) Federal Court of Justice I ZR 59/13, paragraph 60.

[131] Helfer, L., R. and Austin, G. W. (2011) *Human Rights and Intellectual Property: Mapping the Global Interface*, op. cit., p. 305.

[132] Luepke, M. H. H. (2008) Taking Unfair Advantage or Diluting a Famous Mark - a 20/20 Perspective on the Blurred Differences Between U.S. and E.U. Dilution Law. *Trademark Reporter*, 98(3), p. 818.

of trademark law, but rather depends more on the balancing of the fundamental rights at stake.[133]

6. IBALGIN – ILLUSTRATIVE TRADEMARK PARODY CASE

In the following section, the results of the German case law analysis will be applied and tested on the illustrative case from the Czech Republic.

As mentioned above, "IbalGIN" was a pink gin produced by the Fruko-Schulz company, which was sold in bottles with a design similar to the "Ibalgin" pain reliever of the SANOFI company. SANOFI owns numerous national trademark registrations, e.g. No. 347191[134]. The Fruko-Schulz company owns the national word mark registration "IBAL"[135], designated for class 33 (alcoholic beverages), and until 11 October 2023 owned EU RCD of the "IbalGIN" bottle label[136].

In the spring of 2022, the SANOFI company sued for a preliminary injunction consisting of an obligation to refrain from using the sign "IBALGIN" or any combination of the words "IBAL" and "GIN" put on the bottles of gin in "commercial dealings" and to withdraw the products from the market.[137] The Municipal Court in Prague upheld the application and ordered a preliminary measure.[138] The Court of Appeal reversed the decision and dismissed the application for a preliminary injunction.[139] The Court found that the conditions for a preliminary injunction were not satisfied, as there was no violation of "good morality of competition", the products and relevant markets were different, and the reputation of SANOFI's "Ibalgin" trademark had not been declared.[140] Moreover, invalidity procedures were initiated in 2023 for both the "IBAL" trademark and the RCD for the "IbalGIN" bottle label.

[133] Cf. Born, Ch. (2006) Zur Zulässigkeit einer humorvollen Markenparodie Anmerkung zum Urteil des BGH „Lila-Postkarte". *GRUR*, 59 (3), p. 194; see also Kefferpütz, M. and Wrage, A. (2015) Parodie und Marke: Ein ewiger Konflikt. *GRUR-Prax*, 7 (21), p. 453.

[134] Úřad průmyslového vlastnictví (2024) *Trademark registration No. 347191* [online]. Available from: `https://isdv.upv.gov.cz/webapp/webapp.irepgetsoub?pidr=NkLCXMUndGHKvtNbBCvC` [Accessed 6 April 2024].

[135] Úřad průmyslového vlastnictví (2024) *Trademark registration No. 348055* [online]. Available from: `https://isdv.upv.gov.cz/webapp/webapp.irepgetsoub?pidr=sjFQrICRrTFpIDzXUAsL` [Accessed 6 April 2024].

[136] EUIPO (2023) *Design No. 008180582-0001* [online]. Available from: `https://euipo.europa.eu/eSearch/\#details/designs/008180582-0001` [Accessed 18 November 2023].

[137] *SANOFI v. Fruko-Schulz* (2022) Municipal Court Prague 2 Nc 1027/2022 [not published].

[138] Ibid.

[139] *SANOFI v. Fruko-Schulz* (2022) High Court Prague 3 Cmo 36/2022 [not published].

[140] Op. cit., paragraph 7.

On 30 November 2023, the Municipal Court in Prague discontinued the proceedings because SANOFI had withdrawn the action.[141] The out-of-court settlement has been disputed[142] and so the Czech jurisprudence will have to await a decision on trademark parody. The results of the settlement are that the "IBAL" trademark in class 33 is designated to all alcoholic beverages, except gin, juniper, and drinks mixed with/of gin or consisting of juniper, and the RCD for the "IbalGIN" bottle label has been surrendered.

This situation itself proves that the SANOFI company did not enjoy the existence of "IbalGIN" and its associated intellectual property rights (national trademark and the RCD) and successfully negotiated its restriction. As a result, not only the registration of conflicting subject-matters but also their use of non-competing products was minimised, if not prohibited altogether. Notwithstanding this progress, the assessment for the case study might be useful, especially if the opportunity for a proper judicial statement on trademark parody was missed by the Czech court in this case.

6.1. PARODY DEFINITION TEST

As the CJEU stated, parody is an autonomous term of EU law. As there is no other definition of parody in Czech law, first, the characteristics provided by the CJEU shall be tested. In the German *Springender Pudel*[143] case, the court applied the CJEU's *Deckmyn* definition of parody on trademark parody. There is no relevant reason why the copyright legal definition should not be applied in the trademark law.

Firstly, most Czechs would associate "IbalGIN" with the "Ibalgin" medicine. Not only because of the text but also because of the design of the bottle label. The phonetic similarity as well as the similar colours encourages this finding. As such, "IbalGIN" evokes an original (already existing) "Ibalgin" trademark.

Secondly, "IbalGIN" may be seen as humorous. In this context, the humour may lie in the fact that, instead of taking painkillers, you would take alcohol, which could also relieve your pain. As Fruko-Schulz's director points out, "Originally it [the production of IbalGIN – author's note] was

[141] *SANOFI v. Fruko-Schulz* (2023) Municipal Court Prague 2 Cm 15/2022 [not published].

[142] The Financial Statement of Fruko-Schulz s. r. o. of 20 October 2023 [online]. Available from: `https://or.justice.cz/ias/ui/vypis-sl-detail?dokument=78994968\&subjektId=56910\&spis=415334` [Accessed 16 December 2023], paragraph 15 of the Auditor' report.

[143] *Springender Pudel* (2015) Federal Court of Justice I ZR 59/13, paragraph 59.

just a joke"[144]. However, there is no further criticism, caricature or satire in the "IbalGIN" sign.

The third factor is fulfilled when the later mark is noticeably different from the earlier mark. In this case, there is a difference in the categories of goods and in the composition (design) of products. The emphasis here is on the "gin" part of the later sign. Although the signs themselves are similar, the overall impression leaves no doubt as to the difference between the two products and the marks in question.

It can therefore be said that "IbalGIN" constitutes a parody of the "Ibalgin" trademark.

In the *Deckmyn* case, the CJEU also held that the interests of both parties should be balanced when determining parody, considering all relevant circumstances. In the present case, on the one hand, there is a pharmaceutical company with its painkiller medicine, which is one of the best-selling medicines in the Czech Republic.[145] In this sense, SANOFI certainly sought to protect its property interests in pharmaceutical sales and to preserve the reputation of "Ibalgin" trademark. On the other hand, there is a distillery and alcohol producer whose new product was deliberately named after the famous medicine.[146] Such an interest is undoubtedly commercial, aimed at increasing income by creating a humorous link with a reputed trademark.

According to the findings of the German courts in the *eiPott*[147], *Springender Pudle*[148] and *British Hairways*[149] cases, same as of the CJEU's *Polo/Lauren*[150] case, it might be concluded that "IbalGIN" has no comment or criticism and so there is a purely commercial interest based on benefiting from the reputation of "Ibalgin" trademark and its distinctive character. The registration of the "IBAL" trademark for alcoholic beverages in 2015 declares

[144] Bělský, M. (2021) IbalGin zaujal, při covidu jsme posílili ve východní Asii, říká šéf likérky [in press] Submitted to: *iDNES.cz*. Available from: `https://www.idnes.cz/ceske-budejovice/zpravy/nejedly-rum-fruko-schulz-jindrichuv-hradec-ibalgin.A210831_142304_budejovice-zpravy_pkr` [Accessed 9 October 2022]; author's own translation.

[145] Plíhalová, M. (2016) Zentiva v Praze vyrábí už 85 let. Češi jsou zvyklí na růžový Ibalgin, Francouzům stačí bílý. [in press] Submitted to: *Hospodářské noviny* Available from: `https://domaci.hn.cz/c1-65135800-zentiva-v-praze-vyrabi-uz-85-let-cesi-jsou-zvykli-na-ruzovy-ibalgin-francouzum-staci-bily` [Accessed 9 October 2022].

[146] Bělský, M. (2021) IbalGin zaujal, při covidu jsme posílili ve východní Asii, říká šéf likérky [in press] Submitted to: *iDNES.cz*. Available from: `https://www.idnes.cz/ceske-budejovice/zpravy/nejedly-rum-fruko-schulz-jindrichuv-hradec-ibalgin.A210831\_142304\_budejovice-zpravy\_pkr` [Accessed 9 October 2022].

[147] *eiPott* (2010) Hamburg Appeal Court 5 W 84/2010.

[148] *Springender Pudel* (2015) Federal Court of Justice I ZR 59/13.

[149] *British Hairways* (2022) Federal Patent Court of Germany 30 W (pat) 15/19.

[150] Judgment of 18 September 2014, The Polo/Lauren Company, LP v. OHIM, T-265/13, EU:T:2014:779.

the intention to produce "IbalGIN" as a long-term business plan. "IbalGIN" would probably not be protected by freedom of expression.

6.2. TRADEMARK INFRINGEMENT DETERMINATION

Even if "IbalGIN" is found to be a parody, it is necessary to examine the infringement of the trademark by dilution. First of all, it should be noted that the "Ibalgin" trademark is, from this author's point of view, a reputed trademark in the Czech Republic. It is likely to meet both the quantitative and qualitative thresholds for establishing reputation. "Ibalgin" is a medicine sold without a doctor's prescription and has been produced in the Czech Republic for decades. Almost every citizen of the Czech Republic has come across the "Ibalgin" trademark in search of pain relief.[151] Therefore, it can be concluded that "Ibalgin" is known by the relevant public in the Czech Republic.

The likelihood of a confusion test would not be very helpful in this case. Undoubtedly, there could be an association and link between the contested signs, however, there would be no confusion as to their sources, pharmaceutical company against distillery company. "IbalGIN" is not a product under SANOFI's original trademark. There is also no similarity between the categories of products.

The dilution test, which is covered by Sec. 8(2)(c) of the Czech Trademark Act, applies to the protection of reputed trademarks. The first requirement is to prevent unfair advantage from being taken of the distinctive character. According to the CJEU, this is riding "on the coat-tails" of the highly distinctive reputed trademark to "benefit from its power of attraction, its reputation and its prestige, and to exploit, without paying any financial compensation and without being required to make efforts of his own"[152], i.e. a purely commercial activity based on bearing the fruit of someone else's efforts.

The director of Fruko-Schulz explicitly admitted that "IbalGIN" "alludes to popular painkillers. Gin even has a typical pink colour which alludes to the pills."[153] The intention to ride on the coattails of the "Ibalgin's"

[151] Cf. e.g. Barochová, P. (2012) VIDEO: Jak vzniká růžová pilulka, kterou užívají miliony Čechů. [in press]. Submitted to: *iDNES.cz*. Available from: `https://www.idnes.cz/onadnes/zdravi/jak-se-vyrabi-ibalgin.A121112\_230900\_zdravi\_pet` [Accessed 7 December 2023].

[152] Judgement of 18 June 2009, L´Oreal SA v. Bellure NV, C-487/07, EU:C:2009:378, paragraph 49.

[153] Bělský, M. (2021) IbalGin zaujal, při covidu jsme posílili ve východní Asii, říká šéf likérky [in press] Submitted to: *iDNES.cz*. Available from: `https://www.idnes.cz/ceske-budejovice/zpravy/nejedly-rum-fruko-schulz-jindrichuv-hradec-ibalgin.A210831\_142304\_budejovice-zpravy\_pkr` [Accessed 9 October 2022]; author's own translation.

fame is clear from this statement. Consequently, the marketing effort was reduced to a minimum because there was no need to sell an ordinary pink gin. Therefore, on the basis of these findings, the use of "IbalGIN" could be considered to be an unfair advantage.

The second requirement concerns detriment to the distinctive character or the reputation of the earlier reputed mark. To prove a detriment to the distinctive character of the earlier mark it "requires evidence of a change in the economic behaviour of the average consumer of the goods or services for which the earlier mark was registered consequent on the use of the later mark or a serious likelihood that such a change will occur in the future."[154] Although Fruko-Schulz's sales have increased with the new "IbalGIN" product[155], this is a change in the economic behaviour of alcohol consumers, not (primarily) drug consumers. It cannot be assumed that consumers will start buying pink gin instead of pain relievers. Consequently, according to this finding, the simple use of the parodic sign "IbalGIN" should not be prohibited.

To summarize, "Ibalgin" is a trademark with a reputation in the Czech Republic. Although there is no public survey on the recognition of "Ibalgin", given its historical use in the Czech Republic, it can be assumed that it is recognized by a substantial part of the public in the Czech Republic. On the one hand, it is unlikely that the use of the reputed trademark "Ibalgin" would be found to be detrimental to its reputation. On the other hand, the use of "IbalGIN" would undoubtedly take unfair advantage of the distinctive character and reputation of "Ibalgin". There is clear evidence of an intention to create a new product and to attract consumers to buy it by riding on the coattails of "Ibalgin's" reputation. The registration of the "IBAL" word mark in 2015 supports the finding of a long-term business plan ("IbalGIN" was launched in 2020).

7. CONCLUSION

Parody is a form of humorous expression, generally protected by the freedom of expression granted in any democratic society. Its primary aim is to amuse recipients. Occasionally, the joke might be made at the expense of the rights

[154] Judgement of 27 November 2008, Intel Corporation Inc. v. CPM United Kingdom Ltd, C-252/07, EU:C:2008:655, paragraph 77.

[155] "I think people like it, which is proven by the sales statistics. I´m [*the director of Fruko-Schulz – author's note*] very happy with it and its popularity is also evident in many supermarket chains that take it from us in a bulk." Bělský, M. (2021) IbalGin zaujal, při covidu jsme posílili ve východní Asii, říká šéf likérky [in press] Submitted to: *iDNES.cz*. Available from: `https://www.idnes.cz/ceske-budejovice/zpravy/nejedly-rum-fruko-schulz-jindrichuv-hradec-ibalgin.A210831\_142304\_budejovice-zpravy\_pkr` [Accessed 9 October 2022]; author's own translation.

of others. Parody is specifically treated in intellectual property law, in copyright law, respectively, in the form of statutory exception to copyright. The law enables copyrighted works to be used for parody if the requirements of the three-step test are met. Trademark law, however, treats parody differently.

By combining the CJEU's general approaches to trademark infringement (concerning the likelihood of confusion and the determination of dilution) with the analysis of landmark trademark parody cases in Germany, the overall perspective for dealing with parodic signs was introduced and tested on the illustrative case from the Czech Republic.

Based on the above, it can be concluded that when a parodic trademark is created (and meets the basic characteristics of parody), the crucial elements in determining its legality are whether it makes some statement about the original trademark or adds some point to the public discussion and how much commercial interest, or benefit is associated with the parodic mark. If there is some kind of statement, the commercial benefit plays a lesser role in the decision and the possibility of protection by freedom of expression is more likely. On the other hand, if there is no such statement, the assessment would be interpreted as taking advantage of the distinctive character of the original trademark, as was already declared by the CJEU in the *Polo/Lauren* case.

Taking into account the preceding, it will be interesting to see how the CJEU deals with the issue of parody as a "due cause" for the non-consenting use of a trademark and the appreciation of freedom of expression in this matter.

From this author's point of view and the given perspective, the freedom of expression could be understood as "due cause". In the first place, it would depend on the assessment of the extent to which the expression is of public interest is socially relevant or opens a debate. Secondly, the extent to which the expression has a commercial character or purpose would play a decisive role. If the former is marginal, the latter would prevail and the non-consent use *in the course of trade* should be prohibited.

LIST OF REFERENCES

[1] *Act on Copyright and Rights Related to Copyright 2000*, No. 121/2000 Coll. The Czech Republic. Prague: Collection of Laws. In Czech.

[2] *Act on the Protection of Trade Marks and other Signs 1994*, MarkenG. The Federal Republic of Germany. Berlin: Federal Gazzete. In German.

[3] *Act on Trademarks and the Amendments to Act No. 6/2002 Coll. on Courts, Judges, Lay Judges and State Court Administration and on the Amendments*

to Certain Other Acts (Act on Courts and Judges) 2003, No. 441/2003 Coll. The Czech Republic. Prague: Collection of Laws. In Czech.

[4] AIPPI (2002) *Yearbook 2002/I* [online]. Available from: https://aippi.soutron.net/Portal/Default/en-GB/RecordView/Index/2995 [Accessed 8 January 2024].

[5] *Ashby Donald and others v. France* (2013). No. 36769/08, ECHR.

[6] Barochová, P. (2012) VIDEO: Jak vzniká růžová pilulka, kterou užívají miliony Čechů.[in press]. Submitted to: *iDNES.cz*. Available from: https://www.idnes.cz/onadnes/zdravi/jak-se-vyrabi-ibalgin.A121112\230900\zdravi\pet [Accessed 7 December 2023].

[7] Bartoň, M. and Hejč, D. (2021) Čl. 17 [Svoboda projevu a právo na informace]. In: Faisal Husseini et al. (eds). *Listina základní práv a svobod*. Praha: C. H. Beck, pp. 510-570.

[8] Bělský, M. (2021) IbalGin zaujal, při covidu jsme posílili ve východní Asii, říká šéf likérky [in press] Submitted to: *iDNES.cz*. Available from: https://www.idnes.cz/ceske-budejovice/zpravy/nejedly-rum-fruko-schulz-jindrichuv-hradec-ibalgin.A210831\142304\budejovice-zpravy\pkr [Accessed 9 October 2022].

[9] Born, Ch. (2006) Zur Zulässigkeit einer humorvollen Markenparodie Anmerkung zum Urteil des BGH „Lila-Postkarte". *GRUR*, 59 (3), pp. 192-195.

[10] *British Hairways* (2022) Federal Patent Court of Germany 30 W (pat) 15/19.

[11] *Česká pirátská strana v. LEGO Juris A/S* (2017) Czech Constitutional Court I. ÚS 2166/16.

[12] *ČEZ a. s. v. Greenpeace Česká republika, z.s.* (2020) Municipal Court Prague 32 C 2/2019 [not published].

[13] *ČEZ a. s. v. Greenpeace Česká republika, z.s.* (2020) Municipal Court Prague 32 C 7/2019 [not published].

[14] *ČEZ a. s. v. Greenpeace Česká republika, z.s.* (2020) Municipal Court Prague 32 C 1/2020 [not published].

[15] *ČEZ a. s. v. Greenpeace Česká republika, z.s.* (2022) High Court Prague 3 Co 54/2021 [not published].

[16] *ČEZ a. s. v. Greenpeace Česká republika, z.s.* (2022) High Court Prague 3 Co 55/2021 [not published].

[17] *ČEZ a. s. v. Greenpeace Česká republika, z.s.* (2022) High Court Prague 3 Co 56/2021 [not published].

[18] *ČEZ a. s. v. Greenpeace Česká republika, z.s.* (2023) Supreme Court 23 Cdo 2178/2022.

[19] *ČEZ a. s. v. Greenpeace Česká republika, z.s.* (2023) Supreme Court 23 Cdo 2403/2022.

[20] *ČEZ a. s. v. Greenpeace Česká republika, z.s.* (2023) Supreme Court 23 Cdo 2627/2022.

[21] *ČEZ a. s. v. Greenpeace Česká republika, z.s.* (2024) Constitutional Court I. ÚS 2956/23.

[22] *ČEZ a. s. v. Greenpeace Česká republika, z.s.* (2024) Constitutional Court I. ÚS 2957/23.

[23] *ČEZ a. s. v. Greenpeace Česká republika, z.s.* (2024) Constitutional Court IV. ÚS 2979/23.

[24] *Charter of Fundamental Rights and Freedoms 1993*, No. 2/1993 Coll. The Czech Republic. Prague: Collection of Laws. In Czech.

[25] *Charter of Fundamental Rights of the EU*, 18 December 2000 (2000/C 364/01). Available from: `https://www.europarl.europa.eu/charter/pdf/text\_en.pdf` [Accessed 27 November 2023].

[26] Charvát, R (2012). Ochranná známka s dobrým jménem dle práva Evropské unie a České republiky. *Právní rozhledy*, 20(22), pp. 781-789.

[27] Clark, B. (2015) *Dogged Pursuit of a trade mark parody: PUMA v PUDEL in the Bundesgerichtshof.*[blog entry] 21 April. The IPKat. Available from: `https://ipkitten.blogspot.com/2015/04/dogged-pursuit-of-trade-mark-parody.html` [Accessed 7 December 2023].

[28] *Cliffs Notes, Inc. v. Bantam Doubleday Dell Publishing Group, Inc.* (1989) United States Court of Appeals, Second Circuit, 886 F.2d 490.

[29] *Coca-Cola Company v. Gemini Rising* (1972) District Court for the Eastern District of New York, 346 F. Supp. 1183.

[30] Commission Proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No 6/2002 on Community designs and repealing Commission Regulation (EC) No 2246/2002. 28 November 2022. Available from `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:666:FIN` [Accessed 11 May 2024].

[31] *Convention for the Protection of Human Rights and Fundamental Freedoms*, 4 November 1950. Available from: https://www.echr.coe.int/documents/d/echr/convention\ENG [Accessed 27 November 2023].

[32] Dentith, S. (2000) *Parody*. London: Routledge.

[33] *Dermacour Laboratories s.r.o. v. Úřad průmyslového vlastnictví* (2018) Supreme Administrative Court 6 As 71/2018.

[34] Directive (EU) 2015/2436 of the European Parliament and of the Council of 16 December 2015 to approximate the laws of the Member States relating to trade marks. *Official Journal of the European Union* (L 336/1) 23 December 2015. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX\%3A32015L2436 [Accessed 7 October 2022].

[35] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society. *Official Journal of the European Union* (L 167) 22 June 2001. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex\%3A32001L0029 [Accessed 3 October 2022].

[36] *eiPott* (2010) Hamburg Appeal Court 5 W 84/2010.

[37] EUIPO (2023) *Design No. 008180582-0001* [online]. Available from: https://euipo.europa.eu/eSearch/\#details/designs/008180582-0001 [Accessed 18 November 2023].

[38] European Parliament resolution of 9 July 2015 on the implementation of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society. *Official Journal of the European Union* (C 265/121) 11 August 2017. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52015IP0273 [Accessed 3 October 2022].

[39] Fletcher, A. L. (2010). The Product with the Parody Trademark: What's Wrong with Chewy Vuiton. *The Trademark Reporter*, 100 (5), pp. 1091-1146.

[40] Geiger, Ch. and Izyumenko, E. (2014) Copyright on the Human Rights' Trial: Redefining the Boundaries of Exclusivity Through Freedom of Expression. *International Review of Intellectual Property and Competition Law*, 45 (3), pp. 316-342.

[41] Gerhardt, D. R. (2007). The 2006 Trademark Dilution Revision Act Rolls out Luxury Claim and Parody Exemption. *North Carolina Journal of Law and Technology*, 8(2), pp. 205-230.

[42] *Greenpeace v Esso* (2008) The French Court of Cassation No. 06-10961.

[43] Helfer, L., R. and Austin, G. W. (2011) *Human Rights and Intellectual Property: Mapping the Global Interface*. New York: Cambridge University Press.

[44] Hernandez, I. et al. (2020) *Comparative Advertising and Parodies: Treatment Through a Fair Use Approach Under Trademark and Copyright Law in Selected Jurisdictions* [online]. Available from: `https://www.inta.org/wp-content/uploads/public-files/advocacy/testimony-submissions/Comparative-Advertising-and-Parodies-Survey-4.20.20.pdf` [Accessed 3 October 2022].

[45] Judgement of 11 November 1997, Sabel v. PUMA, C-251/95, EU:C:1997:528.

[46] Judgement of 14 September 1999, General Motors Corporation v. Yplon SA, C-375/97, EU:C:1999:408.

[47] Judgement of 18 June 2009, L´Oreal SA v. Bellure NV, C-487/07, EU:C:2009:378.

[48] Judgement of 22 October 2020, Silver Plastics GmbH & Co. KG and Johannes Reifenhäuser Holding GmbH & Co. KG v. European Commission, C-702/19 P, EU:C:2020:857.

[49] Judgement of 27 November 2008, Intel Corporation Inc. v. CPM United Kingdom Ltd, C-252/07, EU:C:2008:655.

[50] Judgement of 3 September 2014, Johan Deckmyn, Vrijheidsfonds VZW v. Helena Vandersteen, C-201/13, EU:C:2014:2132.

[51] Judgment of 18 September 2014, The Polo/Lauren Company, LP v. OHIM, T-265/13, EU:T:2014:779.

[52] Judgment of 23 October 2003, Adidas-Salomon AG and Adidas Benelux BV v. Fitnessworld Trading Ltd., C-408/01, EU:C:2003:582.

[53] Kefferpütz, M. and Wrage, A. (2015) Parodie und Marke: Ein ewiger Konflikt. *GRUR-Prax*, 7 (21), pp. 451-453.

[54] Knedlo Zelo Wear (2024) *Main Page* [online]. Available from https://www.knedlozelowear.cz/ [Accessed 14 April 2024].

[55] Kosař, D. (2012) Čl. 10 [Svoboda projevu]. In: Jiří Kmec et al (eds.). *Evropská úmluva o lidských právech. Komentář*. Praha: C. H. Beck, pp. 993-1098.

[56] Koukal, P. (2019) *Autorské právo, public domain a lidská práva*. Brno: Masarykova univerzita.

[57] *Lila-Postkarte* (2005) Federal Court of Justice I ZR 159/02.

[58] *Louis Vuitton Malletier v. Haute Diggity Dog* (2007) Court of Appeals for the Fourth Circuit, 507 F.3d 252.

[59] Luepke, M. H. H. (2008) Taking Unfair Advantage or Diluting a Famous Mark - a 20/20 Perspective on the Blurred Differences Between U.S. and E.U. Dilution Law. *Trademark Reporter*, 98(3), pp. 789-833.

[60] Machnicka, A. A. (2016) Louis Vuitton does not laugh at its bags´ parody. *Journal of Intellectual Property Law & Practice*, 11 (5), pp. 324-326.

[61] Myers, G. (1996) Trademark Parody: Lessons from the Copyright Decision in Campbell v. Acuff-Rose. *Law and Contemporary Problems*, 59 (2), pp. 181-211.

[62] Myška, M. (2013), Ashby Donald v pirátské zátoce: svoboda projevu a vymáhání autorského práva v aktuální judikatuře ESLP. *Revue pro právo a technologie*, 4 (8), pp. 37-41. Available from: `https://journals.muni.cz/revue/article/view/5005` [Accessed 4 November 2023].

[63] *Neij and Kolmisoppi v. Sweden* (2013). No. 40397/12, ECHR.

[64] Nordemann, J. B. and Kraetzig, V. (2016) *The German Bundesgerichtshof changes its concept of parody following CJEU Deckmyn v. Vrijheidsfonds/ Vandersteen.* [blog entry] 3 November. Kluwer Copyright Blog. Available from: `http://copyrightblog.kluweriplaw.com/2016/11/03/the-german-bundesgerichtshof-changes-its-concept-of-parody-following-cjeu-deckmyn-v-vrijheidsfonds-vandersteen/` [Accessed 3 October 2022].

[65] OED (2023) *Oxford English Dictionary, s.v. "parody (n.2), sense 1.a,"* [online] Available from: `https://doi.org/10.1093/OED/4390633272` [Accessed 14 December 2023].

[66] OHIM the Boards of Appeal decision of 2 September 2015, case R 519/2015-4.

[67] OHIM the Boards of Appeal decision of 7 July 2015, case R 353/2015-5.

[68] Opinion of Advocate General Bobek, delivered on 2nd July 2019, case C-240/18 P, Constantin Film Produktion GmbH v European Union Intellectual Property Office (EUIPO). *European Court Reports*. Available from: `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62018CC0240` [Accessed 27 November 2023].

[69] Opinion of Advocate General Collins, delivered on 15th June 2023, case C-451/22, RTL Nederland BV, RTL Nieuws BV. *European Court Reports*. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62022CC0451 [Accessed 27 November 2023].

[70] Opinion of Advocate General Jacobs, delivered on 10th July 2003, case C-408/01, Adidas-Salomon AG and Adidas Benelux BV v. Fitnessworld Trading Ltd. *European Court Reports* (I-12537) 10 July 2003. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX\3A62001CC0408 [Accessed 7 October 2022].

[71] *Paris Convention for the Protection of Industrial Property*, 20 March 1883, as amended on 28 September 1979. Available from: https://www.wipo.int/wipolex/en/text/287556 [Accessed 7 December 2023].

[72] Parotta, N. and Lubberger, A. *INTA Attempts to File Amicus Brief with CJEU in Preliminary Ruling Case.* [online]. International Trademark Association. Available from: https://www.inta.org/news-and-press/inta-news/inta-attempts-to-file-amicus-brief-with-cjeu-in-preliminary-ruling-case-involving-ikea/ [Accessed 10 May 2024].

[73] Pemsel, M. (2023) *British Hairways did not take off – as a trade mark.* [blog entry] 4 July. The IPKat Available from: https://ipkitten.blogspot.com/2023/07/british-hairways-did-not-take-off-as.html [Accessed 28 November 2023].

[74] Peřinová, E. (2020) Komentář k § 7. In: Peřinová, E. et al. (eds). *Zákon o ochranných známkách: Praktický komentář*. Praha, Wolters Kluwer, pp. 37-72.

[75] Piráti (2022) *Program České pirátské strany: Právní problémy duševního vlastnictví* [online]. Available from: https://wiki.pirati.cz/kci/dusevko [Accessed 11 November 2022].

[76] Plíhalová, M. (2016) Zentiva v Praze vyrábí už 85 let. Češi jsou zvyklí na růžový Ibalgin, Francouzům stačí bílý. [in press] Submitted to: *Hospodářské noviny* Available from: https://domaci.hn.cz/c1-65135800-zentiva-v-praze-vyrabi-uz-85-let-cesi-jsou-zvykli-na-ruzovy-ibalgin-francouzum-staci-bily [Accessed 9 October 2022].

[77] Pontes, L. M. (2015) Trademark and Freedom of Speech: A comparison between the U.S. and the EU System in the Awakening of Johan Deckmyn v. Helena Vandersteen. In: *Ninth WIPO Advanced Intellectual Property Research Forum: Towards a Flexible Application of Intellectual*

Property Law - A Closer Look at Internal and External Balancing Tools, World Intellectual Property Organization, pp. 1-61.

[78] Ramalho, A. (2009). Parody in Trademarks and Copyright: Has Humour Gone Too Far. *Cambridge Student Law Review*, 5(1), 58-74.

[79] Regulation (EU) 2017/1001 of the European Parliament and of the Council of 14 June 2017 on the European Union trade mark. *Official Journal of the European Union* (L 154) 16 June. Available from: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32017R1001 [Accessed on 27 November 2023].

[80] Request for a preliminary ruling of 8 May 2023, C-298/23. *Official Journal of the European Union* (C-286/21) 4 August 2023. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62023CN0298 [Accessed 27 November 2023].

[81] Response of the Industrial Property Office of the Czech Republic of 3. 12. 2021, No. 2021/D21113596/11/ÚPV.

[82] Rosati, E. (2023) *What role for freedom of expression under EU trade mark law? An "IKEA-PLAN" prompts a CJEU referral.* [blog entry] 9 July. The IPKat. Available from: https://ipkitten.blogspot.com/2023/07/what-role-for-freedom-of-expression.html [Accessed 27 November 2023].

[83] *SANOFI v. Fruko-Schulz* (2022) High Court Prague 3 Cmo 36/2022 [not published].

[84] *SANOFI v. Fruko-Schulz* (2022) Municipal Court Prague 2 Nc 1027/2022 [not published].

[85] *SANOFI v. Fruko-Schulz* (2023) Municipal Court Prague 2 Cm 15/2022 [not published].

[86] Senftleben, M. Adapting EU Trademark Law to New Technologies - Back to Basics? In: Geiger, C. (ed.) *Constructing European Intellectual Property: Achievements and New Perspectives.* Cheltenham: Edward Elgar Publishing, pp. 137-176.

[87] Simon, D. A. (2013). The Confusion Trap: Rethinking Parody in Trademark Law. *Washington Law Review*, 88(3), pp. 1021-1102.

[88] Sitko, J. (2018) Parodia w kontekście naruszenia prawa do zarejestrowanego znaku towarowego (analiza prawnoporównawcza). In: Janusz Barta, Jakub Chwalba, Ryszard Markiewicz, Piotr Wasilewski (eds.) *Qui bene dubitat, bene sciet. Księga jubileuszowa dedykowana Profesor Ewie Nowińskiej*. Warsaw: Wolters Kluwer Polska, pp. 678-696.

[89] *Sousa Goucha v. Portugal* (2016). No. 70434/12, ECHR.

[90] *Springender Pudel* (2015) Federal Court of Justice I ZR 59/13.

[91] Telec, I. and Tůma, P. (2019) Komentář k § 38g. In: Ivo Telec, Pavel Tůma (eds.). *Autorský zákon: Komentář*. Praha: C. H. Beck, pp. 470-473.

[92] The Financial Statement of Fruko-Schulz s. r. o. of 20 October 2023 [online]. Available from: https://or.justice.cz/ias/ui/vypis-sl-detail?dokument=78994968&subjektId=56910&spis=415334 [Accessed 16 December 2023].

[93] Úřad průmyslového vlastnictví (2022) *Trademark registration No. 476663* [online]. Available from: https://isdv.upv.cz/obr/ozvyprej/663/O-476663.pdf [Accessed 1 October 2022].

[94] Úřad průmyslového vlastnictví (2024) *Trademark registration No. 347191* [online]. Available from: https://isdv.upv.gov.cz/webapp/webapp.irepgetsoub?pidr=NkLCXMUndGHKvtNbBCvC [Accessed 6 April 2024].

[95] Úřad průmyslového vlastnictví (2024) *Trademark registration No. 348055* [online]. Available from: https://isdv.upv.gov.cz/webapp/webapp.irepgetsoub?pidr=sjFQrICRrTFpIDzXUAsL [Accessed 6 April 2024].

[96] Żelechowski, Ł. (2018) Invoking freedom of expression and freedom of competition in trade mark infringement disputes: legal mechanisms for striking a balance. *ERA Forum*, 19, pp. 115-135. Available from: https://link.springer.com/article/10.1007/s12027-018-0498-3 [Accessed 13 April 2024].

DOI 10.5817/MUJLT2024-1-3

THE "OBJECTIVE TEST" AND THE DOWNSTREAM MARKET PRESENCE REQUIREMENT IN BIG DATA ACCESS CASES UNDER THE ESSENTIAL FACILITIES DOCTRINE - A CRITICAL ASSESSMENT

by

ROK DACAR *

One possible way to gain access to competitively relevant sets of Big Data is to apply the essential facilities doctrine. However, the European Commission and the European Court of Justice have established several different criteria for applying the doctrine. Since neither institution has yet applied the doctrine in Big Data access cases, it is not clear which of the criteria applies in such positions. This paper attempts to analyze the impact of the "objective test" and the requirement that the controlling company be active in the downstream market (which are included in all assessment criteria) in Big Data access cases, with the goal of answering the research question, "Do the application of the "objective test" and the requirement that the controlling company be active in the downstream market impede the effectiveness of the doctrine in Big Data access cases under EU competition law, and if so, how should they be changed?" The conclusion is that in Big Data access cases, the "objective test" should be mitigated and replaced by the "subjective test" or the "average company test" and the requirement that the controlling company be active in the downstream market should be discarded altogether in order for the doctrine to be an effective tool for accessing competitively relevant sets of Big Data.

KEY WORDS

The Essential Facilities Doctrine, Big Data, Mandated Data Access, Bronner Ruling

* Teaching assistant and doctoral student at the Faculty of Law of the University of Maribor, Slovenia; e-mail: rok.dacar@um.si.

1. INTRODUCTION AND STRUCTURE OF THE PAPER

Big Data, also called the "new oil"[1] is undoubtedly one of the most economically important resources of the modern age, which companies can use to offer new and innovative products in countless markets. Even traditional (brick-and-mortar) industries (such as construction, automotive, and banking) are being heavily influenced by Big Data which is used to improve the products they offer.[2][3]

At the same time, Big Data and Big Data-driven markets pose unprecedented challenges to competition policy and law, as traditional competition law tools are not tailored to the specifics of Big Data-driven markets[4] The purpose of this paper is to shed light on the possibilities of applying the essential facilities doctrine (henceforth: the doctrine), an institute of competition law that allows a company to demand access to a product controlled by another (dominant) company under particularly restrictive conditions, to Big Data. It will do so by examining whether the conditions developed in the Court's[5] jurisprudence for the application of the doctrine in European union (henceforth: EU) competition law, can address the specificities of Big Data and Big Data-driven markets. No single set of criteria for the use of the doctrine has emerged, as the precise conditions

---

1 The Economist. (2017) *The World's Most Valuable Resource Is No Longer Oil, But Data*. [online] London: The Economist. Available from: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data [Accessed 12 April 2023].

2 In the interest of greater clarity of the text, the term "product" is used to refer to both products and services.

In the automotive industry, for example, Big Data is being used to improve vehicle safety, maintenance, and customer experience by analyzing sensor data from vehicles and customer feedback in real time. By collecting and analyzing data from these sensors in real time, manufacturers can identify patterns and trends related to accidents and near misses. For example, if incidents of abrupt braking are consistently reported for a particular model, the manufacturer can investigate and address potential safety issues such as faulty brakes.

3 For more see: Minevick, M. (2020) *The Automotive Industry and the Data Driven Approach.* [online] 13 July. Jersey City: Forbes. Available from: https://www.forbes.com/sites/markminevich/2020/07/13/the-automotive-industry-and-the-data-driven-approach/?sh=84cfedcf9a53 [Accessed 8 September 2023].

4 A notable and much discussed example is the difficulty of defining a market (which is the first step in abuse of dominance cases) when the relevant products have no monetary price. This is rarely the case in "brick and mortar" markets, but is common in Big Data-driven markets, where the phenomenon of "two-sided markets" is common. In these cases, the SSNIP test, which defines markets based on the impact of a hypothetical small but significant and non-transitory price increase on consumer demand, cannot be applied. For a more in-depth discussion see: Mandrescu, D. (2018) The SSNIP Test and Zero-Price Strategies.*European Competition and Regulatory Law Review*, 2(4), pp. 244-260.

5 The term Court is used as a generic term for the Court of Justice of the European Communities, the Court of Justice of the European Union, and the General Court of the European Union, unless otherwise indicated.

for its application depend on the type of facility requested. However, an analysis of prior cases involving essential facilities suggests three distinct lines of reasoning: the Bronner criteria, applicable to tangible facilities and services; the IMS Health criteria, applicable to facilities protected by intellectual property rights (henceforth: IPRs); and the Microsoft criteria (a milder version of the IMS Health criteria), the precise scope of which remains unknown in the absence of subsequent case law. It is beyond the scope of this paper to explore which of the above criteria are best suited for application to Big Data or, rather, whether an entirely new set of criteria should be developed.

However, this paper explores two conditions that are common to all of the above criteria, namely the "objective test" and the requirement that the controlling (dominant) company[6]be active in the downstream market (henceforth: downstream market presence requirement). It does so with the aim of answering the research question: "Do the application of the "objective test" and the requirement that the controlling company be active in the downstream market impede the effectiveness of the doctrine in Big Data access cases under EU competition law, and if so, how should they be modified so as to make the doctrine an effective tool for accessing sets of Big Data".

The impact of Big Data on competition policy and law is the subject of a number of theoretical contributions[7] while the position of Big Data as

[6] The paper uses the term "controlling company" to refer to the company controlling the (alleged) essential facility.

[7] Crémer, J., de Montjoye, Y. A. in Schweitzer, H. (2019) *Competition Policy for the Digital Era*, Luxembourg: Publications Office of the European Union; Hayashi, S. and Arai, K. (2019) How Competition Law Should React in the Age of Big Data and Artificial Intelligence. *The Antitrust Bulletin*, 64 (3), pp. 447-456; Kadar, M. and Bogdan, M. (2017) 'Big Data' and EU Merger Control - a Case Review. *Journal of European Competition Law and Practice*, 8 (8), pp. 479-491; Katz, M. L. (2019) Multisided Platforms, Big Data, and a Little Antitrust Policy. *Review of Industrial Organization*, 54, pp. 695-716; Kupčik, J. and Mikeš, S. (2018) Discussion on Big Data, Online Advertising and Competition Policy. *European Competition Law Review*, 39 (9), pp. 393-402; Lasserre, B. and Mundt, A. (2017) Competition Law and Big Data: The Enforcers View. *Rivista Italiana di Antitrust*, (1), pp. 87-103; Lugard, P. and Roach, L. (2017) The Era of Big Data and the EU/U.S. Divergence for Refusals to Deal. *Antitrust*, 31 (2), pp. 58-64; Modrall, J. (2018) Big Data and Merger Control in the EU. *Journal of European Competition Law & Practice*, 9 (9), pp. 569-578; Pfeiffer, R. A. C. (2019) Digital Economy, Big Data and Competition Law. *Market and Competition Law Review*, 3 (1), pp. 53-89; Qi, J. (2020) Application of Essential Facilities Doctrine to "Big Data": US and EU Perspectives. *European Competition Law Review*, 40(4), pp. 182-189; Ryan, D. (2021) Big Data and the Essential Facilities Doctrine: A Law and Economics Approach to Fostering Competition and Innovation in Creative Industries. *UCL Journal of Law and Jurisprudence*, 10 (1), pp. 84-112; Sivinski, G., Okuliar, A. and Kjolbye, L. (2017) Is Big Data a Big Deal? A Competition Law Approach to Big Data. *European Competition Journal*, 13 (2/3), pp. 199-227

an essential facility is discussed in only a handful of articles.[8] However, these do not discuss the issues addressed in this paper, but rather provide a more general overview of the possibilities of applying the doctrine to sets of Big Data, focusing mostly on the transatlantic comparative aspect. This paper is therefore novel in that it offers an analysis of aspects of the doctrine's application that have not yet been the subject of scholarly debate. The paper is divided into three main parts. The first part highlights the institutes and concepts necessary for its understanding. It analyses the concept of the doctrine and the relevant case law of the Court and explains that no uniform criteria have been developed in EU competition law for assessing the character of a facility as essential under the doctrine. In addition, this part of the paper attempts to define the basic characteristics of Big Data and to present the current position of Big Data as an essential facility. The second part of the paper analyses the possibilities of applying two conditions common to all sets of criteria for assessing the potentially essential character of a facility under the doctrine, namely the "objective test" and the downstream market presence requirement. It concludes that both of these conditions severely limit the applicability of the doctrine to Big Data-driven markets. In addition, it suggests replacing the "objective test" with a "subjective test" or the "average company test" and removing the downstream market presence requirement in Big Data access cases to increase the doctrine's effectiveness. The third and final part of the paper summarizes its findings.

2. SETTING THE SCENE

2.1. THE ESSENTIAL FACILITIES DOCTRINE

In competition law, the doctrine is an idea that "the owner of a facility which is not replicable by the ordinary process of innovation and investment, and without access to which competition on a market is impossible or seriously impeded has to share it with a rival."[9]Essential facility cases typically involve two vertically related markets, where the product from the upstream market is an essential input for the activity on the downstream market, i.e. the activity in the downstream market is impossible without access to the product

[8] Colangelo G. and Maggiolino M. (2017) Big Data as Misleading Facilities. *European Competition Journa*l, 13 (2/3), pp. 249-281; Lugard, P. and Roach, L. (2017) The Era of Big Data and the EU/U.S. Divergence for Refusals to Deal. Antitrust, 31 (2), pp. 58-64; Qi, J. (2020) Application of Essential Facilities Doctrine to "Big Data": US and EU Perspectives. *European Competition Law Review*, 40(4), pp. 182-189.

[9] Craig, P. and de Burca, G. (2015) EU Law: Text, Cases, and Materials. 6th ed. Oxford: Oxford University Press, p.p. 1074.

from the upstream market.[10]In Commercial Solvents,[11]the upstream market was the market for the chemical aminobutanol, which is an essential input for the activity on the market for the chemical ethambutol (downstream market), since the latter cannot be produced without aminobutanol. In the Bronner case, the market for the delivery of daily newspapers in Austria was the upstream market, while the market for daily newspapers in Austria was the downstream market. If the company that denies access to the essential input is dominant in the upstream market and the refusal to supply is abusive,[12]the company that has been denied access to the input in question can demand (mandatory) access to it by invoking the doctrine.[13]

The doctrine has both ardent supporters and passionate opponents. Some argue that it allows smaller companies access to essential inputs they could not otherwise obtain, which increases the intensity of competition in the (downstream) market and thus the level of consumer welfare due to the higher quality and lower prices of products.[14] However, more critical voices[15]claim that the possibility of mandated access reduces incentives to invest in the development and/or improvement of (potentially) essential facilities in two ways. First, companies with dominant market positions (on upstream markets) will reduce their investment in existing and new essential facilities because of the threat of mandated access,[16]and second,

[10] See e.g. Judgement of 6 March 1974, Istituto Chemioterapico Italiano S.p.A. and Commercial Solvents Corporation v Commission, C-6/73, EU:C:1974:18, that concerned the refusal to supply the chemical aminobutanol, which is essential for the production of the chemical ethambutol.

[11] Judgement of 6 March 1974, Istituto Chemioterapico Italiano S.p.A. and Commercial Solvents Corporation v Commission, C-6/73, EU:C:1974:18.

[12] Refusal to supply an essential input is a form of abuse of market dominance, therefore, if the company refusing access to an essential input does not have a dominant market position on the relevant product market (upstream market), the doctrine cannot be invoked.

[13] This article presents only the mere basics on the doctrine. For a more in-depth analysis see: Eilmansberger, T. (2005) The Essential Facilities Doctrine Under Art. 82: What is the State of Affairs After IMS Health and Microsoft. *King's Law Journal*, 16 (2), pp. 329-346; Hohmann, H. (2001) *Die essential Facility Doctrine im Recht der Wettbewerbsbeschränkungen*. Baden-Baden: Nomos; Muller, U. and Rodenhausen, A. (2008) The Rise and Fall of the Essential Facility Doctrine. *European Competition Law Review*, 29(5), pp. 310-329; Seelen, C. M. (1997) The Essential Facilities Doctrine: What Does it Mean to be Essential. *Marquette Law Review*, 80 (4), pp. 1117-1134.

[14] E.g.: Hatzopoulos, V. (2006) *The EU Essential Facilities Doctrine*. Bruges: College of Europe.

[15] Some of them being: Areeda, P. (1989) Essential Facilities: an Epithet in need of Limiting Principles. *Antitrust Law Journal*, 58 (3), pp. 841-853; Gerber, D. J. (1988) Rethinking the Monopolist's Duty to Deal: a Legal and Economic Critique of "Essential Facilities". *Virginia Law Review*, 74 (6), pp. 1069-1113.

[16] Also see: Opinion of AG Jacobs of 28 May 1998, Oscar Bronner GmbH & Co. KG v Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co. KG, Mediaprint Zeitungsvertriebsgesellschaft mbH & Co. KG and Mediaprint Anzeigengesellschaft mbH & Co. KG, EU:C:1998:264, paragraph 57. In his seminal opinion AG Jacobs clearly gave priority to competition for the market over competition in the market.

companies that need the essential facilities to enter downstream markets will refrain from developing competing facilities (substitutes) because it is cheaper for them to "free-ride" on existing facilities. Herbert Hovenkamp, one of the doctrine's harshest critics, even pointed out that it is "one of the most problematic, incoherent and uncontrollable institutes of competition Law, without which, the world would be a better place."[17]

Despite the theoretical and practical controversy over the doctrine, both the European Commission (henceforth: the Commission) and the Court have frequently applied it, especially from the late 1980s to the beginning of the second millennium. However, despite the abundance of relevant case law, no universal criteria for the application of the doctrine developed. As a result, the requirements for its use vary from case to case and from essential facility to essential facility.

A careful analysis of the relevant case law, however, reveals several different sets of criteria for applying the doctrine. The criteria developed in the Bronner ruling[18] are considered the gold standard upon which most essential facility cases rely, although they have been fully applied in only three cases.[19]In general, the Bronner criteria[20] are applicable in cases where the alleged essential facility is either a materialized facility (such as a railroad or a local loop) or a non-digital service, as implicitly recognized in the recent Slovak Telekom[21] and Lietuvos geležinkeliai[22] cases.Both rulings state that the Bronner criteria are not applicable in the cases at hand, as a duty to grant access to the facilities in question (a local loop in Slovak Telekom and a railway in Lietuvos geležinkeliai) already exists on the basis of (ex-ante)

[17] Hovenkamp, H. (2011) *Federal Antitrust Policy, the Law of Competition and its Practice*. 4th ed. St. Paul: West, p. 336.

[18] Judgement of 26 November 1998, Oscar Bronner GmbH & Co. KG v Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co. KG, Mediaprint Zeitungsvertriebsgesellschaft mbH & Co. KG and Mediaprint Anzeigengesellschaft GmbH & Co. KG, C-7/97, EU:C:1998:569.

[19] Besides the Bronner case also in: Judgement of 9 September 2009, Clearstream Banking AG and Clearstream International SA v Commission of the European Communities, T-301/04, EU:T:2009:317; Commission Decision of 27 August 2003 relating to a proceeding pursuant to Article 82 of the EC Treaty of (COMP/37.685 GVG/FS). Official Journal of the European Union (2003/C-3057). 27th August. Available from: https://eur-lex.europa.eu/legal_content/EN/TXT/PDF/?uri=CELEX:32004D0033&qid=1681140533022&from=en [Accessed 10 April 2023].

[20] These conditions are: i.) The refusal to supply will eliminate all competition in the downstream market, ii.) there are no objective justifications for the refusal to supply, iii.) the facility is indispensable for competition in the downstream market as there are no actual or potential substitutes for it.

[21] Judgement of 25 March 2021, Slovak Telekom v Commission, C-165/19 P, EU:C:2021:239.

[22] Judgement of 12 January 2023, Lietuvos geležinkeliai v Commission, C-42/21 P, EU:C:2023:12.

sector regulation. If such regulation does not exist one can presume, ad contrario, that the Bronner criteria are applicable.[23]

Importantly, the Bronner ruling introduced the "objective test", according to which the economic unviability of the creation of a substitute by the demanding company[24] is not relevant, since the duplication of the facility must be economically unviable for a company with a comparable market position to the controlling company.[25] In other words, the economic weakness of the demanding company compared to the controlling company is in no way relevant for the doctrine's application.[26] The second set of criteria applies to cases where the allegedly essential facility is protected by IPRs, in particular patents and copyrights.[27] In such a case, access to the IPR-protected facility (usually its licensing) is necessary for the activity on the downstream market. For example, in the Magill case,[28] access to the (copyrighted) television programs of the individual television stations in Ireland was necessary for the creation of a consolidated program of all television stations in Ireland (in other words, an essential input), while in the IMS Health case,[29] activity in the market for the supply of regional sales data for pharmaceutical products in Germany was impossible without access to the 1860 brick structure formatting. Thus, the alleged essential facility is not the IPR as such, but the facility it protects.

---

[23] For more see: Czapracka, K. (2021) The Essential Facilities Doctrine and the Bronner Judgment Clarified, Case C-165/19 P Slovak Telekom v Commission. *Journal of European Competition Law & Practice*, 13 (4), pp. 278-280.

[24] The paper uses the term "demanding company" to refer to the company demanding access to the (alleged) essential facility.

[25] Judgement of 26 November 1998, Oscar Bronner GmbH & Co. KG v Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co. KG, Mediaprint Zeitungsvertriebsgesellschaft GmbH & Co. KG and Mediaprint Anzeigengesellschaft mbH & Co. KG, C-7/97, ECLI:EU:C:1998:569, paragraphs 44-46.

[26] This clearly shows that the doctrine does not protect individual companies but rather market competition as an institution.

[27] Despite this, the broader term "intellectual property conditions" is widely used in literature. See: Chen, Y. (2014). Refusal to Deal, Intellectual Property Rights, and Antitrust. *The Journal of Law, Economics, and Organization*, 30 (3), pp. 533-557; Cotter, T. F. (1999). Intellectual Property and the Essential Facilities Doctrine. *Antitrust Bulletin*, 44 (1), pp. 211-250; Ginsburg, D., Garadin, D. and Klovers, K. (2019) Antitrust and Intellectual Property in the United States and the European Union. In: Muscolo, G. and Tavassi, M. A. (eds.) *The Interplay between Competition Law and Intellectual Property: An International Perspective*. Alpen aan den Rijn: Kluwer Law International, pp. 99-120; Graef I (2011) Tailoring the Essential Facilities Doctrine to the IT sector: Compulsory Licensing of Intellectual Property Rights after Microsoft. *Cambridge Student Law Review*, 7 (1), pp. 1-20.

[28] Judgment of the Court of 6 April 1995, Radio Telefis Eireann (RTE) and Independent Television Publications Ltd (ITP) v Commission of the European Communities, joined cases C-241/91 P and C-242/91 P, EU:C:1995:98. Judgement of 29 April 2004, IMS Health GmbH & Co. OHG v NDC Health GmbH & Co. KG, C-418/01, EU:C:2004:257.

[29] Judgement of 29 April 2004, IMS Health GmbH & Co. OHG v NDC Health GmbH & Co. KG, C-418/01, EU:C:2004:257.

Although the Court first recognized the potential character of IPRs as essential facilities in the 1988 Renault[30] and Volvo[31] rulings, systematic criteria for applying the doctrine in IPR cases were first established in the Magill judgement. These were further elaborated in the 2004 IMS Health ruling,[32] which was also heavily influenced by the Ladbroke judgement.[33] The latter, importantly, introduced the requirement that the controlling company must be present in the downstream market,[34] which has not been surpassed by subsequent case law and thus still applies. The IPR criteria are even stricter than the (already strict) Bronner criteria, as the "new product" condition was added.[35] Accordingly, the doctrine can only be used if the denial to licence IPRs prevents the emergence of a new product for which there is at least potential consumer demand.[36] After the IMS Health ruling, the conditions for the application of the doctrine were relatively clear, with the Bronner criteria applicable in cases involving materialized facilities and services and the IMS Health criteria applicable in IPR cases. However, this dichotomy was turned on its head by the General Court's 2007 Microsoft ruling,[37] which concerned Microsoft's refusal to grant access to interoperability protocols that were protected by IPRs. Therein, the General Court replaced the "new product" condition with the "technical progress" condition. Thus, it was no longer necessary to prove that the refusal to licence IPRs hindered the emergence of a new product as it sufficed that it impeded technical progress. In my opinion the term "technical progress" is semantically ambiguous, as it can range from minimal improvements of the product to significant technical advances that already meet the "new product" condition. Moreover, it was no longer necessary to prove that the refusal to licence will eliminate all competition in the downstream market

[30] Judgement of 5 October 1988, Consorzio Italiano della Componentistica di Ricambio per Autoveiculi and Maxicar v Régie des Usines Renault, C-53/87, EU:C:1988:472.

[31] Judgement of 5 October 1988, AB Volvo v Erik Veng (UK) Ltd, C-238/87, EU:C:1988:477.

[32] Judgement of 29 April 2004, IMS Health GmbH & Co. OHG v NDC Health GmbH & Co. KG, C-418/01, EU:C:2004:257.

[33] Judgement of 11 November 1997, Commission of the European Communities and French Republic v Ladbroke Racing Ltd., C-359/95 P, EU:C:1997:531.

[34] Rinaldi, A. (2020) Re-Imagining the Abuse of Economic Dependence in a Digital World. *European Competition Law Review*, 4 (2), pp. 253-256, p. 254.

[35] Van den Bergh and Camesasca argue that milder conditions would have a negative impact on dynamic efficiency. See: van den Bergh, R. and Camesca, P. D. (2006) *European Competition Law and Economics: A Comparative Perspectiv*e. 2nd ed. London: Sweet & Maxwell, p. 280.

[36] Judgement of 29 April 2004, IMS Health GmbH & Co. OHG v NDC Health GmbH & Co. KG, C-418/01, EU:C:2004:257, paragraph 39 states that for the doctrine to be applied "three cumulative conditions must be satisfied, namely, that that refusal is preventing the emergence of a new product for which there is a potential consumer demand, that it is unjustified and such as to exclude any competition on a secondary market."

[37] Judgement of 27 June 2012, Microsoft Corp. v European Commission, T-167/08, EU:T:2012:323.

but only that it will eliminate all effective competition in it. Due to the very specific factual situation, the mitigation of the "traditional" IPR criteria (IMS Health criteria) was necessary for the application of the doctrine,[38] but in the absence of subsequent case law, the exact scope of the Microsoft criteria remains unclear. It is therefore unsettled whether they were tailored to the present case or whether their applicability is broader or even general.

2.2. BIG DATA AS ESSENTIAL FACILITIES

Despite the importance of Big Data for today's economy (also called economy or even society 4.0.), there is no unified definition of what exactly Big Data is and how it differs from "ordinary" data. However, all definitions of Big Data agree on several characteristics that distinguish Big Data from "ordinary" data, namely the huge volume of data contained in a set of Big Data,[39] the high velocity at which new data is collected and processed, and the wide variety of data in a set of Big Data.[40] This paper adopts the Commission's definition of Big Data, as "large amounts of different types of data produced with high velocity from a high number of various types of sources, whose handling requires new tools and methods, such as powerful processors, software and algorithms."[41]

---

[38] A more in-depth analysis of the Microsoft case can be, inter alia, found in: Andreangeli, A. (2009) Interoperability as an "Essential Facility" in the Microsoft Case: Encouraging Stifling Competition or Innovation? European Law Review, 4, pp. 584-611; Butts, C. (2010) The Microsoft Case 10 Years Later: Antitrust and New Leading "New Economy" Firms. *Northwestern Journal of Technology and Intellectual Property*, 8 (2), pp. 275-291; Eilmansberger (2005) op. cit., pp. 329-346.

[39] It is important to distinguish between Big Data and a set of Big Data, which are related but at the same time distinct concepts. While both terms refer to large amounts of structured and unstructured data from a large number of different sources that is being gathered at a quick rate, a set of Big Data is a subset of the larger universe of Big Data. A set of Big Data can be used for multiple purposes, including machine learning, analytics, artificial intelligence creation, and decision making. A set of Big Data is created for a specific business purpose and is typically more concentrated and smaller than Big Data.

[40] For other definitions of Big Data also see: de Hert, P. and Sajfert, J. (2019) Regulating Data in and out of the Data Protection Policy Field: two Scenarios of post-GDPR Law-Making and the Actor Perspective. *European Data Protection Law Review*, 5 (3), pp. 338-351, p. 338; van Schendel, S. and van der Sloot, B. (2016) Ten Questions for Future Regulation of Big Data: a Comparative and Empirical Legal Study. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 7 (2), pp. 110-145, p. 113.

[41] European Commission. (2014) Communication from the Commission of 2 July 2014: Towards a thriving data-driven economy. COM/2014/0442. p. 4. Available from: `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex\%\3A52014DC0442`[Accessed 11 April 2015].

Although the Commission had the opportunity to do so in the Facebook/WhatsApp,[42] Google/DoubleClick,[43] and Telefónica UK/Vodafone UK/ Everything Everywhere[44] decisions, it avoided taking a clear position on whether Big Data can be an essential facility.

It should be noted, however, that these decisions involved mergers and were not, in themselves, essential facility cases. They did, however, provide an opportunity for the Commission to clarify in an obiter dictum whether a set of Big Data could be an essential facility, which the Commission did not do. In my view, this was the case because Big Data was still a relatively new concept at the time of the decisions, relating to huge and complex data sets rather than tangible facilities, services, or IPRs, and therefore did not fit within the concept of essential facilities. Moreover, at the time the decisions were published, the debate about the relevance of Big Data for competition law and policy was only beginning to develop, reaching its peak at the end of the second decade of the new millennium.[45] Later on, however, with some provisions of the proposal for the Digital Markets Act, [46] which remaining unchanged in the adopted version, [47] the Commission has acknowledged that a set of Big Data can constitute an essential facility. Moreover, the fact that Big Data can be an essential facility is explicitly recognized in the German Act against Restraints of Competition (Gesetz gegen Wettbewerbsbeschränkungen) following its (recent) tenth amendment.[48] A similar conclusion can be drawn from the rulings in the hiQ

[42] Commission Decision of 3 October 2014 declaring a concentration to be compatible with the common market (Facebook/WhatsApp), *Official Journal of the European Union* (COMP/M.7217) 3 October. Available from: `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX\%\3A32014M7217` [Accessed 12 April 2023].

[43] Commission Decision of 11 March 2008 declaring a concentration to be compatible with the common market and the functioning of the EEA Agreement (Google/DoubleClick), *Official Journal of the European Union* (COMP/M.4731) 11 March. Available from:`https://ec.europa.eu/competition/mergers/cases/decisions/m4731_20080311_20682_en.pdf` [Accessed 12 April 2023].

[44] Commission Decision of 4 September 2012 declaring a concentration to be compatible with the internal market and the functioning of the EEA Agreement (Telefónica UK/ Vodafone UK/ Everything Everywhere/ JV), *Official Journal of the European Union* (COMP/M.6314) 4 September. Available from: `https://ec.europa.eu/competition/mergers/cases/decisions/m6314_20120904_20682_2898627_EN.pdf` [Accessed 12 April 2023].

[45] See inter alia: footnote 10.

[46] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828. *Official Journal of the European Union* (OJ L 265) 12 October. Available from: `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX\%\3A32022R1925` [Accessed 13 April 2023].

[47] Ibid, paragraphs 9 and 10 of article 5 and paragraphs 10 and 11 of article 6. Moreover, see recital 3.

[48] Gesetz gegen Wettbewerbsbeschränkungen in der Fassung der Bekanntmachung vom 26. Juni 2013 (BGBl. I S.1750, 3245), das zuletzt durch Artikel 4 des Gesetzes vom 20. Mai 2022

Labs [49] and PeopleBrowsr cases[50] in the United States of America, where sets of Big Data were an essential facility for operating in downstream markets.[51] Thus, there is no question that Big Data can be an essential facility. However, it remains unclear which of the existing criteria should be used to assess whether a set of Big Data is an essential facility or whether entirely new criteria should be developed instead.

3. MODIFICATION OF THE EXISTING CRITERIA FOR THE USE OF THE DOCTRINE IN BIG DATA ACCESS CASES

3.1. IMPOSSIBILITY OF DUPLICATION OF THE FACILITY AND THE "OBJECTIVE TEST"

The application of the doctrine presupposes that it is impossible to duplicate the facility in question. This impossibility may be permanent or temporary[52] and may be caused by topographical, technical, physical, legal, or economic reasons. Topographical, technical and physical impossibility of duplicating a facility is in principle permanent but can be overcome by technological progress, while legal and economic impossibility is temporary.[53] Topographical, technical, and physical impossibility of duplication is not relevant in cases of access to Big Data, since any set of Big Data can always be, from a purely technical point of view, duplicated with significant enough investment. One can imagine situations in which the duplication of a set of Big Data is legally impossible, but only if it contains personal data.[54] However, the most common reason for the impossibility of duplicating a set of Big Data is its economic unviability, i.e., too high (prohibitive) investments related to setting up the facilities needed for data collection and analysis (powerful processors, advanced software, skilled engineers, etc.).

(BGBl. I S. 730) geändert worden ist. Germany. Berlin: Das Bundesministerium der Justiz and das Bundesamt für Justiz. In German, point 4 of paragraph 2 of article 19.

49 *hiQ Labs, Inc. v. LinkedIn Corp.* (2019) United States Court of Appeals for the Ninth Circuit, 9 September.

50 *PeopleBrowsr, Inc. v. Twitter, Inc.* (2013) United States District Court for the Northern District of California, 6 March.

51 Although the doctrine was not used, as it was de facto banned from the U.S. legal system by the Supreme Court's Trinko ruling. See: *Verizon Communications Inc. v. Law Offices of Curtis V. Trinko, LLP* (2004) United States of America Supreme Court, 13 January.

52 Rottenbiler, S. (2002) *Essential Facilities als ordnungspolitischer Problem*. Frankfurt: Peter Lang Verlag, pp. 28-37.

53 Hohmann (2001) op. cit., p. 228.

54 For a more in-depth discussion see: Dacar, R. (2022) Is the Essential Facilities Doctrine Fit for Access to Data Cases? The Data Protection Aspect. *Croatian Yearbook of European Law and Policy*, 18, pp. 61-81.

The possibilities for arguing that a facility's duplication is impossible due to economic unviability were severely limited by the "objective test" introduced by the Bronner ruling. This test does not consider the market position of the demanding company, as it requires that duplication of a facility be economically unviable for a company with a comparable market position to the controlling company. Consequently, in the Bronner ruling, the Court indicated that application of the doctrine requires that duplication of the newspaper delivery network be economically unviable for a company with a comparable market position to the controlling company, not just for the demanding company.[55] In other words, the low daily circulation and resulting low market share of the demanding company could not have been considered in determining whether duplication of the newspaper delivery network was impossible. [56] The goal of the "objective test" is to limit the application of the doctrine to cases where market competition as an institution, and not just the market position of individual companies, is threatened. [57] In my view, however, applying the "objective test" to Big Data-driven markets overshoots the mark and makes the application of the doctrine virtually impossible. The latter markets have several important distinguishing features as compared to brick-and-mortar markets, among others:

- Extreme and ad infinitum economies of scale (and the absence of diseconomies of scale), which are not present in brick-and-mortar markets, where the economies of scale reach a tipping point - if production continues beyond this point, diseconomies of scale occur. However, the economic efficiency of collecting and analysing Big Data increases linearly or even exponentially as the amount of data increases and never reaches the tipping point that leads to diseconomies of scale.[58] One of the main reasons for the extreme economies of scale in

[55] The controlling company, Mediaprint, had a market share of 46% while the demanding company, Der Standard, owned by Oskar Bronner, had a market share of 3,6% in the relevant (downstream) market.

[56] Also see: Judgement of 26 November 1998, Oscar Bronner GmbH & Co. KG v Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co. KG, Mediaprint Zeitungsvertriebsgesellschaft mbH & Co. KG and Mediaprint Anzeigengesellschaft mbH & Co. KG, C-7/97, EU:C:1998:569, paragraphs 44-46.

[57] The ruling followed the opinion of AG Jacobs who showed great reticence towards the doctrine's application, pointing out that mandated access to a facility can increase the level of competition in the short-term, but lower it in the long-term by decreasing the incentives to invest in developing new facilities and improving existing ones. See: Opinion of AG Jacobs of 28 May 1998, Oscar Bronner GmbH & Co. KG v Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co. KG, Mediaprint Zeitungsvertriebsgesellschaft mbH & Co. KG and Mediaprint Anzeigengesellschaft mbH & Co. KG, EU:C:1998:264, paragraph 57.

[58] Cédric. O. (2021), Le digital markets act: Un nouveau chapitre dans l'histoire du droit de la concurrence. *Esprit*, 472, pp. 126-138, p. 132. Also see: Bagnoli, V. (2020) Digital

Big Data-driven markets is the significant upfront investment required to build the infrastructure and technology needed to process massive amounts of data. Companies must build extensive data centers, acquire advanced hardware, develop sophisticated software, and hire data scientists and engineers. As these initial costs are spread over a growing volume of data, the cost per unit of data processing or storage drops significantly.

- Extreme direct and indirect network effects (network externalities)[59] that increase the market power of the leading companies and represent an important barrier to entry for potential competitors. Extreme direct network effects have been recognized by the German Federal Cartel Office (Bundeskartellamt) as the main reason for Meta's ultra-dominant position in the market for social networks in Germany.[60] The stronger the network effects, the more difficult it is for a new product to compete with a product already on the market. Network effects, both direct and indirect, are particularly pronounced in Big Data-driven markets,[61] where they are typically related to either the vast amount of data a company controls, its content, or both.[62] A typical example of strong network effects in Big Data-driven markets are social platforms such as Facebook, Instagram, or Twitter. The more users join these platforms, the more data is generated in the form of posts, likes, shares and comments. This data, in turn, helps these platforms improve

Platforms as Public Utilities. *International Review of Intellectual Property and Competition*, 51(8), pp. 903-905; Pfeiffer, R. A. C. (2019) Digital Economy, Big Data and Competition Law. *Market and Competition Law Review*, 3 (1), p. 68.

[59] Direct network effects represent the increase in the value of a product to an individual user resulting from the increase in the total number of users, while indirect network effects represent the increase in the number and quality of complementary products with the increase in the number of users of the primary product. For more see e.g.: Kolasky, W. J. (1999) Network Effects: A Contrarian View. *George Mason Law Review*, 7(3), pp. 577-616, p. 579; Lemley, M. A. and McGowan, D. (1998) Legal Implications of Network Economic Effects. *California Law Review*, 86(3), pp. 479-612, p. 481; Waller, S. W. (2012) Antitrust and Social Networking. *North Carolina Law Review*, 90(5), pp. 1771-1806.

[60] In the seminal Facebook decision, the German Federal Cartel Office concluded that if consumers wanted to use social networks in general, they would have no choice but to use the social network Facebook, because there were no actual or potential substitutes for it due to extreme network effects. See: Decision of the Bundeskartellamt of 6 February 2019 in Facebook, B6-22/16. Available from: `http://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.pdf\%\3F__blob\%\3DpublicationFile\%\26v\%\3D5` [Accessed on 14 April 2023].

[61] See: Graef, I. (2016), *Data as Essential Facility Competition and Innovation on Online Platforms*. [online] Ph.D. University of Tilburg, pp. 44-50.

[62] Tucker, C. (2019) Digital Data, Platforms and the Usual (Antitrust) Suspects: Network Effects, Switching Costs, Essential Facility. *Review of Industrial Organization*, 54(4), p. 685.

their algorithms for content recommendations, ad targeting and user engagement. The more data they have, the better they can customize the user experience and make the platform more valuable to both users and advertisers.

- The first-mover advantage,[63] which leads to a rapid consolidation of market positions and a monopolistic (in the best case, oligopolistic) market structure from a global perspective, as evidenced by Meta, Apple, Google, Amazon and Netflix, among others. These companies gained enormous market shares and corresponding market power through their early market entry,[64] which gives them privileged access to extensive and unexplored data sources. Over time, first movers accumulate valuable data and, equally important, experience in data management and analysis. This becomes a formidable obstacle for potential competitors, leading to a "winner takes it all" structure of the market where a single dominant player can capture the lion's share of the market, leaving little room for competition.[65]

- The snowball effect in Big Data-driven markets symbolizes the remarkable growth of benefits derived from the continuous accumulation and effective use of data resources. By amassing increasingly rich data sets from multiple sources, companies gain deeper insights, foster innovation, and solidify their competitive position. This effect is gaining momentum over time, giving those who embrace it early on a significant head start. They use data not only for marketing and sales, but also for operational improvements, customer-focused strategies, and product innovation.[66]

[63] A phenomenon (occurring mainly in markets that require high start-up costs) in which the first company to enter the market is more successful than its competitors simply because it entered the market first. The later company can thus consolidate its market position to such an extent that effective competition is no longer possible.

[64] Bughin J., et. al. (2016) The Age of Analytics: Competing in a Data-Driven World. [online]. Washington DC: McKinsey Global Institute, p. 26. Available from:https://www.mckinsey.com/~/media/mckinsey/industries/public\%\20and\%\20social\%\20sector/our\%\20insights/the\%\20age\%\20of\%\20analytics\%\20competing\%\20in\%\20a\%\20data\%\20driven\%\20world/mgi-the-age-of-analytics-full-report.pdf [Accessed on 10 April 2023].

[65] de Moncuit, A. (2018) Connecting Competition Law Standards to the Internet of Things. *Concurrences*, 4-2018, p. 86.

[66] Also see: Gambaro, M. (2018) Big data competition and market power. *Market and Competition Law Review*, 2(2), p. 110.

The aforementioned characteristics lead to extremely high market concentration, which is not common in brick-and-mortar markets,[67] and reduce the intensity of competition in the market by erecting virtually insurmountable barriers to entry.[68] As a result, monopolistic or at best oligopolistic structures are not only common but rather the rule in Big Data-driven markets, with competitive markets being an exception.[69]

The companies that control most of the world's data are also among the most powerful companies in the world: 6 of the world's 10 largest companies by market capitalization operate exclusively or largely in Big Data-driven markets (e.g., Meta, Netflix, Amazon, Apple, and Microsoft).[70] Because of their strong or even monopolistic positions in key Big Data-driven markets (such as the market for social networks, internet search and targeted advertising), they have built up significant market power and unprecedented access to factors of production.[71] In my view, it is therefore reasonable to argue, that, at least in theory, they would be able to duplicate almost any set of Big Data if they decided to allocate sufficient factors of production to that end. An example of this is Meta's recent attempt to duplicate Twitter (now X) with its Threads application, which included duplicating the Big Data that Twitter thrives on. Although Threads' user base shrank radically about six weeks after the application's launch, and the attempt to seriously compete with Twitter thus failed, the initial duplication was still possible and even quite successful, as evidenced by the initial high number of users.[72] The reasons for the failure of Threads do not lie in Meta's inability to duplicate Big Data, but rather in the strong network effects associated with Twitter and Threads' design flaws.[73]

---

[67] Graef, I. (2016), *Data as Essential Facility Competition and Innovation on Online Platforms*. [online] Ph.D. University of Tilburg, pp. 54, 55.

[68] The danger of market concentration for competition in Big Data-driven markets has been recognized by a number of scholars. See e.g.: de Loecker, J., Eeckhout, J. and Unger, G. (2020) The Rise of Market Power and the Macroeconomic Implications. *The Quarterly Journal of Economics*, 135(2), pp. 561-644; Orbach, B. (2021) Anything, Anytime, Anywhere: Is Antitrust Ready for Flexible Market Arrangements? *Antitrust Source*, 20(5), pp. 1-15.

[69] Also see: Gambaro, M. (2018), Big Data Competition and Market Power. *Market and Competition Law Review*, 2(2), pp. 110-111.

[70] See: Ventura, L. (2023) *World's Largest Companies* 2023. [online] New York: Global Finance. Available from:`https://www.gfmag.com/global-data/economic-data/largest-companies` [Accessed 17 April 2023].

[71] Kai, L. (2019) Keeping Big Tech at Bay. *International Financial Law Review*, 2019(5), pp. 18-21.

[72] Chow, K., (2023) *Twitter's Rival Threads is Already Unraveling*. [online] Time Magazine. Available from: `https://time.com/6305383/meta-threads-failing/` [Accessed 19 September 2023].

[73] See: Isaac, M., (2023) *Why the Early Success of Threatds May Crash Into Reality*. [online] New York:The New York Times. Available from:`https://www.nytimes.com/2023/07/11/technology/threads-zuckerberg-meta-google-plus.html` [Accessed 19 September 2023]; Chow, op. cit.; Kantrowitz, A. (2023) *Threads is not an Automatic Win*

Now imagine a small start-up company in need of access to a set of Big Data controlled by one of the above companies (this set of Big Data is an essential input for activity on the downstream market). Since the "objective test" makes application of the doctrine conditional on the impossibility of duplication of the facility by a company with a comparable market position to the controlling company, the doctrine could only apply if the set of Big Data in question could not be duplicated by a company with a comparable market position to one of the "Big Tech" companies. Whether or not this is the case must, of course, be examined on a case-by-case basis. In general, however, it can be stated that a company with a market position comparable to Meta or the like would most likely be able to duplicate most sets of Big Data. There are, of course, cases where a set of Big Data cannot be duplicated, even by Big Tech. This could be the case if the data was collected over a long period of time and/or under very specific and non-reproducible circumstances.

While it should be noted that market dominance, which is a prerequisite for the application of the doctrine, generally involves significant economic power, it is clear that the economic power of a Big Tech company dominating a Big Data-driven market is far greater than that of dominant companies in the vast majority of traditional essential facility cases,[74] In other words, companies that are dominant in Big Data-driven markets tend to be far more economically powerful than companies in other markets where the doctrine has traditionally been applied.[75] This, by its nature, makes it much more difficult to meet the "objective test" in cases where the alleged essential facility is controlled by a Big Tech company than in traditional essential facility cases.Because most of the world's data is controlled by a handful of powerful companies,[76] the "objective test" severely limits the usefulness of the doctrine in Big Data access claims, restricting it to the few cases where

for Meta. [online] Slate. Available from: `https://slate.com/technology/2023/07/threads-meta-twitter-risks-opportunities.html` [Accessed 20 September 2023]; Dooley, R. (2023) Threads Engagement Drops 70%. Here's how it can Recover. [online] Forbes. Available from: `https://www.forbes.com/sites/rogerdooley/2023/07/25/threads-engagement-drop-not-shocking/?sh=42aabd66659c` [Accessed 20 September 2023].

[74] In Bronner, for example, Mediaprint had a dominant position on the market for newspaper delivery services in Austria, in Magill the relevant television stations had dominant positions on the market for individual television station programs in Ireland while in Lietuvos Geležinkeliai the said company had a dominant position on the market for the management of railway infrastructure in Latvia.

[75] One of such companies, for example is Meta, whom the German Federal Cartel Office (Bundeskartellamt) concluded had an "ultra dominant position" on the market for social networks. See: Decision of the Bundeskartellamt of 6 February 2019, Facebook, B6-22/16.

[76] Also see: Fukuyama, F. (2021) How to Save Democracy from Technology: Ending Big Tech's Information Monopoly. *Foreign Affairs*, 100(1), pp. 98-110; Klick, J. (2021) Big Tech's Robber Barrons. *Regulation*, 44(3), pp. 26-29.

the relevant sets of Big Data are either controlled by smaller companies or so specific that they cannot be reasonably duplicated even by another Big Tech company. Therefore, I believe that the "objective test" should be discarded in cases where Big Data is the alleged essential facility and replaced with a "subjective test", or at least the "average company test", where the "subjective test" takes into account the subjective ability of the demanding company to create a substitute set of Big Data and the "average company test" takes into account the ability of an average company operating in the relevant market to do so.

However, it should not be overlooked that competition law in the EU is based on the "as-efficient-competitor test", which aims to protect competitors that have the same efficiency as dominant companies or the potential to achieve it. Adopting the "subjective" or even the "average company" test would result in an ambiguous standard under which the less competitive a company is, the more protection it would receive, while more innovative and expanding companies would receive less protection. This could tempt some companies to intentionally take a weak position and subsequently seek access rights. Despite this, I believe that the mitigation of the "objective test" is justified because of the peculiarities of Big Data-driven markets described above, which were not taken into account in its creation.[77] In addition, Big Data differs from traditional essential facilities in that access to it is an essential prerequisite for opening numerous (theoretically countless) downstream markets (which do not yet exist).[78] Thus, the relevance of the ability of companies to access competitively relevant sets of Big Data goes beyond the purely economic interests of individual companies, as it has a positive impact on the economy as a whole.[79]

3.2. DOWNSTREAM MARKET PRESENCE REQUIREMENT

According to the Court's Ladbroke ruling, the doctrine can only be applied in cases where the controlling company is itself present in the downstream market.[80] The Ladbroke case involved the refusal of the French Societés des

[77] Which is only natural, since Big Data-driven markets did no exist at the time.

[78] Gambaro, op. cit., p. 102.

[79] This is a traditional characteristic of infrastructure facilities. Moreover, Big Data may also have other characteristics of infrastructure facilities, such as high start-up costs, its non-rival nature, economies of scale related to Big Data collection and analysis, and others. Of course, not all sets of Big Data exhibit the characteristics of infrastructure, and even if they do, they are not necessarily an essential facility. For more see: Scholz L. H. (2019) Big Data is not Big Oil: The Role of Analogy in the Law of New Technologies. *Tennessee Law Review*, 86(4), pp. (2019), pp. 863-894, p. 884; Vezzoso, S. (2020) All Happy Families are Alike: The EDPS Bridges Between Competition and Privacy. *Market and Competition Law Review*, 4(1), pp.41-68, p. 45.

[80] Also see: Colangelo G. and Maggiolino M. (2017) Big Data as Misleading Facilities. *European Competition Journal*, 13(2-3), pp. 249-281, p. 277; Korah, V. (2001) The Interface Between

courses (operators of horse races) to grant a licence to the Belgian company Ladbroke to broadcast, in Belgium, French horse races they operated. The Court concluded that no duty to deal existed, inter alia, because the Societés des courses were not present in the Belgian market for the broadcasting of horse races. The requirement that the dominant company must be active at least on the downstream market was retained in subsequent case law and thus remains valid.

This requirement is not problematic when the doctrine is applied in brick-and-mortar markets, where the downstream markets exist independently of the activity of the demanding company. For example, in Bronner, the market for daily newspapers in Austria existed independently of the activity of the newspaper Der Standard. In other words, there was no causal connection between the sail of the newspaper Der Standard and the existence of the market for daily newspapers in Austria. Ahead, in IMS Health, the downstream market for the supply of German regional sales data to pharmaceutical companies existed independently of the activity of the demanding company, NDC Health.[81] The same can be said for most essential facilities cases, where the controlling companies usually transfer their market power from the upstream to the downstream market, while demanding companies seek to enter the already existing downstream market.

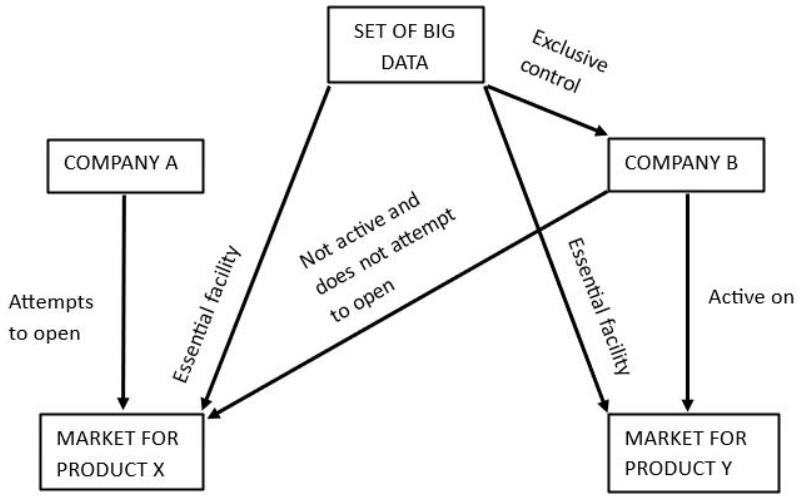
I argue that this is not necessarily the case in dynamic and propulsive markets driven by Big Data. Consider a hypothetical scenario in which an innovative startup (company A) wants to introduce a breakthrough (disruptive) product (product X) which is so innovative that it opens up a new, previously non-existent, market. An example of such a scenario is the creation of the dating app market, which was opened by the application Tinder. Later, other dating apps which were tailored to specific needs entered the market. The successful realization of product X is irrevocably dependent on company A gaining access to a specific set of Big Data that is under company B's exclusive control. In other words, this set of Big Data is an essential prerequisite for opening the market for product X. Company B uses this set of Big Data to offer a different product (product Y), but remains completely uninvolved in the emerging market for product X.[82] Since opening the market for product X requires access to the corresponding set of Big Data, this market cannot be opened by company A until it obtains access

Intellectual Property and Antitrust: the European Experience. *Antitrust Law Journal*, 69(3), pp. 801-839, p. 814.

[81] See: Judgement of 29 April 2004, IMS Health GmbH & Co. OHG v NDC Health GmbH & Co. KG, C-418/01, EU:C:2004:257, paragraph 46.

[82] Since different information can be extracted from the same set of Big Data it can be an essential input for the offering of different (theoretically countless) products.

to this set of Big Data from company B. Should company B choose to deny access to this set of Big Data, the doctrine cannot be applied because company B cannot be present in the market for product X, which does not yet exist and thus the downstream market presence requirement cannot be satisfied. This situation is illustrated graphically below.



Even if company B does not actively participate in the market for product X, it may have compelling incentives to hinder the emergence of the market. In my view, two main motivations may underlie such behavior. First, company B may seek to reserve the market for product X as a precautionary measure to preserve it for possible future entry.[83] Second, company B may

[83] "Pre-emptive market reservation" refers to a strategic action taken by a company to secure or reserve a particular market or industry segment in anticipation of potential future entry. This pre-emptive strategy is often used to prevent or make it more difficult for competitors to enter or gain a foothold in that market. A practical example of pre-emptive market reservation is Microsoft's bundling of Internet Explorer with the Windows operating systems in the late 1990s. Microsoft's action was seen as an attempt to reserve the market for Web browsers and to prevent competition from other Web browsers such as Netscape Navigator. Microsoft's actions sparked the "first browser war" and led to a significant antitrust case in the United States of America. See: United States v. Microsoft Corp (2001). United States Court of Appeals for the District of Columbia Circuit, June 28, 2001; Campbell, W. J. (2015) *The '90s Startup That Terrified Microsoft and Got Americans to Go Online.* [online] Wired. Available from: https:https://www.wired.com/2015/01/90s-startup-terrified-microsoft-got-americans-go-online/ [Accessed 19 September 2023]; Usama, J. (2023) *29 years ago, Microsoft thought of bundling Internet Explorer with Windows.* [online] XDA. Available from: https://www.xda-developers.

be concerned that the emergence of the market for product X may increase company A's market power and thereby threaten company B's position in a related horizontal market, particularly if company B engages in activities that are relevant to the market for product X. In other words: In the absence of contractual arrangements, only company B (or another company granted access to the relevant Big Data by company B) can open the market for product X. This leads to the conclusion that the downstream market presence requirement actually means that only the company controlling a set of Big Data (without a data sharing contract, of course) can open a new market for which this set of Big Data is an essential input, as the use of the doctrine is not possible in such positions. It can therefore be concluded that the downstream market presence requirement hinders the establishment of new downstream markets and thus has a negative impact on (disruptive) innovation. This is especially problematic in Big Data-driven markets, which are already prone to high degrees of market concentration.

4. CONCLUSION

Despite the reluctance the Court to confirm the character of a set of Big Data as an essential facility, a set of Big Data may indeed be an essential input for activities on the downstream market, as has been confirmed, inter alia, by the German Act Against Restraints of Competition, the Digital Markets Act, and a handful of U.S. court cases.

However, it is not clear what criteria should be used in EU competition law to assess the character of a set of Big Data as an essential facility (the Bronner criteria, the IMS Health criteria, or the Microsoft criteria). Since this is a question of competition policy rather than competition law, this paper has not attempted to address it. However, it has examined how the application of the "objective test" and the downstream market presence requirement, which are common to all criteria for assessing the essential character of a facility under the doctrine, affect the effectiveness of the doctrine in Big Data access cases.

The application of the "objective test" means that, for the doctrine to apply, the duplication of the facility in question must be impossible for a company with a comparable market position to the controlling company, and not just for the demanding company, with the impossibility being projected especially in economic unviability. Thus, an economically weak company cannot request access to an essential facility on the grounds that it cannot duplicate it because of its own economic weakness. The "objective test" was

com/microsoft-bundling-internet-explorer-windows-29-years/[Accessed 23 September 2023].

introduced in the Bronner ruling with the aim of limiting the scope of the doctrine to cases where the denial of access to an essential facility threatens market competition as an institution and not just the position of individual competitors. This is intended to preserve the incentives of controlling companies to invest in the development of essential facilities. In my view, however, the "objective test" overshoots the mark in Big Data-driven markets. These markets are very different from traditional markets in that monopolistic or oligopolistic market structures are not only common, but the norm (due to several peculiarities of Big Data-driven markets, in particular (but not only) extreme economies of scale, extreme network effects, the "winner takes it all" operating principle, and the snowball principle). For example, the majority of the world's data is controlled by a handful of powerful companies such as Meta, Alphabet, Apple, Netflix, Microsoft, etc., which have ample access to capital and other factors of production (as they are also among the world's largest companies). In my opinion, it would be rare that a company with a comparable market position to one those companies would not be able to duplicate most sets of Big Data if it decided to invest sufficient factors of production for that purpose. Applying the "objective test" thus severely limits the doctrine's applicability on Big Data-driven markets, restricting it mainly to cases where duplication of a set of Big Data would not be possible even for a company in a comparable position to one of the most powerful companies in the world. This could be the case if the data in question was collected over a long period of time and/or under very specific circumstances. Moreover, taking into account the "objective test", the doctrine can also be applied in cases where the set of Big Data in question is controlled by a smaller company and the company with a comparable market position is not able to duplicate the Big Data in question.

Therefore, I believe that the "objective test" should be discarded in Big Data access cases and replaced by the "subjective test" or the "average company test". The mitigation of the "objective test" is controversial because EU competition law is based on the "as-efficient-competitor test," which protects companies that are as efficient as the dominant company. Applying the "subjective test" or even the "average company test" could also create incentives for companies to remain small (and inefficient) in order to be able to use the doctrine to gain access to sets of Big Data on preferential terms over larger and/or more efficient companies. Nonetheless, I believe that the elimination of the "objective test" could be justified by the characteristics of Big Data-driven markets discussed above, as well as by the fact that access by innovative companies to competitively relevant sets of Big Data is not only in their interest, but also in the interest of society as a whole, as it enables

the development of new products, business models, or entirely new markets, which increases consumer welfare.

I also argue that the downstream market presence requirement should be eliminated altogether in Big Data access cases. The latter requirement, like the "objective test", was introduced with the goal of limiting the scope of the doctrine and increasing investment incentives for controlling companies. In my view, however, it is extremely harmful in Big Data-driven markets, as it renders the doctrine virtually inapplicable in a large portion of cases. Traditionally, in essential facility cases, downstream markets exist independently of the activities of the demanding company and are usually controlled to a significant degree by the controlling company, which transfers its dominance from the upstream to the downstream market. In Bronner, for example, the market for daily newspapers (downstream market) existed independently from the activity of the company Mediaprint (demanding company) on it. In other words, the market for daily newspapers in Austria existed, regardless of whether Mediaprint was active on it or not. However, the situation is different in Big Data-driven markets. It is not uncommon that a demanding company needs access to a relevant set of Big Data to open a new, as of yet inexistent, market. Since the market has not yet been opened, the controlling company cannot have a presence in it. Therefore, as the downstream market presence requirement cannot be met, the doctrine cannot be applied. The only way for the demanding company to apply the doctrine in such a situation is to wait until the controlling company opens the market in question, which leads to that company being active in it, fulfilling the downstream market presence requirement. Companies controlling sets of Big Data may well have an interest in preventing the opening of new markets in which they do not operate, either as a preventive (market) reservation or to limit the market power of the demanding company (especially if they compete in another market).

In my view, the Commission and the Court will have to address the issue of Big Data as an essential facility in the near future, most likely in the context of Big Data access claims that go beyond the scope of the Digital Markets Act. To make the doctrine an effective tool for access to competitively relevant sets of Big Data, the existing conditions for the application of the doctrine will need to be modified. Regardless of what criteria will be used in the assessment, the above analysis has shown that the "objective test" must be mitigated, and the downstream market presence requirement dropped altogether.

LIST OF REFERENCES

[1] Andreangeli, A. (2009) Interoperability as an "Essential Facility" in the Microsoft Case: Encouraging Stifling Competition or Innovation? *European Law Review*, 35(4), pp. 584-611.

[2] Areeda, P. (1989) Essential Facilities: an Epithet in need of Limiting Principles. *Antitrust Law Journal*, 58(3), pp. 841-853.

[3] Bagnoli, V. (2020) Digital Platforms as Public Utilities. *International Review of Intellectual Property and Competition*, 51(8), pp. 903-905.

[4] Botta, M. and Wiedemann, K. (2019) The Interaction of EU Competition, Consumer and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey. *Antitrust Bulletin*, 64(3), pp. 428-446.

[5] Bughin J., et. al. (2016) *The Age of Analytics: Competing in a Data-Driven World*. [online] Washington DC: McKinsey Global Institute. Available from: https://www.mckinsey.com/~/media/mckinsey/industries/public%20and%20social%20sector/our%20insights/the%20age%20of%20analytics%20competing%20in%20a%20data%20driven%20world/mgi-the-age-of-analytics-full-report.pdf [Accessed on 10 April 2023].

[6] Butts, C. (2010) The Microsoft Case 10 Years Later: Antitrust and New Leading "New Economy" Firms. *Northwestern Journal of Technology and Intellectual Property*, 8(2), pp. 275-291.

[7] Campbell, W. J. (2015) *The '90s Startup That Terrified Microsoft and Got Americans to Go Online*, [online] Forbes. Available from: https://www.wired.com/2015/01/90s-startup-terrified-microsoft-got-americans-go-online/[Accessed 19 September 2023].

[8] Chen, Y. (2014). Refusal to Deal, Intellectual Property Rights, and Antitrust. *The Journal of Law, Economics, and Organization*, 30(3), pp. 533-557.

[9] Chow, K., (2023) Twitter's Rival Threads is Already Unraveling. [online] Time Magazine. Available from: https://time.com/6305383/meta-threads-failing/ [Accessed 19 September 2023].

[10] Colangelo G. and Maggiolino M. (2017) Big Data as Misleading Facilities. *European Competition Journal*, 2-3/2017, pp. 249-281.

[11] Commission Decision of 11 March 2008 in Google/DoubleClick, COMP/M.4731. Available from: https://ec.europa.eu/competition/mergers/cases/decisions/m4731_20080311_20682_en.pdf [Accessed 12 April 2023].

[12] Commission Decision of 11 March 2008 declaring a concentration to be compatible with the common market and the functioning of the EEA

Agreement (Google/DoubleClick), *Official Journal of the European Union* (COMP/M.4731) 11 March. Available from:https://ec.europa.eu/competition/mergers/cases/decisions/m4731_20080311_20682_en.pdf [Accessed 12 April 2023]

[13] Commission Decision of 3 October 2014 in Facebook/WhatsApp, *Official Journal of the European Union* (COMP/M.7217) 3 October. Available from:https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014M7217 [Accessed 12 April 2023].

[14] Commission Decision of 4 September 2012 in Telefónica UK/ Vodafone UK/ Everything Everywhere/ JV, Official Journal of the European Union (COMP/M.6314) 4 September. Available from:https://ec.europa.eu/competition/mergers/cases/decisions/m6314_20120904_20682_2898627_EN.pdf [Accessed 12 April 2023].

[15] European Commission. (2014) *Communication from the Commission of 2 July 2014: Towards a thriving data-driven economy*. COM/2014/0442. p. 4. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52014DC0442 [Accessed 11 April 2015].

[16] Cotter, T. F. (1999). Intellectual Property and the Essential Facilities Doctrine. *Antitrust Bulletin*, 44(1), pp. 211-250.

[17] Craig, P. and de Burca, G. (2015) *EU Law: Text, Cases, and Materials*. 6th ed. Oxford: Oxford University Press

[18] Crémer, J., de Montjoye, Y. A. in Schweitzer, H. (2019) *Competition Policy for the Digital Era*, Luxembourg: Publications Office of the European Union.

[19] Czapracka, K. (2021) The Essential Facilities Doc-trine and the Bronner Judgment Clarified, Case C-165/19 P Slovak Telekom v Commission. *Journal of European Competition Law Practice*, 13(4), pp. 278-280.

[20] Dacar, R. (2022) Is the Essential Facilities Doctrine Fit for Access to Data Cases? The Data Protection Aspect. *Croatian Yearbook of European Law and Policy*, 18, pp. 61-81.

[21] de Hert, P. and Sajfert, J. (2019) Regulating Data in and out of the Data Protection Policy Field: two Scenarios of post-GDPR Law-Making and the Actor Perspective. *European Data Protection Law Review*, 5(3), pp. 338-351.

[22] de Moncuit, A. (2018) Connecting Competition Law Standards to the Internet of Things. *Concurrences*, 4-2018, pp. 85-94.

[23] Decision of the Bundeskartellamt of 6 February 2019 in Facebook, B6-22/16. Available from: http://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Entscheidungen/Missbrauchsaufsicht/2019/

B6-22-16.pdf%3F__blob%3DpublicationFile%26v%3D5 [Accessed on 14 April 2023].

[24] Dooley, R. (2023) *Threads Engagement Drops 70%. Here's how it can Recover*, [online] Forbes. Available from: https://www.forbes.com/sites/rogerdooley/2023/07/25/threads-engagement-drop-not-shocking/?sh=42aabd66659c [Accessed 20 September 2023].

[25] Eilmansberger, T. (2005) The Essential Facilities Doctrine Under Art. 82: What is the State of Affairs After IMS Health and Microsoft. *King's College Law Review*, 16(2), pp. 329-346.

[26] Fukuyama, F. (2021) How to Save Democracy from Technology: Ending Big Tech's Information Monopoly. *Foreign Affairs*, 100(1), pp. 98-110.

[27] Gambaro, M. (2018) Big Data Competition and Market Power. *Market and Competition Law Review*, 2(2), pp. 99-124.

[28] Gerber, D. J. (1988) Rethinking the Monopolist's Duty to Deal: a Legal and Economic Critique of "Essential Facilities". *Virginia Law Review*, 74(6), pp. 1069-1113.

[29] *Gesetz gegen Wettbewerbsbeschränkungen in der Fassung der Bekanntmachung vom 26. Juni 2013 (BGBl. I S.1750, 3245), das zuletzt durch Artikel 4 des Gesetzes vom 20. Mai 2022 (BGBl. I S. 730) geändert worden ist.* Germany. Berlin: Das Bundesministerium der Justiz and das Bundesamt für Justiz. In German.

[30] Ginsburg, D., Garadin, D. and Klovers, K. (2019) Antitrust and Intellectual Property in the United States and the European Union, pp. 99-120. In: Muscolo, G. and Tavassi, M. A. (eds.) *The Interplay between Competition Law and Intellectual Property: An International perspective*. Alpen aan den Rijn: Kluwer Law International.

[31] Graef, I. (2011) Tailoring the Essential Facilities Doctrine to the IT sector: Compulsory Licensing of Intellectual Property Rights after Microsoft. *Cambridge Student Law Review*, 7(1), pp. 1-20.

[32] Graef, I. (2016), *Data as Essential Facility Competition and Innovation on Online Platforms*. [online] Ph.D. University of Tilburg

[33] Hatzopoulos, V. (2005) *The EU Essential Facilities Doctrine*. Bruges: College of Europe.

[34] Hayashi, S. and Arai, K. (2019) How Competition Law Should React in the Age of Big Data and Artificial Intelligence. *The Antitrust Bulletin*, 64(3), pp. 447-456.

[35] *hiQ Labs, Inc. v. LinkedIn Corp.* (2019) United States Court of Appeals for the Ninth Circuit, 9 September 2019.

[36] Hohmann, H. (2001) *Die essential Facility Doctrine im Recht der Wettbewerbsbeschränkungen*. Baden-Baden: Nomos.

[37] Hovenkamp, H. (2011) *Federal Antitrust Policy, the Law of Competition and its Practice*. 4th ed. St. Paul: West.

[38] Isaac, M., (2023) Why the Early Success of Threatds May Crash Into Reality. [online] The New York Times. Available from: https://www.nytimes.com/2023/07/11/technology/threads-zuckerberg-meta-google-plus.html [Accessed 19 September 2023].

[39] Judgement of 11 May 1988, Consorzio Italiano della Componentistica di Ricambio per Autoveiculi and Maxicar v Régie des Usines Renault, EU:C:1988:472.

[40] Judgement of 11 November 1997, Commission of the European Communities and French Republic v Ladbroke Racing Ltd., C-359/95 P, EU:C:1997:531.

[41] Judgement of 12 January 2023 in Lietuvos geležinkeliai v Commission, C-42/21 P, EU:C:2023:12.

[42] Judgement of 26 November 1998, Oscar Bronner GmbH & Co. KG v Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co. KG, Mediaprint Zeitungsvertriebsgesellschaft mbH & Co. KG and Mediaprint Anzeigengesellschaft mbH & Co. KG, C-7/97, ECLI:EU:C:1998:569.

[43] Judgement of 29 April 2004, IMS Health GmbH Co. OHG v NDC Health GmbH & Co. KG, C-418/01, EU:C:2004:257.

[44] Judgement of 5 October 1988, 238/87, AB Volvo v Erik Veng (UK) Ltd, EU:C:1988:477.

[45] Judgement of 6 March 1974, Istituto Chemioterapico Italiano and Commercial Solvents v Commission, C-6/73, EU:C:1974:18.

[46] Judgement of 9 September 2009, Clearstream Banking AG and Clearstream International SA v Commission of the European Communities, T-301/04, EU:T:2009:317.

[47] Judgement of March 2021 in Slovak Telekom v Commission, C-165/19 P, EU:C:2021:239.

[48] Kadar, M. and Bogdan, M. (2017) "Big Data" and EU Merger Control - a Case Review. *Journal of European Competition Law and Practice*, 8(8), pp. 479-491.

[49] Kai, L., (2019) Keeping Big Tech at Bay. *International Financial Law Review*, 2019(5), pp. 18-21.

[50] Kantrowitz, A. (2023) *Threads is not an Automatic Win for Meta*. [online] Slate. Available from: https://slate.com/technology/2023/07/threads-meta-twitter-risks-opportunities.html [Accessed 20 September 2023].

[51] Katz, M. L. (2019) Multisided Platforms, Big Data, and a Little Antitrust Policy. *Review of Industrial Organization*, 54(4), pp. 669-716.

[52] Klick, J. (2021) Big Tech's Robber Barrons. *Regulation*, 44(3), pp. 26-29.

[53] Kolasky, W. J. (1999) Network Effects: A Contrarian View. *George Mason Law Review*, 7(3), pp. 577-616.

[54] Korah, V. (2002) The Interface Between Intellectual Property and Antitrust: the European Experience. *Antitrust Law Journal*, 69(3), pp. 801-839.

[55] Kupčik, J. and Mikeš, S. (2018) Discussion on Big Data, Online Advertising and Competition Policy. *European Competition Law Review*, 39(9), pp. 393-402.

[56] Lasserre, B. and Mundt, A. (2017) Competition Law and Big Data: The Enforcers View. *Rivista Italiana di Antitrust*, 1/2017, pp. 87-103.

[57] Lemley, M. A. and McGowan, D. (1998) Legal Implications of Network Economic Effects. *California Law Review*, 86(3), pp. 479-612.

[58] Loecker, J., Eeckhout, J. and Unger, G. (2020) The Rise of Market Power and the Macroeconomic Implications. *The Quarterly Journal of Economics*, 135(2), pp. 561-644.

[59] Lugard, P. and Roach, L. (2017) The Era of Big Data and the EU/U.S. Divergence for Refusals to Deal. *Antitrust*, 31(2), pp. 58-64.

[60] Mandrescu, D. (2018) The SSNIP Test and Zero-Price Strategies. *European Competition and Regulatory Law Review*, 2(4), pp. 244-260.

[61] Minevick, M. (2020) *The Automotive Industry and the Data Driven Approach*. [online] Jersey City: Forbes. Available from: `https://www.forbes.com/sites/markminevich/2020/07/13/the-automotive-industry-and-the-data-driven-approach/?sh=84cfedcf9a53` [Accessed 8 September 2023].

[62] Modrall, J. (2018) Big Data and Merger Control in the EU. *Journal of European Competition Law and Practice*, 9(9), pp. 569-578.

[63] Muller, U. and Rodenhausen, A. (2008) The Rise and Fall of the Essential Facility Doctrine. *European Competition Law Review*, 29(5), pp. 310-329.

[64] O. C. (2021), Le digital markets act: Un nouveau chapitre dans l'histoire du droit de la concurrence. *Esprit*, 3-2021, pp. 125-138.

[65] Opinion of AG Jacobs of 28 May 1998, Oscar Bronner GmbH & Co. KG v Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co. KG, Mediaprint Zeitungsvertriebsgesellschaft mbH & Co. KG and Mediaprint Anzeigengesellschaft mbH & Co. KG, EU:C:1998:264.

[66] Orbach, B. (2021) Anything, Anytime, Anywhere: Is Antitrust Ready for Flexible Market Arrangements? *Antitrust Source*, 20(5), pp. 1-15.

[67] *PeopleBrowsr, Inc. v. Twitter, Inc.* (2013) United States District Court for the Northern District of California, 6 March.

[68] Pfeiffer, C., Augusto, R. (2019) Digital Economy, Big Data and Competition Law. *Market and Competition Law Review*, 3(1), pp. 53-90.

[69] Qi, J. (2020) Application of Essential Facilities Doctrine to "Big Data": US and EU Perspectives. *European Competition Law Review*, 40(4), pp. 182-189.

[70] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828. *Official Journal of the European Union* (OJ L 265) 12 October. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925 [Accessed 13 April 2023].

[71] Rinaldi, A. (2020) Re-Imagining the Abuse of Economic Dependence in a Digital World. *European Competition Law Review*, 4(2), pp. 253-256.

[72] Rottenbiler, S. (2002) *Essential Facilities als ordnungspolitischer Problem*. Frankfurt: Peter Lang Verlag.

[73] Ryan, D. (2021) Big Data and the Essential Facilities Doctrine: A Law and Economics Approach to Fostering Competition and Innovation in Creative Industries. *UCL Journal of Law and Jurisprudence*, 10/2021, pp. 84-112.

[74] Scholz L. H. (2019) Big Data is not Big Oil: The Role of Analogy in the Law of New Technologies. *Tennessee Law Review*, 86(4), pp. (2019), pp. 863-894.

[75] Seelen, C. M. (1997) The Essential Facilities Doctrine: What Does it Mean to be Essential. *Marquette Law Review*, 80(4) (1997), pp. 1117-1134.

[76] Sivinski, G., Okuliar, A. and Kjolbye, L. (2017) Is Big Data a Big Deal? A Competition Law Approach to Big Data. *European Competition Journal*, 13(2/3), pp. 199-227.

[77] Suarez, F. and Lanzolla, G. (2005) The Half-Truth of First Mover Advantage. *Harvard Business Review*, 83(4), pp. 121-127.

[78] The Economist. (2017) *The World's Most Valuable Resource Is No Longer Oil, But Data*. [online] London: The Economist. Available from: https://www.economist.com/leaders/2o7/05/o6/the-worlds-most-valuable-resource-is-no-longer-oil-but-data [Accesseds 12 April 2023].

[79] Tucker, C. (2019) Digital Data, Platforms and the Usual (Antitrust) Suspects: Network Effects, Switching Costs, Essential Facility. *Review of Industrial Organization*, 54(4), p. 683-693.

[80] *United States v. Microsoft Corp.* (2001). United States Court of Appeals for the District of Columbia Circuit, 28 June 2001.

[81] Usama, J. (2023) *29 years ago, Microsoft thought of bundling Internet Explorer with Windows.* [online] XDA. Available: https://www.xda-developers.com/

microsoft-bundling-internet-explorer-windows-29-years/ [Accessed 23 September 2023].

[82] van den Bergh, R. and Camesca, P. D. (2006) *European Competition Law and Economics: A Comparative Perspective*. 2nd ed. London: Sweet & Maxwell

[83] van Schendel, S. and van der Sloot, B. (2016) Ten Questions for Future Regulation of Big Data: a Comparative and Empirical Legal Study. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 7(2), pp. 110-145.

[84] Ventura, L. (2023) *World's Largest Companies 2023*. [online] New York: Global Finance. Available from: https://www.gfmag.com/global-data/economic-data/largest-companies [Accessed 17 April 2023].

[85] *Verizon Communications Inc. v. Law Offices of Curtis V. Trinko* (2004). United States of America Supreme Court, 13 January.

[86] Vezzoso, S. (2020) All Happy Families are Alike: The EDPS Bridges Between Competition and Privacy. *Market and Competition Law Review*, 4(1), pp.41-68.

[87] Waller, S. W. (2012) Antitrust and Social Networking. *North Carolina Law Review*, 90(5), pp. 1771-1806.

DOI 10.5817/MUJLT2024-1-4

UNVEILING THE BLACK BOX: BRINGING ALGORITHMIC TRANSPARENCY TO AI

by

GYANDEEP CHAUDHARY *

Overall, algorithmic transparency is an important aspect of responsible AI development and deployment. Ensuring that AI systems are transparent and accountable will help build trust and confidence in these systems and ensure that they are used ethically and effectively. Artificial intelligence (AI) has emerged as a cutting-edge domain that is fundamentally redefining different areas of daily experiences, such as health care, transport, finance, education, and others. The systems are not created for making a judgment like human judgment of natural language, spotting patterns and problem-solving; rather AI produces machines that also have intelligence level same as that of human beings.

AI having more influence over us, it is to be considered the ethical directions of these tools and see that they operate under principles of transparency and accountability. The element regarding algorithmic transparency, which means the process of understanding the functioning and explanation of how AI systems make their decisions is the one that is most crucial. The issue of algorithm transparency is of fundamental importance for many considerations. AI systems are not only supported by fairness but also by their non-discrimination. If we do not know how a system of AI arrives at the decisions made, it becomes impossible to determine if the provided results meet equal treatment for everybody. If used in delicate areas like recruitment, credit, and legal system- where the AI-machine must make choices which are life changing, then this aspect is very important.

On top of fairness, algorithmic transparency is also an important factor for accountability. If we are ignorant about what an artificial intelligence algorithm does and what is the source of its decision-making process, we are unable to track and classify the mistakes or mishaps of the system. This has always mattered when central to the operation of systems with high stake, such as those used in

* Assistant Professor, School of Law, Bennett University, India, gyan.2889@gmail.com

self-driving vehicles or in health care. Algorithmic transparency may be reached using different instruments. The transparent AI systems can be made by a more transparent design, for example, the simple modelling tools, that use interpretable models. Another method is designing technologies and techniques that can help people why the artificial systems difficult to be decoded but easy to understand which they can utilize in making decisions.

Therefore, algorithmic transparency is a key factor of the AI made responsibly and used by the society. It is crucial that AI machines are both transparent and accountable since this will lead to people building trust in the system and accepting its ethical and practical implications. This paper examines regulation of algorithmic transparency in the EU, specifically provisions under the General Data Protection Regulation (GDPR), it aims to situate analysis of the GDPR's provisions on explainability of AI systems within broader technology ethics and policy discourse. The paper's scope is limited to EU regulations applicable to AI data processing transparency.

KEY WORDS

Artificial Intelligence, Accountability, Algorithmic Transparency, Explainability, Right to Explanation

1. INTRODUCTION

New technologies that blur the distinctions between the *"analogue world"* and the *"digital world"* will have far-fetching effects on many spheres of society, including education, industry, politics, and the arts. The notion of an emerging *"digital ecosystem"* in which decision-making centres are migrating to automated and intelligent systems is described by some as the fourth industrial revolution.[1] These new models use AI and machine learning algorithms that can process vast datasets, learn from experience, and solve complex problems that were once considered exclusively human abilities.[2] However, this shift towards algorithmic decision-making also poses risks to fundamental civil liberties, as opaque systems undermine public trust in the fairness and legality of the choices ultimately made.[3] Experts in fields such as psychology and education are working to address the challenge of making algorithmic decisions more scrutable and open to

[1] Schwab, K. (2017) *The fourth industrial revolution*. Crown Publishing Group, New York.

[2] Brynjolfsson, E. and Mitchell, T. (2017) What can machine learning do? Workforce implications. *Science*, 358(6370), pp. 1530-1534. see also, Data Guidance. (2022) *Norway - Data Protection Overview*. [online] Available from: `https://www.dataguidance.com/notes/norway-data-protection-overview` [Accessed 5 September 2023].

[3] Pasquale, F. (2015) *The Black Box Society: The Secret Algorithms That Control Money and Information*, Harvard University Press, Massachusetts, p.320.

public examination.[4] For instance, in February 2020, a Dutch court banned the government from using the SyRI system, which detected welfare fraud by combining various data,[5] because authorities refused to disclose the source code.[6] New technologies that blur the distinctions between the *"analogue world"* and the *"digital world"* will have far-fetching effects on many spheres of society, including education, industry, politics, and the arts. The notion of an emerging *"digital ecosystem"* in which decision-making centres are migrating to automated and intelligent systems is described by some as the fourth industrial revolution.[7] These new models use AI and machine learning algorithms that can process vast datasets, learn from experience, and solve complex problems that were once considered exclusively human abilities.[8] However, this shift towards algorithmic decision-making also poses risks to fundamental civil liberties, as opaque systems undermine public trust in the fairness and legality of the choices ultimately made.[9]

Experts in fields such as psychology and education are working to address the challenge of making algorithmic decisions more scrutable and open to public examination.[10] For instance, in February 2020, a Dutch court banned the government from using the SyRI system, which detected welfare fraud by combining various data,[11] because authorities refused to disclose the source code.[12]

---

4 Burrell, J. (2016) How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society*, 3(1).

5 Meek, C. (2022) *Artificial Intelligence in The Age of Algorithmic Transparency.* [online] Les Echos. Available from: `https://www.americangreetings.job.com/news/artificial-intelligence-in-the-age-of-algorithmic-transparency/` [Accessed 12 August 2023].

6 Court of The Hague. (2020, February 5). SyRI legislation in conflict with higher law. Rechtspraak.nl. [online] Available from: `https://uitspraken.rechtspraak.nl/\#!/details?id=ECLI:NL:RBDHA:2020:1878` [Accessed 1 August 2023].

7 Schwab, K. (2017) *The fourth industrial revolution*. Crown Publishing Group, New York.

8 Brynjolfsson, E. and Mitchell, T. (2017) What can machine learning do? Workforce implications. *Science*, 358(6370), pp. 1530-1534. see also, Data Guidance. (2022) *Norway - Data Protection Overview*. [online] Available from: `https://www.dataguidance.com/notes/norway-data-protection-overview` [Accessed 5 September 2023].

9 Pasquale, F. (2015) *The Black Box Society: The Secret Algorithms That Control Money and Information*, Harvard University Press, Massachusetts, p.320.

10 Burrell, J. (2016) How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society*, 3(1).

11 Meek, C. (2022) *Artificial Intelligence in The Age of Algorithmic Transparency.* [online] Les Echos. Available from: `https://www.americangreetings.job.com/news/artificial-intelligence-in-the-age-of-algorithmic-transparency/` [Accessed 12 August 2023].

12 Court of The Hague. (2020, February 5). SyRI legislation in conflict with higher law. Rechtspraak.nl. [online] Available from: `https://uitspraken.rechtspraak.nl/\#!/details?id=ECLI:NL:RBDHA:2020:1878` [Accessed 1 August 2023].

The notion of *"algorithmic accountability"* is based on the premise that understanding how machines work enables appropriate oversight.[13] The goal of algorithmic transparency is to ensure that computational processes are accurate and unbiased, which becomes increasingly difficult as algorithms become more complex.[14] However, opaque *"black box"* techniques[15] are being employed in diverse high-stakes decisions about credit, employment, education, government benefits, border-control, surveillance, and even sports stadium monitoring, often with unfair and unexplainable outcomes even to the organizations deploying them.[16]

The primary challenge is to protect the right to informational self-determination while preventing algorithmic harm to individuals and society.[17] Demands for *"traceability"* of automated decisions arise from AI's expanding real-world impacts. More broadly, transparency obligations address the *"opacity of the algorithms"*, which neither users nor designers sufficiently comprehend.[18] Privacy advocates, researchers, and policymakers have raised concerns[19] regarding the inscrutable nature of how machine learning systems categorize new inputs and derive predictions.[20]

Legal frameworks such as the EU's General Data Protection Regulation (GDPR) provide starting points for discovering applicable rules even when AI is involved in processing personal data.[21] GDPR enables algorithmic impact assessments through provisions around evaluating effects on personal information rights. It also mandates strict transparency requirements,

[13] Diakopoulos, N. (2016) Accountability in Algorithmic Decision-Making. *Communications of the ACM*, 59(2), pp. 56-62.

[14] Ananny, M., and Crawford, K. (2018) Seeing Without Knowing: Limitations of The Transparency Ideal and Its Application to Algorithmic Accountability. *New Media & Society*, 20(3), pp. 973-989.

[15] Chaudhary, G. (2020), Artificial Intelligence: The Liability Paradox, *ILI Law Review*, p. 144.

[16] O'Neil, C. (2017) *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York: Crown Publishers. See also Pasquale, F. (2015) *The Black Box Society: The Secret Algorithms That Control Money and Information*, Harvard University Press, Massachusetts, p.320.

[17] Mittelstadt, B. D. et al. (2016) The ethics of algorithms: Mapping the debate. *Big Data & Society*, 3(2).

[18] Burrell, J. (2016) How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society*, 3(1).

[19] Lepri, B. et al. (2018) Fair, transparent, and accountable algorithmic decision-making processes. *Philosophy & Technology*, 31(4), pp. 611-627.

[20] Mitrou, L. (2018) Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'? [online] *Tilburg: TILT Law & Technology Working Paper Series* Available at SSRN: `https://ssrn.com/abstract=3386914` or `http://dx.doi.org/10.2139/ssrn.3386914`[Accessed 28 August 2023]; *see also* Wischmeyer, T. (2020) Artificial Intelligence and Transparency: Opening the Black Box. In: Wischmeyer, T. et.al. (eds) *Regulating Artificial Intelligence*, Switzerland, pp. 75-101.

[21] Goodman, B. and Flaxman, S. (2016) *EU regulations on algorithmic decision-making and a "right to explanation"*. [preprint] arXiv:1606.08813.

notably that data controllers must inform people about the *"existence of automated decision-making and provide meaningful information*[22] *about the logic involved"*[23]- which implies elucidating the algorithm's basic principles in plain language rather than code.[24] Does the duty explain a computer's decision to fall within this obligation? Once a choice is made, can people whose data have been used ask for an explanation of the AI model's decision-making process? If so, what kind of information should be included in such an explanation? Whether this duty extends to explaining specific decisions of an AI model post hoc remains debated among legal experts and computer scientists.[25]

In the intricate landscape of data protection, the GDPR stands as a pivotal framework governing the handling of personal data.[26] However, it is crucial to note that GDPR primarily concerns itself with personal data, leaving a notable gap in the regulatory framework when it comes to non-personal data. The European Data Strategy, unveiled in 2020, recognizes the significance of harnessing the potential of non-personal data while underscoring the necessity for a regulatory framework to ensure responsible and fair usage (European Commission, 2020).[27] Additionally, various EU member states have initiated efforts to bridge this gap by formulating legislation specific to non-personal data, such as the French Data Protection Act[28] and the German Federal Data Protection Act.[29] These national legislations complement GDPR by extending regulatory oversight to encompass non-personal data, emphasizing the need for

[22] Wachter, S. et al. (2017) Transparent, explainable, and accountable AI for robotics. *Science Robotics*, 2(6), eaan6080.

[23] GDPR §§ Articles 13(2)(f), 14(2)(g).

[24] Meek, C. (2022) *Artificial Intelligence in The Age of Algorithmic Transparency.* [online] Les Echos. Available from: https://www.americangreetings.job.com/news/artificial-intelligence-in-the-age-of-algorithmic-transparency/ [Accessed 12 August 2023].

[25] Wachter, S. et al. (2017) Transparent, explainable, and accountable AI for robotics. *Science Robotics*, 2(6), eaan6080.

[26] European Parliament & Council. (2016). 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). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX\%3A32016R0679 [Accessed 15 January 2024].

[27] European Commission. (2020). European Data Act. https://digital-strategy.ec.europa.eu/en/policies/data-act

[28] France. (2018). Law No. 2018-493 of June 20, 2018, on the Protection of Personal Data. https://www.legifrance.gouv.fr/eli/loi/2018/6/20/JUSX1721380L [Accessed 20 January 2024].

[29] Bundesministerium der Justiz und für Verbraucherschutz. (2017). Federal Data Protection Act (BDSG). https://www.gesetze-im-internet.de/englisch_bdsg/[Accessed 10 January 2024].

a harmonized approach to safeguard all forms of data. This nuanced evolution in legislation reflects a broader global trend, where jurisdictions are grappling with the complexities of data governance, acknowledging the pivotal role non-personal data plays in the digital era. As we navigate this intricate regulatory landscape, it becomes imperative to strike a delicate balance, ensuring the facilitation of innovation while upholding fundamental principles of data protection.

This article examines the transparency and explainability issues surrounding AI, considering the challenges and concerns raised, and situating them in the evolving regulatory landscape. The "*black box*" nature of complex AI models poses transparency and accountability challenges and ultimately, ensuring *"black box"* does not become Pandora's box will require interdisciplinary collaboration between law, computer science, and social sciences to balance innovation, ethics, and human rights. However, opacity also represents a knowledge problem- neither designers nor regulators fully grasp modern algorithmic systems. Advancing research on interpretable machine learning and auditing processes, combined with public education, provides paths to make AI ethical and accountable. This article examines regulation of algorithmic transparency in the EU, specifically provisions under the General Data Protection Regulation (GDPR) and analyses legal debates on whether GDPR mandates 'ex-post' explanations of specific AI decisions. It discusses technical and legal obstacles to transparency such as proprietary interests and data privacy. The notion of 'qualified transparency' is proposed as a nuanced approach involving disclosures tailored to diverse stakeholders. The article argues transparency is essential for accountability but must balance competing values. It recommends ongoing interdisciplinary collaboration to make algorithmic systems interpretable, auditable, and ethical while upholding innovation and human rights. Overall, this article focuses on the regulatory framework around algorithmic transparency and accountability in the EU. It aims to situate analysis of the GDPR's provisions on explainability of AI systems within broader technology ethics and policy discourse. The paper's scope is limited to EU regulations applicable to AI data processing transparency.

2. THE BLACK BOX

The term AI encompasses a broad spectrum[30] of technological advancements designed to emulate human cognition and behaviour.[31] At its core, AI enables machines to learn from data and past experiences, reason through complex problems, and make autonomous decisions.[32] One prevalent technique is deep learning, which uses multi-layered artificial neural networks loosely inspired by biological neural networks. These networks can discern intricate patterns and relationships within massive datasets by adjusting internal parameters during training.[33] Consequently, deep learning models can extract insights from new data by generalizing patterns learned from training data.[34]

The advent of 'Big Data' has amplified both the potential and complexity of AI systems. The sheer volume, velocity, and variety of digital data now available for analysis is unprecedented. However, our capacity to fully comprehend the inner workings of sophisticated AI models remains limited. Their decision-making processes can be as opaque as the human mind.[35] Experts liken unravelling the 'black box' of AI to deciphering neurobiological processes in the brain.[36] We can observe the inputs and outputs of AI systems but lack granular visibility into how interconnected nodes within neural networks produce outputs. Even developers struggle to pinpoint the factors

[30] Samoili, S., Cobo, M.L., et al. (2020) *AI Watch. Defining Artificial Intelligence, Towards an Operational Definition and Taxonomy of Artificial Intelligence*. EUR 30117 EN, Publications Office of the European Union, Luxembourg.

[31] European Commission (2018) *Communication from the Commission to the European Parliament, the European Economic and Social Committee and the Committee of the Regions*. [online] Available from: `https://commission.europa.eu/publications/communication-commission-european-parliament-council-european-economic-and-social-committee-and\_en` [Accessed 5 September 2023].

[32] Samoili, S., Cobo, M.L., et al. (2020) *AI Watch. Defining Artificial Intelligence, Towards an Operational Definition and Taxonomy of Artificial Intelligence*. EUR 30117 EN, Publications Office of the European Union, Luxembourg.

[33] European Commission (2018) *Communication from the Commission to the European Parliament, the European Economic and Social Committee and the Committee of the Regions*. [online] Available from: `https://commission.europa.eu/publications/communication-commission-european-parliament-council-european-economic-and-social-committee-and\_en` [Accessed 5 September 2023].

[34] Data Guidance. (2022) *Norway - Data Protection Overview*. [online] Available from: `https://www.dataguidance.com/notes/norway-data-protection-overview` [Accessed 5 September 2023].

[35] Bathaee, Y. (2018) The Artificial Intelligence Black Box and The Failure of Intent and Causation, *Harvard Journal of Law and Technology*, 31(2), p. 891.

[36] Council of Europe Committee of experts on internet intermediaries (MSI-NET). (2017) *Study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications*. [online] Available from: `https://rm.coe.int/study-hrdimension-of-automated-data-processing-incl-algorithms/168075b94a` [Accessed 5 September 2023].

that hold the greatest weight for any given decision.[37] Thus, AI judgments often emerge from a metaphorical 'black box'[38] devoid of any interpretability or explainability.[39]

As algorithmic decision-making permeates more aspects of daily life, the need to demystify AI's black box becomes increasingly urgent.[40] We are entering an 'Algorithmic Society' where social and economic outcomes hinge on automated systems and agents.[41] AI now extends far beyond the controlled laboratory setting into consequential real-world applications. More individual and collective decisions will depend on algorithmic calculations. Properly implemented, AI can uplift human rights and democratic principles.[42] However, opacity also increases the risks of bias, discrimination, manipulation, violations of due process, and physical harm.[43] Even well-intentioned developers can engrain unfairness within models by training them in incomplete, biased, or unrepresentative data.[44] Without visibility into AI reasoning, auditing the process, remedying harms, and ensuring equitable treatment becomes challenging. Thus, transparency has emerged as an ethical imperative and prerequisite for socially responsible AI deployment.[45]

3. A RIGHT TO EXPLANATION

The critical principle called 'transparency' is one such concept on which GDPR is based.[46] The persons whose data are being used should be clearly informed by the person in charge. The main idea is that people whose data is being processed should be informed about it and, by extension, about

[37] Castelvecchi, D. (2016) Can We Open the Black Box Of AI? *Nature,* 538(7623), p. 20.

[38] Chaudhary, G. (2020), *Artificial Intelligence: The Liability Paradox*, *ILI Law* Review, p. 144.

[39] Pasquale, F. (2015) *The Black Box Society: The Secret Algorithms That Control Money and Information*, Harvard University Press, Massachusetts, p.320.

[40] Ibid.

[41] Balkin, J. (2017) The Three Laws of Robotics in The Age of Big Data, Ohio State Law Journal, 78, p. 1218.

[42] Council of Europe Committee of experts on internet intermediaries (MSI-NET). (2017) *Study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications*. [online] Available from: `https://rm.coe.int/study-hrdimension-of-automated-data-processing-incl-algorithms/168075b94a` [Accessed 5 September 2023].

[43] Ibid.

[44] CNIL. (2021) *How Can Humans Keep the Upper Hand? The Ethical Matters Raised by Algorithms and Artificial Intelligence*. [online] Available from:`https://www.cnil.fr/sites/default/files/atoms/files/cnil\_rapport\_ai\_gb\_web.pdf` [Accessed 5 September 2023].

[45] Ibid.

[46] European Commission. (2018) *Guidelines on Automated Individual Decision-Making and Profiling for The Purposes of Regulation 2016/679 (Wp251rev.01)*. [online] Available from: `https://ec.europa.eu/newsroom/article29/items/612053`[Accessed 5 September 2023].

the risks that come with it so that they can make intelligent decisions and protect their interests.

The data subject has every right to be informed about the data collection being done by the third party or otherwise directly as per the regulations contained within the GDPR, most notably Article 13 and 14. Data controllers must warn individuals about *"the existence of automated decision-making"* and offer *"meaningful information about the logic involved and the expected consequences of such processing"* in accordance with Articles 14(2)(g) and 13(2)(f). Furthermore, people have the right to access their own details and personal data under Article 15(1)(h). Article 22(3) also states that when automated decisions are made, data controllers must *"take appropriate measures to protect the rights, freedoms, and legitimate interests of the data subject, including at least the right to get human intervention from the controller, to express his or her point of view, and to contest the decision"*. Finally, individuals enjoy the right to "specific information" and *"the right to get an explanation of the decision reached after such an [automated] assessment",* all of which are required safeguards for automated processing, under Recital 71 of GDPR.

As per the above discussion, it is clear enough to state that a right to know about the outcome of the correct model or weight and to consider the data used in this situation vests upon the data subject. However, contrary to common opinion, the right to an explanation is not part of natural control. There is a linguistic barrier between the preamble and the articles. The preamble is not binding and cannot provide a right to an explanation in and of itself. Then, is the 'right to explanation' in the GDPR equivalent to the 'right to information'?

First, we must define what it means to 'explain' an automated judgement before deciding whether the GDPR affords persons the right to an explanation.[47] Researchers distinguish between discussing how a system operates in general and explaining how a particular choice was made by or through an AI system. Furthermore, researchers say that to explain how an automated system for making decisions works, one must explain its "*logic, significance, expected consequences, and general functionality*". In contrast, addressing individual decisions necessitates elaborating on the "*reasons and individual circumstances of a specific automated decision*", such as the elements considered, and their relative importance or the case-specific

[47] Burt, A (2020) *Is there a 'right to explanation' for machine learning in the GDPR?* [online] International Association of Privacy Professionals. Available from: `https://iapp.org/news/a/is-there-a-right-to-explanation-for-machine-learning-in-the-gdpr/` [Accessed 5 September 2023].

decision rules defined by the machine.[48] It is also possible to differentiate between explanations by examining the order in which they are given during decision-making. A preliminary declaration is made before automatic selection. Hence, it is only logical that it describes how the system operates. Conversely, ex-post descriptions are provided after an automated decision has already been made and detail the procedure's inner workings and the rationale behind a given conclusion.[49] As a result, the second justification offered for decisions after they have already been made may be the only kind to which a meaningful right to explanation applies.

Part of the theory of law has been critical of the right to explanation.[50] Opponents have made a big deal because this right was intentionally excluded of the final draft of GDPR. Considering the most recent drafts of the GDPR and the feedback received during the trialogue negotiations, the original versions of the draft incorporated stringent protections for profiling and automated decision-making. However, the right to a legally binding explanation of one's decisions was abandoned.[51] In addition, the idea that recitals are legally binding has been questioned. A renowned group of researchers stated that *"Recitals have no positive effect of their own and cannot give rise to legitimate expectations"*.[52] *"In principle, the ECJ does not give effect to recitals written in normative terms"*, experts argue, supporting this view. Recitals can assist in explaining why and how a normative instrument was developed. They can also be used to clarify issues in the legislation to which they pertain, but they lack independent legal authority.[53] The European Court of Justice (ECJ) precedents were used to show that it is not the job of data protection law to determine whether a particular set of findings and evaluations is correct. To prove this, we used the ECJ

[48] Ferretti, A. et.al. (2018) Machine Learning in Medicine: Opening the New Data Protection Black Box. *European Data Protection Law Review,* 4, p322(2018).

[49] Wachter, S. et.al. (2017) Why A Right to Explanation of Automated Decision Making Does Not Exist in The General Data Protection Regulation. *International Data Private Law,* 7, p.81.

[50] European Commission. (2018) *Guidelines on Automated Individual Decision-Making and Profiling for The Purposes of Regulation 2016/679 (Wp251rev.01*). [online] Available from: `https://ec.europa.eu/newsroom/article29/items/612053` [Accessed 5 September 2023].

[51] Wachter, S. et.al. (2017) Why A Right to Explanation of Automated Decision Making Does Not Exist in The General Data Protection Regulation. *International Data Private Law,* 7, p.81.

[52] Klimas, T. and Vaitiukait, J. (2008) The Law of Recitals in European Community Legislation. *ILSA Journal of International and Comparative Law*, 15(1), pp. 65-93.

[53] Baratta, R.14 (2014) Complexity of EU law in the domestic implementing process. In: 19th Quality of Legislation Seminar EU Legislative Drafting: Views from those applying EU law in the Member States. *Brussels: European Commission Service Juridique - Quality of Legislation Team*, 3 July. Available from: `https://ec.europa.eu/dgs/legal\service/seminars/20140703\baratta\speech.pdf` [Accessed 21 June 2023].

case law as an example.[54] The construction methodology of AI systems validates these assertions. For example, explaining how intricate algorithmic decision-making systems operate and the reasons behind the judgments they make is a complex problem from a technical standpoint. The use of such explanations is called into question because it is likely that the data subjects would not receive a significant amount of beneficial information from them.

Today, however, it appears that most academics think this logic is incorrect. Therefore, it would be overly formalistic to dismiss the concept of the right to an explanation only because recitals are not legally enforceable, given the ECJ's consistent treatment of recitals as interpretative aids in its case law.[55] According to experts, recitals, are intended to clarify the interpretation of a legal norm. Even though they cannot act as such a rule, they are given a grey area of the law and are not enforceable. However, they are generally accepted as definitive interpretations of the GDPR in cases of uncertainty. To better understand how the standards of the GDPR should be implemented, consider reading the accompanying recitals. Often, they include language that goes well beyond GDPR due to political compromises made during negotiations. Recitals cannot be used to create new legal requirements; however, it can be challenging to determine what constitutes a legal interpretation of a new law and what does not.[56] Recital 71 is thus not considered superfluous but instead serves a clear purpose in facilitating interpretation and contributing to the determination of positive law.[57] Because the GDPR is collaborative and evolving, researchers who debate the normative character of the recitals risk cutting themselves off from potentially valuable sources of clarification for data subjects as the legislation advances (differentiating between harsher and softer legal instruments). This is because scholars who disagree with the Recitals' normative status argue on a technicality: the need to distinguish between tougher and softer legal instruments.[58]

[54] Wachter, S. et.al. (2017) Why A Right to Explanation of Automated Decision Making Does Not Exist in The General Data Protection Regulation. *International Data Private Law,* 7, p.81.

[55] Brkan, M (2019) Do Algorithms Rule the World? Algorithmic Decision-Making in The Framework of The GDPR And Beyond. *International Journal of Law and Information Technology*, 27(2), pp. 91-121; *see also* Wischmeyer, T (2020) Artificial Intelligence and Transparency: Opening the Black Box. In: Wischmeyer, T. and Rademacher (eds.) *Regulating Artificial Intelligence.* Switzerland: Springer International Publishing, pp. 75-101.

[56] Kaminski, M. (2019) The Right to Explanation, Explained Berkeley Technology Law Journal, 34, p.194.

[57] Selbst, A. and Powles, J. (2017) Meaningful Information and The Right to Explanation. *International Data Privacy Law*, 7, p.235.

[58] Kaminski, M. (2019) The Right to Explanation, Explained Berkeley Technology Law Journal, 34, p.194.

The Article 29 Working Party Guidelines interpret and intend Recital 71 in the same way, stating that it is a necessary and sufficient condition *"conditio sine qua non"* to safeguard the rights of the data subject.[59] GDPR provides an individual with a form of algorithmic due process in the form of a hearing, as explained in the Guidelines.[60] According to the Guidelines, controllers must take necessary precautions to maintain the legitimate interests, freedom, and rights of data subjects,[61] *"including a mechanism for human intervention in defined cases, such as providing a link to an appeals process at the time an automated decision is communicated to the data subject, with agreed timescales and a named contact"*.

Data protection authorities have also raised this human-in-the-loop methodology. The UK's Information Commissioner's Office (ICO) has acknowledged that the rights to intervention and acquire human explanation present new encounters to developers and industry, urging *"Big Data organisations to exercise caution before relying on machine learning decisions that cannot be rationalised in human-understandable terms"*.[62] According to the French Commission (CNIL), *"What seems to matter is the ability to comprehend the general logic underlying the algorithm's operation"*. This emphasis on understanding the algorithm's logic comes at the expense of transparency. Because it must be communicated in words rather than code, this justification needs to be easily understood. The most crucial factor is not that the code is clear but that we understand the algorithm's inputs, outputs, and purpose. This needs to be made clear.[63]

The potential of automated decision-making processes has been acknowledged by the European Parliament as having the potential to revolutionize the data industry in its resolution of new digital services such as chatbots and virtual assistants.[64] However, the Parliament clarifies that

[59] European Commission. (2018) *Guidelines on Automated Individual Decision-Making and Profiling for The Purposes of Regulation 2016/679 (Wp251rev.01)*. [online] Available from: `https://ec.europa.eu/newsroom/article29/items/612053` [Accessed 5 September 2023].

[60] Kaminski, M. (2019) The Right to Explanation, Explained Berkeley Technology Law Journal, 34, p.194.

[61] Art. 22 GDPR and Recital 71.

[62] Information Commissioner's Office (2017) *Big Data, Artificial Intelligence, Machine Learning and Data Protection*. [online] Available from: `https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf` [Accessed 5 August 2023].

[63] *Ibid.*

[64] European Parliament. (2020) *European Parliament Resolution Of 12 February 2020 on Automated Decision-Making Processes: Ensuring Consumer Protection and Free Movement of Goods and Services*. [online] Available from: `https://www.europarl.europa.eu/doceo/document/TA-9-2020-0032\_EN.html` [Accessed 25 June 2023].

"in light of the significant impact it can have on consumers, one should be properly informed about how a system that automates decision-making operates, how to reach a human with decision-making authority, and how the system's decisions can be reviewed and corrected". The resolution emphasizes that these systems must employ high-quality, objective datasets and clear, explicable, and accurate algorithms. Concurrently, automated choice procedures for detecting and correcting flaws should be developed. The Parliament's official stance is that *"humans must always be ultimately responsible for and able to override decisions made using automated decision-making processes"*.

In a technical report published by the Joint Research Centre in a similar vein but with more urgent implications, the significance of 'explainability-by-design' in AI systems may endanger users' fundamental rights.[65] This report asserts that for human oversight to be effective, algorithmic processing must be understandable to the person conducting the evaluation.

GDPR is not the first recent law to approach the issue of algorithmic accountability and transparency. By requiring that the regulations that define such action and its key features be provided to those who seek them, the French Act for the Digital Republic[66] ensures that those impacted by administrative algorithmic choices can obtain an explanation of such decisions. Furthermore, administrative organizations are obligated to report the type and extent of algorithmic processing used in decision-making, the treatment parameters used, and, if applicable, the weights assigned to those considerations.

4. ALGORITHMIC TRANSPARENCY: A PRACTICAL ISSUE

People's right to be informed under the GDPR involves several practical challenges, such as explaining what information should be disclosed and the AI-based decision-making process. Theoretically, the difficulties of the rationalization process of artificial intelligence, particularly unsupervised models,[67] have been emphasised. It is generally agreed that the inherent complexity of the data volume, algorithm modularity, iterative processing, and randomised tiebreaking may pose a formidable cognitive obstacle.[68] Furthermore, the dynamic character of several algorithms seems to contradict the static nature of transparency. Continuous updates and modifications are

---

65 *Ibid.*

66 *Digital Republic Act 2016*, Law No. 2016-132117. France. In French.

67 Wang, P. (2012) Theories of Artificial Intelligence—Meta-Theoretical Considerations. *Atlantis Thinking Machines*, 9, pp. 305–323.

68 Z C Lipton, Z.C. (2018) The Mythos of Model Interpretability. In Machine Learning, The Concept of Interpretability Is Both Important and Slippery. *ACMQueue*, 16(3), p.13.

made to the algorithms, although any transparency disclosure refers only to the current algorithm.[69] Decontextualization is also a technical barrier that, occurs when algorithmic models initially used for one purpose are repurposed for a different purpose and context.[70]

Machine learning, however, is not a monolithic idea; it includes various methodologies, from the tried-and-true (such as decision tree algorithms and linear regression) to the cutting edge (such as various forms of neural networks). The difficulty of establishing an ex-post causal relationship between a particular input and output varies significantly among different methods.[71] Improved accuracy can be seen across the board with Bayesian classifiers, additive models, decision trees, and spare linear models, the likelihood that they will provide models that people can comprehend. These algorithms frequently employ several internal features (i.e., paths, controls, or characteristics) to adequately track and explain their results. Deep learning algorithms build high-dimensional input-based applications, such as speech recognition, picture identification, and natural language processing by using intricate networks across network layers to develop extremely nonlinear correlations among inputs and outputs.[72] As the number of nonlinear parameters a system considers while making a decision grows, it becomes harder for humans to understand the model.

We need to consider at the legal and regulatory obstacles to algorithmic transparency in addition to the technical ones posed by algorithms' inherent flexibility and unpredictability. It is understandable to want to limit the amount of detail that can be provided about models and procedures to protect proprietary information and intellectual property.[73] Data controller competition and security requirements could limit algorithm access.[74] Because it constitutes a non-transferable competitive advantage, companies are unwilling to disclose information about their assets. Similarly, privacy and security professionals stress the dangers of revealing sensitive information about an organisation's inner workings, which could increase

[69] Wischmeyer, T. (2020) Artificial Intelligence and Transparency: Opening the Black Box. In: Wischmeyer, T. et.al. (eds) *Regulating Artificial Intelligence*, Switzerland, pp. 75-101.

[70] Donovan, J., Matthews, J., et al. (2018) *Algorithmic Accountability: A Primer*. [online] Data & Society. Available from: `https://datasociety.net/output/algorithmic-accountability-a-primer/` [Accessed 1 September 2023].

[71] Wischmeyer, T. (2020) Artificial Intelligence and Transparency: Opening the Black Box. In: Wischmeyer, T. et.al. (eds) *Regulating Artificial Intelligence*, Switzerland, pp. 75-101.

[72] Rai, A. (2020) Explainable AI: From Black Box to Glass Box. *Journal of the Academy of Marketing Science*, 48, pp. 137–141.

[73] GDPR. EU (n.d.) *Recital 63, Right of access*. [online] Available from: `https://gdpr.eu/recital-63-right-of-access/` [Accessed 15 July 2023].

[74] Veale, M. et.al. (2018) Algorithms That Remember: Model Inversion Attacks and Data Protection Law. *Philosophical Transactions of the Royal Society A*, 376 (2133).

cyberattacks.[75] Another legal basis for limiting access to information is protecting state secrets and public interests, which must be protected from disclosure to the public.[76] Access to information is often seen as a key issue in the regulation of AI-based systems because it is necessary for external parties, such as regulatory authorities and auditors, to be able to assess the performance and risks of these systems. Without access to information, it is difficult for these parties to understand how the systems work and identify any potential issues or risks. In some cases, access to information may be restricted because of concerns about confidentiality, intellectual property, or national security. In these cases, it may be necessary to find ways to balance the need for access to information with these other considerations. There are also technical challenges that can make it difficult to provide access to information about AI-based systems. For example, some AI systems may be complex and have many components that are difficult to understand or analyse. In addition, there may be issues with data privacy and security that need to be addressed when providing access to information. Overall, access to information is an important issue in the regulation of AI-based systems, and finding ways to ensure that regulatory authorities and other external parties have the necessary access to information will be crucial to the effective oversight and regulation of these systems.[77]

The potential consequences of this new right for the AI sector and the advancement of AI, in general, have also been mentioned as a source of concern. Access to algorithms alone is not sufficient to effectively clarify and comprehend a decision-making process. Therefore, companies require time and expertise to conduct this type of assessment.[78] Owing to the interrelated nature of algorithms and datasets in complex information systems and the potential for errors and biases in models and data to become concealed over time, *"explainability may prove especially disruptive for data-intensive industries"*. Some have argued that the GDPR threatens one of AI's most

[75] Wischmeyer, T. (2020) Artificial Intelligence and Transparency: Opening the Black Box. In: Wischmeyer, T. et.al. (eds) *Regulating Artificial Intelligence*, Switzerland, pp. 75-101.

[76] Burrell, J. (2016) How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms. *Big Data Society*, p.9.

[77] Meek, C. (2022) *Artificial Intelligence in The Age of Algorithmic Transparency.* [online] Les Echos. Available from: `https://www.americangreetings.job.com/news/artificial-intelligence-in-the-age-of-algorithmic-transparency/` [Accessed 12 August 2023].

[78] Ananny, M. and Crawford, K. (2016) Seeing Without Knowing: Limitations of The Transparency Ideal and Its Application to Algorithmic Accountability. *New Media Society*, 20(3), p.975.

beneficial uses by restricting the usage of AI's most desirable characteristics: automation and autonomy.[79]

5. TOWARDS A QUALIFIED TRANSPARENCY

Unlocking the 'black box' does not have to be done just because people are curious. The data subject must comprehend the reasoning behind decisions to pursue undesirable outcomes and what, if anything, could be done differently in the future considering the current decision-making model.[80] Technical data and in-depth analyses of the algorithms may not be helpful.[81] In the framework of meaningful transparency, data subjects may be given access to information on several parts of the algorithmic process at any time.[82] Human participation details, input/output details, data quality (how training data were collected/labelled, source reliability, precision, timeliness), algorithm model/architecture/variables/weights/inference process details are all examples of such things (including the margin of error predicted).[83]

Furthermore, the ability to criticise a decision based on the facts presented is not necessarily related to the need for openness and explanation. These protections are integral to the principles of fairness and responsibility and are essential for creating unbiased and robust AI systems. Thus, algorithmic accountability is a part of algorithmic transparency, the idea that an algorithmic system should employ numerous checks and balances to ensure that the system functions as intended by the human operator. The undesirable results can be pinpointed and fixed.[84] Data controllers are responsible for enforcing specific measures inside their organisations to guarantee adherence to data protection obligations by the principle of accountability. These steps may include using a privacy-by-design system architecture or setting up data protection impact assessments.

[79] Mitrou, L. (2018) Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'? [online] *Tilburg: TILT Law & Technology Working Paper Series* Available at SSRN: https://ssrn.com/abstract=3386914or http://dx.doi.org/10.2139/ssrn.3386914 [Accessed 28 August 2023].

[80] Wachter, S. et.al. (2017) Why A Right to Explanation of Automated Decision Making Does Not Exist in The General Data Protection Regulation. *International Data Private Law*, 7, p.81.

[81] European Commission. (2018) *Guidelines on Automated Individual Decision-Making and Profiling for The Purposes of Regulation 2016/679 (Wp251rev.01).* [online] Available from: https://ec.europa.eu/newsroom/article29/items/612053 [Accessed 5 September 2023].

[82] The Council of Europe (2019).

[83] Kamarinou, D. et.al. (2017) Machine Learning with Personal Data. In: Leenes, R. et.al., (eds) *Data Protection and Privacy: The Age of Intelligent Machines.* Hart: Oxford University Press.

[84] New, J. and Castro, D. (2018) *How Policymakers Can Foster Algorithmic Accountability. [online]* Centre for Data Innovation. Available from: https://datainnovation.org/2018/05/how-policymakers-can-foster-algorithmic-accountability/ [Accessed 18 May 2023].

Decision-makers with access to sensitive information must ensure that no group or individual is subjected to a disproportionate share of the risks or rewards associated with using data-driven decisions. Unless adequate governance structures are developed, there is a rising fear that the opaque nature of algorithmic systems could result in circumstances in which individuals are negatively impacted without resorting to a profound explanation and a rectification procedure.[85]

To meet these stringent standards, the decision-making process, the development of AI systems, and the justification for their deployment must be communicated to stakeholders, documented, and audited.[86] Working Party Guidelines on Article 29, call for a system that makes decisions based on algorithms to be constantly tested and given feedback to stop mistakes, inaccuracies, and unfair treatment. Source code, databases, and technical data may not be accessible to individuals but are accessible to regulatory authorities and other parties.[87] This occurs because the concept of transparency may vary depending on the circumstances. The system's manufacturer or operator performs testing to guarantee that it is accurate and fair. In addition to the aforementioned uses, they also allow the testing of whole subsystems by authorised users, the explanation of algorithmic or operational methods by computer scientists and managers, and the submission of findings to regulatory bodies.[88] None of the parts of an algorithmic system should be treated equally with respect to transparency. The algorithmic system's unique characteristics, the complexity of the situations needing governance, and the goals of the governing body all call for diverse applications of this principle.[89]

Kaminski makes a good point when he says, "*It seems that the GDPR is the closest to creating what Frank Pasquale has called 'qualified transparency'* ",

[85] European Parliament Think Tank. (2019) *EU guidelines on Ethics in Artificial Intelligence: Context and implementation*. [online] Available from:

`https://www.europarl.europa.eu/thinktank/en/document/EPRS\_BRI(2019)640163` [Accessed 5 September 2023].

[86] European Commission. (2018) *Guidelines on Automated Individual Decision-Making and Profiling for The Purposes of Regulation 2016/679 (Wp251rev.01)*. [online] Available from:

`https://ec.europa.eu/newsroom/article29/items/612053`[Accessed 5 September 2023].

[87] European Data Protection Board. (2018) Article 29 Working Party. [online] Available from:

`https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party\_en` [Accessed 1 September 2023].

[88] *Ibid*.

[89] New, J. and Castro, D. (2018) *How Policymakers Can Foster Algorithmic Accountability. [online]* Centre for Data Innovation. Available from: `https://datainnovation.org/2018/05/how-policymakers-can-foster-algorithmic-accountability/` [Accessed 18 May 2023].

which is a scheme of targeted disclosures with *"different levels of depth and scope that are meant for different people"*. In practise, transparency does not just mean telling the public what is happening. It also integrates internal company oversight, regulatory oversight, and communication with affected parties. Each of these disclosures may have a distinct character or level of depth. For instance, a board of directors may have access to the full source code, whereas individuals may only have quick, uncomplicated summaries of the information.[90]

The pursuit of transparency can stem from simple curiosity in some cases. However, its true value lies in empowering individuals to comprehend the reasoning behind decisions that negatively impact them. This understanding allows them to question the decision advocate for change and contribute to the development of more accountable and transparent AI systems. Nevertheless, merely granting access to technical details and complex algorithms might overwhelm and prove unhelpful for most people.[91]

As a result, the notion of "qualified transparency" emerges as a nuanced approach. It suggests offering varying degrees of transparency based on the needs and comprehension levels of stakeholders. This approach aligns with calls, for 'meaningful transparency', which goes beyond mere technical disclosures and focuses on providing users with actionable insights.[92]

Tailored Transparency for Diverse Stakeholders:

- **Data Subjects:** Individuals directly affected by algorithmic decisions should have access to clear explanations of the outcome, the factors that influenced it, and the potential for bias. This could involve summaries of the data used, the decision-making process, and the associated risks and limitations.

- **Regulators and Auditors:** Regulatory bodies tasked with overseeing algorithmic fairness and compliance require deeper access to technical details, including algorithm architecture, training data quality, and testing methodologies. This enables them to effectively assess potential risks and ensure adherence to regulations.

[90] Kaminski, M. (2019) The Right to Explanation, Explained *Berkeley Technology Law Journal*, 34, p.194.

[91] Chaudhary, G. (2023) Explainable Artificial Intelligence (xAI): Reflections on Judicial System. *Kutafin Law Review*, 10(4), pp. 872-889. https://doi.org/10.17803/2713-0533.2023.4.26.872-889.

[92] Rai, A. (2020) Explainable AI: from black box to glass box. *Journal of the Academy of Marketing Science*, 48, pp. 137–141. https://doi.org/10.1007/s11747-019-00710-5

- **Internal Stakeholders:** Developers, engineers, and managers responsible for designing and maintaining the algorithm need comprehensive access to the inner workings of the system. This allows them to identify and address issues, improve performance, and ensure responsible development practices.

Transparency Mechanisms:

Several mechanisms can be implemented to achieve qualified transparency:

- **Explainable AI (XAI) techniques:** These techniques can provide human- understandable explanations of how algorithms arrive at decisions, making them more interpretable for non-technical audiences.
- **Interactive dashboards and visualizations:** Interactive interfaces can allow users to explore data, understand how different factors influence outcomes, and identify potential biases.
- **Algorithmic impact assessments:** Conducting regular assessments can help identify and mitigate potential negative impacts of algorithms on specific groups or individuals.[93]
- **Clear and accessible communication:** Providing clear and concise communication to users about how their data is used, what decisions are made based on it, and how they can exercise their rights is crucial for building trust and transparency.

While transparency is essential for fostering trust and accountability in AI systems, it must be balanced with other important values such as privacy, security, and intellectual property. For instance, disclosing sensitive trade secrets or user data could have negative consequences. Therefore, it is crucial to carefully consider the potential risks and benefits of transparency before implementing any specific measures.[94]

Qualified transparency, achieved through targeted disclosures and appropriate mechanisms, is not just about satisfying curiosity but about empowering individuals, ensuring fairness, and fostering responsible AI development. By providing the right information to the right stakeholders, we can build AI systems that are not only effective but also accountable and trustworthy.

---

[93] Selbst, A.D. (2021) An Institutional View of Algorithmic Impact Assessments. *Harvard Journal of Law & Technology*, 35(1).

[94] Katyal, S.K. (2022) Democracy & Distrust in an Era of Artificial Intelligence. *Daedalus*, 151(2), pp. 322-334. doi:10.1162/daed_a_01919.

6. THE WAY FORWARD

There is little doubt that this discussion regarding AI transparency and explainability will continue for a considerable time, as AI systems still need to tackle numerous difficulties. The biggest obstacle is switching from 'black box' to 'glass box' models without halting creativity. Every person or group, whether private or public, plays an integral part in this process. Many scientific projects are ongoing in Explainable AI (XAI).[95] Computer scientists have been focussing a lot of their recent work on figuring out the reasons behind decisions made by artificial intelligence, investigating techniques, and developing built-in tools that can perform these tasks and explain them in a way that humans can understand.

Moreover, data processors and controllers must employ particular organisational and technical safeguards[96] to ensure compliance with GDPR standards. It is anticipated that implementing data protection impact assessments (DPIAs) in high-risk activities will dramatically affect AI research and application.[97] The goal of adopting a "*risk-based approach*" to data protection—which includes DPIAs—is to shift the focus from managing data processing to managing risks associated with that processing.[98] Even if the term "*high-risk threshold*" is not precise, most AI and ML applications likely fall under the processing category requiring a DPIA.[99] As a result, DPIAs should be conducted by both the private and public sectors before creating and implementing AI systems and computerised decision-making methods to foresee and prepare for potential risks to human beings. It is also crucial to determine what national supervisory agencies or courts will say about these DPIAs and how they will rule, and how data controllers in different business sectors will interpret and implement the principles of openness and explainability in their DPIAs.

---

[95] Data Guidance. (2022) *Norway - Data Protection Overview*. [online] Available from: https://www.dataguidance.com/notes/norway-data-protection-overview [Accessed 5 September 2023].

[96] Information Commissioner's Office (2017) *Big Data, Artificial Intelligence, Machine Learning and Data Protection*. [online] Available from: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf [Accessed 5 August 2023].

[97] Mitrou, L. (2018) Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'? [online] *Tilburg: TILT Law & Technology Working Paper Series* Available at SSRN: https://ssrn.com/abstract=3386914 or http://dx.doi.org/10.2139/ssrn.3386914 [Accessed 28 August 2023].

[98] *Ibid.*

[99] Information Commissioner's Office (2017) *Big Data, Artificial Intelligence, Machine Learning and Data Protection*. [online] Available from: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf [Accessed 5 August 2023].

On the other hand, regulators and policymakers are anticipated to play an essential role in developing AI. Already, there are calls for policymakers to get involved and technology-specific laws to be enacted. In addition, it is planned to create a regulatory body for algorithmic decision-making whose job will be to develop the standards by which we can distinguish between safe and harmful AI systems. Algorithmic decision-making system providers should also be held to strict and transparent obligations, such as publicising the source code of their systems.[100]

In this approach, regulation is crucial for developing AI because it promotes transparency and openness, reduces disparities and errors, and delivers legal certainty to individuals. On the other hand, many rules or oversights could add to bureaucracy, slow down the development of technology, and make it take longer for artificial intelligence products to be commercially sold. Governments must strike a balance between stifling creativity and the digital revolution, protecting citizens' rights, and addressing unintended consequences. To achieve this objective, policymakers must abandon conventional regulatory frameworks, revaluate current methods, and explore alternative models such as collaborative, hybrid, outcome-based self-regulation, and co-regulation.

6.1. EUROPEAN UNION'S AI ACT

As part of its digital strategy, the European Union has enacted pioneering legislation regulating AI to promote responsible development and adoption of this transformative technology. The new AI Act establishes a risk-based framework that imposes varying obligations on AI providers and users. Although many systems present minimal risk, assessment is required. Adoption of the AI Act represents a momentous decision, constituting the first regulatory regime governing much-discussed AI innovations promising to revolutionize society. Passage was uncertain until the final days, as the French, German, and Italian governments advocated substituting the legislation with a less stringent AI code of conduct. Their rationale was that minimizing compliance burdens for European companies would better position them to compete internationally. However, legislators rejected this path, judging that balanced regulation would also compel global firms to meet the Act's standard's as well. In their assessment, this would enable fairer market competition. With this trailblazing law, Europe asserts leadership in directing AI toward ethical evolution and alignment with societal priorities.

[100] European Parliament Think Tank. (2019) *Understanding algorithmic decision-making: Opportunities and challenges.* [online] Available from:

`https://www.europarl.europa.eu/thinktank/en/document/EPRS\_STU(2019)624261` [Accessed 28 August 2023].

In line with this objective, the Act's definition of AI systems aligns with internationally recognized criteria from OECD guidelines, which characterize such systems as follows:[101]

> "Machine-based systems that, based on explicit or implicit objectives, make inferences from received inputs to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments."

The expansive breadth of AI's potentially disruptive reach underscores the need for judicious governance, with the exception of certain domains such as national defence, military, and scientific research, which require tailored policies that balance innovation against ethical risks.

A fiercely debated exception to the AI Act's broad regulatory ambit pertains to systems built on free and open-source software. However, the tightly circumscribed scope of the said exception renders it applicable almost solely to private, non-commercial AI applications. Specifically, the free and open-source software waiver does not apply

- **1.** If the AI system is either
  (a) for high-risk use-case,
  (b) falls under prohibited uses, or
  (c) is a use-case with transparency requirements,[102] and
- **2.** If the free and open-source software licensed system furnishes extensive documentation of its model architecture, training methodology, and other technical particulars, it limits its legal duties to providing said summaries and adhering to copyright strictures. However, the exemption becomes void upon the system's commercial deployment or professional commissioning i.e., it is "made available on the market" or "put into service".

[101] OECD. AI-Principles overview - OECD.AI. The OECD Artificial Intelligence Policy Observatory - *OECD.AI*. [online] Available from: `https://oecd.ai/en/ai-principles` [Accessed 3 February 2024].

[102] European Parliament (2023) EU AI Act: first regulation on artificial intelligence. [online] Available from: `https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence` [Accessed 5 December 2023].

Regardless of whether an AI system qualifies for free and open source software exemptions, those exemptions no longer apply if the system is categorized as GPAI with systemic risks.[103]

A governance framework is implemented for general purpose artificial AI systems and foundation models. General-purpose AI refers to an AI system capable of adaptable functionality across multiple domains. Governance considerations also extend to the integration of general-purpose AI capabilities into supplementary high-risk architectures. Foundation models constitute expansive AI architectures adept at undertaking a diverse range of tasks including video, text, and image generation, lateral natural language processing, mathematical computation, and computer code synthesis.[104]

The AI Act emphasizes safeguarding fundamental rights and promoting transparency, mandating human rights impact evaluations for high-risk AI architectures, including those deployed in the insurance and banking sectors. General purpose AI systems carrying systemic risk implications must meet additional requirements[105]

i. *Risk Management*: Entities must conduct rigorous model assessments harnessing state-of-the-art audit protocols and instruments.

ii. *Red Teaming*: Exhaustive adversarial evaluations must be undertaken and documented thoroughly to unveil and mitigate systemic hazards.

iii. *Cybersecurity*: Robust cybersecurity defences for both the AI model and the supporting physical infrastructure must be instituted.

iv. *Energy Consumption*: Obligatory tracking, logging, and public disclosure of actual or projected energy consumption by the model.

In addition, providers must adhere to Union copyright legislation, integrate technological solutions as necessary, and furnish a comprehensive inventory detailing training data used for model development. Presumably,

[103] Gibney, E. (2024) What the EU's tough AI law means for research and ChatGPT. *Nature*. https://doi.org/10.1038/d41586-024-00497-8.

[104] Süme, O. (2023) The proposed regulation of AI Foundation models and General Purpose AI under the draft European AI Act. [online] *Fieldfisher*. Available from: https://www.fieldfisher.com/en/insights/the-proposed-regulation-of-ai-foundation-models-and-generative-purpose-ai [Accessed 5 February 2024].

[105] Article 6, Classification Rules for High-Risk AI Systems. *EU AI Act* [Online] Available from: https://www.euaiact.com/article/6\#:\textasciitilde:text=An\%20AI\%20system\%20intended\%20to,that\%20product\%20pursuant\%20to\%20above [Accessed 17 February 2024].

the AI Act's recitals shall explicitly delineate that the requisite training data inventories need not enumerate discrete data points, as this would prove excessively onerous.

In addition, compulsory registration in a European database is mandated, which in tandem with the disclosure of materials used for AI system development noted previously, could engender substantial litigation. Specifically, copyright and privacy laws may provide grounds for legal challenges by right holders of content leveraged by AI architectures regarding usage impropriety.

Regarding governance and conformity, the AI Act establishes a European AI Office for oversight of sophisticated AI architectures. A scientific panel and advisory forum will be constituted to assimilate diverse stakeholder insights, enabling continuously informed, contemporary regulatory approaches attuned to AI progress.

However, delegating authority between centralized and localized entity incubates the debate. Specifically, national and local bodies may resist ceding influence per GDPR precedent. While the AI Office may mitigate inconsistent EU-wide approaches, political friction between disparate local authorities persists as a risk.

Finally, these models must approach artificial intelligence that prioritises humans. This implies that they must place human values at the centre of the design, deployment, use, and monitoring of AI systems. These systems will ensure the protection of all fundamental human rights. Respect for human dignity, which claims that every person possesses a distinct and unchangeable moral standing, is the foundation of all these rights.[106] Given recent technological advances with as-yet-unknown or unclear effects for individuals and society, our ethical and legal mission is to find a mechanism to cast light on 'black boxes' in such a system following the Protagorean dictum "*man is the measure of all things*".[107]

7. CONCLUSION

Algorithmic transparency is an indispensable element of the responsible AI development and also very effective usage. With AI still making an impact across many areas of the life, the critical question remains of how

[106] European Parliament Think Tank. (2019) *EU guidelines on Ethics in Artificial Intelligence: Context and implementation*. [online] Available from: `https://www.europarl.europa.eu/thinktank/en/document/EPRS\_BRI(2019)640163` [Accessed 5 September 2023].

[107] Protagoras. (2016.) *Testimonia, Part 2: Doctrine*. [online] Available at: `https://www.loebclassics.com/view/protagoras-doctrine/2016/pb\_LCL531.43.xml` [Accessed 12 February 2022].

these systems decide. Accountability and fairness are underpinned by the understanding the decision making. The crucial aspect of transparency in the AI systems is very much especially noticed in the sensitive areas like employment and also criminal justice, where unfair and biased decisions may cause a huge consequent.

With the GDPR in place, a data controller is now required to prioritize its transparency and structure while giving the people a right to explain the how automated decisions are made. Nevertheless, such transparency mechanism should be in place, and the explanation of the AI system should be defined by the whom is the target audience. GDPR is a landmark in the road for the ensuring the transparency in AI systems, but it is not the whole answer. There is a need for a country-wide accountability regime for algorithms, which entails the data controllers putting in checks and balances to make sure that all the data processing and algorithm systems adhere to the provisions of the applicable data privacy regime.

One of the crucial problems in creating and implementing AI systems is the so-called 'black box issue'. The opaqueness and the unintelligibility of AI systems may result in a lot of bias, discrimination, and also other disadvantageous behaviours. The responsibility for the establishment of meaningful checks and balances lies on the data controllers to be adhered to all the data processing and also algorithmic systems that will conform to the applicable privacy standards. Transparency and explainability of the algorithms is about a fairness for the users, it is not only an individual issue, but a part of a larger accountability framework for the algorithms.

The chances of getting a fair outcome without algorithmic transparency are slim in fields like employment and criminal justice. Racial and unfair decisions could be devastating to individuals and the entire society. Transparency issue in the AI systems can also create the problem of untrustworthiness in the AI systems, which can consequently, hold back the development and use of these systems.

The lawmakers and regulators need to develop means of privacy safeguards for citizens while not hampering technological advancements. The 'black box' issue solves differently as technology advances and will remain the main concern. Hence, it is necessary to make sure that more efforts are made to support the concepts of transparency and accountability of such systems to make sure that they are used in the right manner.

Transparency of algorithms is one of the most essential features of the responsible AI design and application. It is of paramount importance to understand the need for transparency in AI in these sensitive areas, where the implications of biased or discriminatory decisions can have grave

consequences, like employment and criminal justice. The GDPR is a very important soft measure to usher in transparency in AI systems, but not the entire solution on its own. There should be a wider accountability regime for algorithms, in which data controllers would have the right to ensure that there are check and balance mechanisms for all data processing and algorithmic systems that they control, and that these align with the privacy framework. The black box problem is the greatest issue while developing the AI systems and deploying the AI systems which should be always paid attention to and we should improve the transparency and accountability of AI systems in order to be sure that they are being used ethically and effectively.

LIST OF REFERENCES

[1] Ananny, M., and Crawford, K. (2018) Seeing Without Knowing: Limitations of The Transparency Ideal and Its Application To Algorithmic Accountability. *New Media & Society*, 20(3), pp. 973-989.

[2] Balkin, J. (2017) The Three Laws of Robotics in The Age of Big Data, Ohio State Law Journal, 78, p. 1218.

[3] Baratta, R.14 (2014) Complexity of EU law in the domestic implementing process. In: 19th Quality of Legislation Seminar EU Legislative Drafting: Views from those applying EU law in the Member States. *Brussels: European Commission Service Juridique - Quality of Legislation Team*, 3 July. Available from: `https://ec.europa.eu/dgs/legal\_service/seminars/20140703\_baratta\_speech.pdf` [Accessed 21 June 2023].

[4] Bathaee, Y. (2018) The Artificial Intelligence Black Box and The Failure of Intent and Causation, *Harvard Journal of Law and Technology*, 31(2), p. 891.

[5] Brkan, M (2019) Do Algorithms Rule the World? Algorithmic Decision-Making in The Framework of The GDPR And Beyond. *International Journal of Law and Information Technology*, 27(2), pp. 91-121

[6] Brynjolfsson, E. and Mitchell, T. (2017) What can machine learning do? Workforce implications. *Science*, 358(6370), pp. 1530-1534. see also, Data Guidance. (2022) *Norway - Data Protection Overview*. [online] Available from: `https://www.dataguidance.com/notes/norway-data-protection-overview` [Accessed 5 September 2023].

[7] Burrell, J. (2016) How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society*, 3(1).

[8] Burt, A (2020) *Is there a 'right to explanation' for machine learning in the GDPR?* [online] International Association of Privacy Professionals. Available from: `https://iapp.org/news/a/is-there-a-right-to-explanation-for-machine-learning-in-the-gdpr/` [Accessed 5 September 2023].

[9] Castelvecchi, D. (2016) Can We Open the Black Box Of AI? *Nature*, 538(7623), p. 20.

[10] Chaudhary, G. (2020), Artificial Intelligence: The Liability Paradox, *ILI Law Review*, p. 144.

[11] Chaudhary, G. (2023) Explainable Artificial Intelligence (xAI): Reflections on Judicial System. *Kutafin Law Review*, 10(4), pp. 872-889. https://doi.org/10.17803/2713-0533.2023.4.26.872-889.

[12] CNIL. (2021) *How Can Humans Keep the Upper Hand? The Ethical Matters Raised by Algorithms and Artificial Intelligence*. [online] Available from: https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_ai_gb_web.pdf [Accessed 5 September 2023].

[13] Council of Europe Committee of experts on internet intermediaries (MSI-NET). (2017) *Study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications*. [online] Available from: https://rm.coe.int/study-hrdimension-of-automated-data-processing-incl-algorithms/168075b94a [Accessed 5 September 2023].

[14] Court of The Hague. (2020, February 5). SyRI legislation in conflict with higher law. Rechtspraak.nl. [online] Available from: https://uitspraken.rechtspraak.nl/\#!/details?id=ECLI:NL:RBDHA:2020:1878 [Accessed 1 August 2023].

[15] Data Guidance. (2022) *Norway - Data Protection Overview*. [online] Available from: https://www.dataguidance.com/notes/norway-data-protection-overview [Accessed 5 September 2023].

[16] Diakopoulos, N. (2016) Accountability in Algorithmic Decision-Making. *Communications of the ACM*, 59(2), pp. 56-62.

[17] *Digital Republic Act 2016*, Law No. 2016-132117. France. In French.

[18] Donovan, J., Matthews, J., et al. (2018) *Algorithmic Accountability: A Primer*. [online] Data & Society. Available from: https://datasociety.net/output/algorithmic-accountability-a-primer/ [Accessed 1 September 2023].

[19] European Commission (2018) *Communication from the Commission to the European Parliament, the European Economic and Social Committee and the Committee of the Regions*. [online] Available from: https://commission.europa.eu/publications/communication-commission-european-parliament-council-european-economic-and-social-committee-and_en [Accessed 5 September 2023].

[20] European Commission. (2018) *Guidelines on Automated Individual Decision-Making and Profiling for The Purposes of Regulation 2016/679 (Wp251rev.01)*. [online] Available from: https://ec.europa.eu/newsroom/article29/items/612053 [Accessed 5 September 2023].

[21] European Data Protection Board. (2018) Article 29 Working Party. [online] Available from:

[22] European Parliament Think Tank. (2019) *EU guidelines on Ethics in Artificial Intelligence: Context and implementation*. [online] Available from: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2019)640163 [Accessed 5 September 2023].

[23] European Parliament Think Tank. (2019) *Understanding algorithmic decision-making: Opportunities and challenges*. [online] Available from:

[24] European Parliament. (2020) *European Parliament Resolution Of 12 February 2020 on Automated Decision-Making Processes: Ensuring Consumer Protection and Free Movement of Goods and Services*. [online] Available from: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0032_EN.html [Accessed 25 June 2023].

[25] Ferretti, A. et.al. (2018) Machine Learning in Medicine: Opening the New Data Protection Black Box. *European Data Protection Law Review*, 4, p.322.

[26] GDPR §§ Articles 13(2)(f), 14(2)(g).

[27] GDPR. EU (n.d.) *Recital 63, Right of access*. [online] Available from: https://gdpr.eu/recital-63-right-of-access/ [Accessed 15 July 2023].

[28] Goodman, B. and Flaxman, S. (2016) *EU regulations on algorithmic decision-making and a "right to explanation"*. [preprint] arXiv:1606.08813.

[29] Information Commissioner's Office (2017) *Big Data, Artificial Intelligence, Machine Learning and Data Protection*. [online] Available from: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf [Accessed 5 August 2023].

[30] Kamarinou, D. et.al. (2017) Machine Learning with Personal Data. In: Leenes, R. et.al., (eds) *Data Protection and Privacy: The Age of Intelligent Machines*. Hart: Oxford University Press.

[31] Kaminski, M. (2019) The Right to Explanation, Explained Berkeley Technology Law Journal, 34, p.194.

[32] Katyal, S.K. (2022) Democracy & Distrust in an Era of Artificial Intelligence. Daedalus, 151(2), pp. 322-334. doi:10.1162/daed_a_01919.

[33] Klimas, T. and Vaitiukait, J. (2008) The Law of Recitals in European Community Legislation. *ILSA Journal of International and Comparative Law*, 15(1), pp. 65-93.

[34] Lepri, B. et al. (2018) Fair, transparent, and accountable algorithmic decision-making processes. *Philosophy & Technology*, 31(4), pp. 611-627.

[35] Meek, C. (2022) *Artificial Intelligence in The Age of Algorithmic Transparency.* [online] Les Echos. Available from: https://www.americangreetings.job.com/news/artificial-intelligence-in-the-age-of-algorithmic-transparency/ [Accessed 12 August 2023].

[36] Mitrou, L. (2018) Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'? [online] *Tilburg: TILT Law & Technology Working Paper Series* Available at SSRN: https://ssrn.com/abstract=3386914 or http://dx.doi.org/10.2139/ssrn.3386914 [Accessed 28 August 2023].

[37] Mittelstadt, B. D. et al. (2016) The ethics of algorithms: Mapping the debate. *Big Data & Society*, 3(2).

[38] New, J. and Castro, D. (2018) *How Policymakers Can Foster Algorithmic Accountability. [online]* Centre for Data Innovation. Available from: https://datainnovation.org/2018/05/how-policymakers-can-foster-algorithmic-accountability/ [Accessed 18 May 2023].

[39] O'Neil, C. (2017) *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York: Crown Publishers.

[40] Pasquale, F. (2015) *The Black Box Society: The Secret Algorithms That Control Money and Information*, Harvard University Press, Massachusetts, p.320.

[41] Protagoras. (2016.) *Testimonia, Part 2: Doctrine*. [online] Available at: https://www.loebclassics.com/view/protagoras-doctrine/2016/pb_LCL531.43.xml [Accessed 12 February 2022].

[42] Rai, A. (2020) Explainable AI: from black box to glass box. Journal of the Academy of Marketing Science, 48, pp. 137–141. https://doi.org/10.1007/s11747-019-00710-5

[43] Samoili, S., Cobo, M.L., et al. (2020) *AI Watch. Defining Artificial Intelligence, Towards an Operational Definition and Taxonomy Of Artificial Intelligence*. EUR 30117 EN, Publications Office of the European Union, Luxembourg.

[44] Schwab, K. (2017) *The fourth industrial revolution*. Crown Publishing Group, New York.

[45] Selbst, A. and Powles, J. (2017) Meaningful Information and The Right to Explanation. *International Data Privacy Law*, 7, p.235.

[46] Veale, M. et.al. (2018) Algorithms That Remember: Model Inversion Attacks and Data Protection Law. *Philosophical Transactions of the Royal Society A*, 376 (2133).

[47] Wachter, S. et al. (2017) Transparent, explainable, and accountable AI for robotics. *Science Robotics*, 2(6), eaan6080.

[48] Wachter, S. et.al. (2017) Why A Right to Explanation of Automated Decision Making Does Not Exist in The General Data Protection Regulation. *International Data Private Law,* 7, p.81.

[49] Wang, P. (2012) Theories of Artificial Intelligence—Meta-Theoretical Considerations. *Atlantis Thinking Machines*, 9, pp. 305–323.

[50] Wischmeyer, T (2020) Artificial Intelligence and Transparency: Opening the Black Box. In: Wischmeyer, T. and Rademacher (eds.) *Regulating Artificial Intelligence.* Switzerland: Springer International Publishing, pp. 75-101.

[51] Z C Lipton, Z.C. (2018) The Mythos of Model Interpretability. In Machine Learning, The Concept of Interpretability Is Both Important and Slippery. *ACMQueue*, 16(3), p.13.

<<< ARTICLES

COMMENTS >>>

DOI 10.5817/MUJLT2024-1-5

ONLINE PLATFORMS AND LEGAL RESPONSIBILITY: A CONTEMPORARY PERSPECTIVE IN VIEW OF THE RECENT U.S. DEVELOPMENTS

by

GERGELY GOSZTONYI * FERENC GERGELY LENDVAI †

This paper critically examines the relevance of Section 230 of the Communications Decency Act in the context of recent United States Supreme Court rulings, specifically Twitter v. Taamneh and Gonzalez v. Google. The Supreme Court ruled in 2023 that determining the extent of CDA230's immunity lies with legislators, not the judiciary. This study explores the potential liability of algorithms in supporting terrorism and the implications for European regulations under the Digital Services Act. Findings indicate that while CDA230 has fostered internet growth, it also challenges content regulation. The United States approach contrasts with the European Union's more explicit service provider responsibilities, suggesting a need for legislative updates to balance free expression with the control of harmful content.

KEY WORDS

US, SCOTUS, CDA, Internet, Liability, Google, Twitter

* Habil. Associate Professor of Law, ELTE Law School, Budapest. He is supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences and the ÚNKP-23-5 New National Excellence Program of the Ministry for Culture and Innovation from the source of the National Research, Development and Innovation Fund

† PhD Candidate, Pázmány Péter Catholic University, Budapest. He is supported by the Rosztoczy Foundation and the ÚNKP-23-3 New National Excellence Program of the Ministry for Culture and Innovation from the source of the National Research, Development and Innovation Fund, lendvaigergely@me.com.

"We really don't know about these things. You know, these are not like the nine greatest experts on the internet."[1]
(Elena Kagan, Justice of the Supreme Court of the United States of America, 2023)

1. LIABILITY FOR INTERNET CONTENT IN THE UNITED STATES OF AMERICA

In the context of the nascent Internet in the 1990s in the United States (hereinafter: U.S.), based on early court practice,[2] many online platforms asked themselves whether it was worth moderating the uploaded content since if they did not do so, they were not a publisher but merely a distributor and were exempt from liability. However, this contradicted the need to curb the spread of problematic content on the Internet, as the lack of law and liability would have perpetuated the Wild West (or, in Alfred C. Yen's words, "western frontier"[3]). This dilemma has been resolved by an amendment to the U.S. Telecommunications Act, as was proposed by Republican Chris Cox and Democrat Ron Wyden.[4] This amendment introduced new regulation in a significantly changed online communications environment, and those twenty-six short words have entirely rewritten the history of the Internet.[5] Inserted into Title V of the Telecommunications Act (commonly known as the Communications Decency Act, or CDA) as Section 230(c)(1) (hereinafter: CDA230),[6] stating that "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."

In contrast to the U.S., the European Union chose a slightly different path of liability regulation in Article 14 of the Electronic Commerce Directive of

---

1 Seddiq, O. (2023) *Supreme Court justices aren't the 9 greatest experts on the internet, Elena Kagan said as they heard a major tech case.* [online] New York: Insider. Available from: https://www.businessinsider.com/supreme-court-google-tech-social-media-section-230-justices-internet-2023-2 [Accessed 13 June 2024].

2 *Cubby, Inc. v. Compuserve Inc.* (1991) 776 F. Supp. 135; *Stratton Oakmont, Inc. v. Prodigy Servs.* (1995) N.Y. Sup. Ct. May 24.

3 Yen, A. C. (2002) Western Frontier or Feudal Society? *Berkeley Technology Law Journal*, 17(4), p. 1210. Available from: https://doi.org/10.2139/ssrn.322522.

4 For details, see Cox, C. (2020) *The Origins and Original Intent of Section 230 of the Communications Decency Act*. [blog entry] 27 August. Richmond: Journal of Law & Technology. Available from: https://jolt.richmond.edu/2020/08/27/the-origins-and-original-intent-of-section-230-of-the-communications-decency-act [Accessed 13 June 2024].

5 Kosseff, J. (2019) *The 26 Words That Created the Internet*. New York: Cornell University Press. Available from: https://doi.org/10.7591/9781501735783.

6 Although Section 230 is part of the Telecommunications Act, it is referred to in legal and common practice as CDA230, referring to Chapter V (Communications Decency Act). Pub. L. No. 104-104 (Tit. V), 110 Stat. 133 (Feb. 8, 1996).

2000 followed and replaced in that aspect in Article 4–6 of the Digital Services Act (hereinafter: DSA) of 2022.[7] These rules "use a threefold set of definitions, the first two of which ('mere conduit' and 'caching') give service providers similar immunity from liability as under the US system."[8] Article 6 of DSA also sets up rules for a third category, the hosting providers. Under this, the hosting provider is in principle liable for the content hosted on it and is exempted from liability if:

(a) does not have actual knowledge of illegal activity or illegal content and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or illegal content is apparent; or

(b) upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the illegal content.

Although, Tambiama Madiega noted that the European "jurisprudence on online liability today remains very fragmented",[9] it could be commented that platform providers mostly prefer to remain passive, losing the possibility of immunity from liability if they are active. In that question, the European Court of Human Rights's practice is particularly significant, in that it consciously seeks to establish more generally applicable tests that can assist parties as well as national enforcers.[10]

Based on the European-U.S. liability differences, it is worth examining where U.S. case law is heading on this question and whether there are any issues that are worthy of European attention. As the tech giants are primarily American but provide their services worldwide, European case law must pay attention to American legislation and case law in this particular matter.

In essence, the broad wording of CDA230 has enabled the development of the internet and all the exponential growth we have seen over the past two decades, as it has "enabled internet startups and their investors to populate their platforms with content from ordinary users without having to take legal responsibility for the content written by users."[11] In doing so, the legislator has made a significant contribution to the development of the internet but

---

7 Church, P. and Pehlivan, C.N. (2023) The Digital Services Act (DSA): A New Era for Online Harms and Intermediary Liability. *Global Privacy Law Review*, 4(1), pp. 53-59. Available from: https://doi.org/10.54648/gplr2023005.

8 Gosztonyi, G.: *Censorship from Plato to Social Media. The Complexity of Social Media's Content Regulation and Moderation Practices*. Cham: Springer Nature Switzerland AG, p. 53. Available from: https://doi.org/10.1007/978-3-031-46529-1.

9 Madiega, T. (2020) *Reform of the EU liability regime for online intermediaries. Background on the forthcoming Digital Services Act*. Brussels: European Union, Summary.

10 *Delfi AS v Estonia* (2015). No. 64569/09, §§ 144-161, ECHR 16 June 2015; *Magyar Tartalomszolgáltatók Egyesulete and Index.hu Zrt. v Hungary* (2016). No. 22947/13, § 70, ECHR 2 February 2016; *Pihl v Sweden* (2017). No. 74742/14, § 31, ECHR 9 March 2017.

11 Reynolds, M. (2019) *The strange story of Section 230, the obscure law that created our flawed, broken internet*. [online] San Francisco: Wired. Available from:

has also addressed some of the major problems of our time. Indeed, if service providers considered that a user or a piece of content was not in their interest, they could remove it legally.[12] Even though these companies have grown to unimaginable economic power,[13] CDA230 gives them almost unlimited immunity[14] – whether they restrict or users upload inappropriate content.

Several court rulings have questioned this immunity in recent years,[15] which has led to a heated public debate about the amendment of CDA230. One example of this was then President Donald Trump's signing into law of the Fight Against Online Sex Trafficking Act (FOSTA),[16] which created an exemption to CDA230. Under the FOSTA, CDA230 cannot be invoked if the content gives rise to civil or criminal liability for conduct promoting or facilitating sex trafficking or prostitution. Still, the Act has been criticised by many for 'watering down' the basic rules of CDA230.[17]

Platforms have also set up what appear to be their own courts (such as Facebook's Oversight Board[18]) or have otherwise tried to contribute to resolving the situation themselves (such as Twitter's BlueSky initiative). In a 2020 letter from William P. Barr, the U.S. Attorney General suggested that the framework for immunity should be clarified so that platforms "cannot use

https://www.wired.co.uk/article/section-230-communications-decency-act [Accessed 13 June 2024].

[12] This is the case for the defence known only as 'good Samaritan' (CDA230(c)(2)), i.e. good faith. However, this has resulted in a paradox, as platform providers prefer to remain passive because they lose the possibility of immunity from liability if they are active. Interestingly, in the Gonzalez case before SCOTUS, Judge Ketanji Brown Jackson suggested that U.S. courts should put more emphasis on the interpretation of CDA230(c)(2), which they have failed to do so far.

[13] Birch, K. and Bronson, K. (2022) Big Tech. *Science as Culture*, 31(1), pp. 1-14. Available from: https://doi.org/10.1080/09505431.2022.2036118.

[14] For safe harbours liability, see Riordan, J. (2016) *The Liability of Internet Intermediaries*. New York: Oxford University Press, pp. 377-409. Available from: https://doi.org/10.1093/oso/9780198719779.003.0012.

[15] *Force v. Facebook, Inc* (2019) 934 F.3d 53, 64 (2d Cir. 2019), cert. denied, 140 S. Ct. 2761 (2020); *Marshall's Locksmith Serv. Inc. v. Google, LLC* (2019) 925 F.3d 1263, 1267; *Enigma Software Grp. U.S.A v. Malwarebytes, Inc.* (2019) 946 F.3d 1040, 1052 (9th Cir. 2019), cert. denied, 141 S. Ct. 13, 208 L. Ed. 2d 197 (2020).

[16] Allow States and Victims to Fight Online Sex Trafficking Act of 2017 (the Act is often referred to as the FOSTA/SESTA Act in the United States, as an earlier version was known as the Stop Enabling Sex Traffickers Act (SESTA).

[17] Albert, K., Armbruster, E., Brundige, E., Denning, E., Kim, K., Lee, L., . . . Yang, Y. (2021) FOSTA in legal context. *Columbia Human Rights Law Review*, 52(3), pp. 1084-1158.; Ballon, i. C. (2020) *E-Commerce and Internet Law: Legal Treatise with Forms*. Los Angeles: Glasser LegalWorks.

[18] For more details, see Lendvai, G.F. (2023) "Pure Rat Country" – Reflections on Case Decision 2022-001-FB-UA of Facebook Oversight Board (Knin Cartoon Case). *Journal of Digital Technologies and Law*, 19(3); Mazur, J. and Grambličková, B. (2023) New Regulatory Force of Cyberspace: The Case of Meta's Oversight Board. *Masaryk University Journal of Law and Technology*, 17(1). Available from: https://doi.org/10.5817/MUJLT2023-1-1.

CDA230 as a shield to censor lawful speech in bad faith in ways inconsistent with their own user policies."[19] It is almost thirty years since the U.S. legislation was adopted, but the internet has changed significantly. The threshold for entry has changed, the number of users has changed, the amount of content uploaded has changed, and the technological environment has changed with it. However, the legislation remained unaltered in the previous decades. Thus, one question that needs to be answered is whether the case law must fill in the gaps in the broad wording of CDA230 or whether the politicians will clarify the rules.

On this issue, the Supreme Court of the United States of America (hereinafter: SCOTUS) took a clear position in 2023: it is not for the courts to determine the extent of the immunity provided by CDA230. This was the conclusion reached by SCOTUS in two cases that many expected to set new paths in Internet regulation and fundamentally change the liability regime that we now see as typical in the democratic part of the world. Campaigners for reconsidering CDA230 were looking forward to the SCOTUS' decision with great expectations. At the same time, tamperers feared that an over-radical decision would lead online platforms to over-removal[20] of content uploaded to them, i.e. to censorship. The significant media publicity surrounding the cases has also given rise to a new narrative that if the SCOTUS rules in favour of the plaintiffs, it could effectively "break the internet" and end freedom of expression on the internet.[21] On the latter, Google's general counsel Halimah DeLaine Prado, in a short but heated opinion piece, explicitly stresses that "if SCOTUS were to change the widely accepted application of CDA230, it would result in a digital experience – for everyone – that reflects the exact opposite of Congress' legislative intent. It would impede access to information, limit free expression, hurt the economy, and leave consumers more vulnerable to harmful online content."[22]

[19] Barr, W. P. (2020) Letter to the President of the United States. [online] Washington DC: U.S. Department of Justice. Available from: `https://www.justice.gov/file/1319346/download` [Accessed 13 June 2024].

[20] See *Delfi AS v. Estonia* (2015). No. 64569/09, § 67, ECHR 16 June 2015: "err on the side of caution to avoid possible subsequent liability".

[21] Millhiser, I. (2023) *The Supreme Court appears worried it could break the internet*. [online] New York: Vox. Available from: `https://www.vox.com/politics/2023/2/21/23608851/supreme-court-gonzalez-google-section-230-internet-twitter-facebook` [Accessed 13 June 2024].

[22] Prado, H. D. (2023) *Gonzalez v Google and the future of an open, free and safe internet*. [blog entry] 12 January. Mountain View: Google. Available from: `https://blog.google/outreach-initiatives/public-policy/gonzalez-v-google-and-the-future-of-an-open-free-and-safe-internet/` [Accessed 13 June 2024].

2. TWITTER, GOOGLE, AND THE ISIS

In the mid-2000s, the Islamic State (ISIS[23]) was seen as a real threat.[24] At the time, the Sunni jihadist organisation sought to increase its relevance by carrying out terrorist attacks beyond its borders, which also gave it significant media coverage.[25] ISIS has also carried out attacks in Europe, the most notable of which was the mass attack on the Bataclan Theatre in Paris.[26] However, smaller attacks have also resulted in numerous casualties, such as the attacks on the Paris bistro in 2015, which coincided with the Bataclan massacre, or the Istanbul nightclub[27] in 2017. The victims of these terrorist actions were not only European citizens, and the families of two victims have filed a lawsuit that also investigated the responsibility of the major social media platforms.

A woman of U.S. nationality, Nohemi Gonzalez, was killed in the Paris bistro attack, while a man of U.S.-Jordanian nationality, Nawras Alassaf, was killed in the Reina nightclub in Istanbul. The families of both victims have taken the matter to court, citing the U.S. Counterterrorism Act, and have asked a U.S. court to declare that Twitter[28] and Google[29] should be held liable for allowing content on their platforms that was linked to international terrorism.

---

[23] Islamic State of Iraq and Syria (hereinafter: ISIS). It should be noted that in the summer of 2014, ISIS renamed itself the Islamic State (IS) and declared its intention to establish a global caliphate rather than a local one. In the present study, as in the analysed SCOTUS decisions, we use the more popular ISIS acronym.

[24] Fenwick, H. (2016). Responding to the ISIS threat: extending coercive non-trial-based measures in the Counter-Terrorism and Security Act 2015. *International Review of Law Computers & Technology*, 30(3). Available from: https://doi.org/10.1080/13600869.2016.1145870.

[25] For the terrorist propaganda in social media, see Wakeford, L. and Smith, L. (2020) Islamic State's Propaganda and Social Media: Dissemination, Support, and Resilience. In: Baele, S. J., Boyd, K. A. and Coan, T. G. (eds.) *ISIS Propaganda: A Full-Spectrum Extremist Message, Causes and Consequences of Terrorism*. New York: Oxford University Press, pp. 155-187. Available from: https://doi.org/10.1093/oso/9780190932459; Shehabat, A. and Mitew, T. (2018) Black-Boxing the Black Flag: Anonymous Sharing Platforms and ISIS Content Distribution Tactics. *Perspectives on Terrorism*, 12(1), pp. 81-99.; Lieberman, A.V. (2017) Terrorism, the Internet, and Propaganda: A Deadly Combination. *Journal of National Security Law & Policy*, 9(1), pp. 95-124.

[26] Pacelli, D., Ieracitano, F. and Rumi, C. (2019) The dimensions of fear in the storytelling of European terrorism: the case of Bataclan. In: Baygert, N., Durin, E., Le Moing-Maas, É. and Nicolas, L. (eds.) *La communication européenne, une scène de combats? Positionnements politiques et enjeux médiatiques*. Bruxelles: La Charte Professional Publishing.

[27] McKirdy, E., Yan, H. and Lee, Ian (2017) *Istanbul attack: ISIS claims nightclub shooting; killer still at large*. [online] Atlanta: CNN. Available from: `https://edition.cnn.com/2017/01/02/europe/turkey-nightclub-attack/index.html` [Accessed 13 June 2024].

[28] *Twitter, Inc. et. al. v. Taamneh et al.* (2023) 598 U.S. ___.

[29] *Gonzalez et al. v. Google, LLC* (2023) 598 U.S. ___.

In their request, the families argued that these service providers could be held liable under the secondary liability provisions[30] of the U.S. Anti-Terrorism Act.[31] Section 2333(a) of the Act states:

> *"Any national of the United States injured in his or her person, property, or business by reason of an act of international terrorism, or his or her estate, survivors, or heirs, may sue therefor in any appropriate district court of the United States and shall recover threefold the damages he or she sustains and the cost of the suit, including attorney's fees."*[32]

Another subsection of the Act provides that "liability may be asserted as to any person who aids and abets, by knowingly providing substantial assistance, or who conspires with the person who committed such an act of international terrorism."[33]

The Taamneh family argued that Twitter and other companies knew that their platforms were playing an essential role in ISIS's terrorist efforts yet failed to take steps to remove illegal content from the platforms. In the other case, the Gonzalez family based their argument on the fact that Google facilitated ISIS recruitment by allowing ISIS to post videos inciting violence and recruiting potential ISIS members on YouTube[34] and by recommending ISIS videos to users through its algorithms. In addition, they argued that CDA230's immunity for platforms could not apply in cases where the platform was active, i.e. it has not acted as a sole distributor but as a publisher. Their arguments suggest this was the case here, as the platforms developed the code for the algorithm-driven targeted recommendations. In particular, the applicants' legal argument in neither case blamed the platforms for carrying out the specific attacks, but the families merely requested to establish the secondary liability based on a particular context. In both cases, the defendant's argument was similar: CDA230's immunity extends fully to the platforms, as they acted only as distributors, i.e. they had no role in producing the content. Google's lawyer, Lisa Blatt, later said, "Helping users find the proverbial needle in the haystack is a fundamental need on the Internet."[35]

---

[30] The legislation was inserted into the original text of the Justice Against Sponsors of Terrorism Act of 2015, Pub. L. 114-222 (hereinafter: JASTA).

[31] Antiterrorism Act (hereinafter: ATA), 18 U.S.C. Chapter 113B.

[32] 18 U.S.C. § 2333(a) (2015).

[33] 18 U.S.C. § 2333(d)(2) (2015).

[34] Google LLC has owned YouTube LLC since 2006 and both companies have been under the umbrella of Alphabet Inc. since 2015.

[35] Howe, A. (2023) *'Not, like, the nine greatest experts on the internet': Justices seem leery of broad ruling on Section 230*. [blog entry] 21 February. Bethesda: SCOTUSblog. Available from: `https://www.scotusblog.com/2023/02/not-like-the-nine-greatest-`

As a result of the proceedings in the lower courts,[36] the two cases – which are legally similar in a fundamental sense – raised different issues by the time they reached SCOTUS. In the Gonzalez case, the Court had to decide whether CDA230 covered algorithm-driven recommender systems and whether the Ninth Circuit Court of Appeals (USCNC) was correct in holding that the algorithms of the major online platforms operate in a neutral manner, i.e., they recommend content to users based solely on search history and interests.[37] In the Taamneh case, however, SCOTUS had to rule on liability under the ATA and JASTA. The arguments before SCOTUS demonstrated how the legal issues in the two cases are inseparable, and the arguments on both sides of the cases have become confusing. SCOTUS also had to take a position on the so-called chilling effect,[38] as large online platforms are known to receive more and more requests from authoritarian or quasi-authoritarian governments to remove material posted on them.[39]

3. THE LEGAL PROCEDURE

SCOTUS started hearing the two cases together in October 2022, and the decision was handed down on May 18, 2023. The decision was noted by Justice Clarence Thomas, who pointed out that the amount of content being shared and uploaded on the giant platforms was staggering. YouTube, Facebook and Twitter were marked as examples, underlining that the monthly active users on these platforms could reach billions and that hundreds of thousands of pieces of content were uploaded to these platforms every minute.[40] Judge Thomas also indicated that the content created by members and supporters of ISIS who glorified the terrorists who had committed the attacks was harmful and damaging.[41] Concerning the ATA,

---

experts-on-the-internet-justices-seem-leery-of-broad-ruling-on-section-230/ [Accessed 13 June 2024].

[36] *Gonzalez et al. v. Google, LLC* (2021) 18-16700; *Taamneh et al. v. Twitter, Inc. et al.* (2021) 18-17192.

[37] This argument was rejected by Judge Gould in his dissenting opinion because "where the website (1) knowingly amplifies a message designed to recruit individuals for a criminal purpose, and (2) the dissemination of that message materially contributes to a centralized cause giving rise to a probability of grave harm, then the tools can no longer be considered neutral." Judge Gould did not rule out the possibility that an algorithm could be neutral (citing *Carafano v. Metrosplash.com, Inc.* (2003) 339 F.3d 1119, 1123, as an example), but in the present case he found this reasoning unavailing (*Gonzalez et al. v. Google, LLC* (2021) 18-16700, p. 100).

[38] Pech, L. (2021) *The Concept of Chilling Effect. Its untapped potential to better protect democracy, the rule of law, and fundamental rights in the EU*. Brussels: Open Society European Policy Institute.

[39] Jurecic, Q., Rozenshtein, A. Z. and Wittes, B. (2023) *Have the Justices Gotten Cold Feet About 'Breaking the Internet'?* [blog entry] 24 February. Washington DC: Lawfare. Available from: https://www.lawfaremedia.org/article/have-justices-gotten-cold-feet-about-breaking-internet [Accessed 13 June 2024].

[40] *Twitter, Inc. et. al. v. Taamneh et al.* (2023) 598 U.S. ___, pp. 3-4.

[41] *Op. cit.*, p. 5.

SCOTUS also interpreted and ruled on Section 2333(a), stating that the critical issue in the case was to determine whether the platforms, as defendants, knowingly provided substantial assistance to the commission of the terrorist action or, more simply put, whether the distribution of terrorist content could constitute aiding and abetting.[42]

The SCOTUS examined what was meant by aiding and abetting and what Twitter did to aid and abet the terrorists.[43] Here, the SCOTUS recalled, with particular reference to JASTA, the Halberstam case – a leading case on aiding, abetting, and liability for conspiracy.[44] With that case reference, SCOTUS proposed three crucial criteria for establishing aiding and abetting in the Taamneh case. First, the aiding and abetting party must assist in an unlawful activity that causes harm. Second, the party must know that its involvement is part of the illegal activity. Thirdly, the assistance must be substantial in addition to being known. However, Judge Thomas pointed to the fact that assistance is not a "limitless concept" and that the applicability of the Halberstam case was very difficult because of the substantial differences between the facts, thus pointing out that the USCNC had driven an analogy too close between the Taamneh case and the Halberstam case. As a sub-conclusion could be drawn, there were no helpful analogies for the judges to decide in these cases.

The SCOTUS paid even more attention to determining what, if anything, was the activity that Twitter aided and abetted as a potential accomplice. A key segment of Justice Thomas's opinion explained that the plaintiffs' and defendants' arguments were both based on flawed premises. The plaintiffs overly adhered to the Halberstam case and failed to consider that the aiding and abetting, in that case, was established because of being systematic, while the defendants overstated the nexus required by Section 2333(d)(2) between the alleged aiding and abetting and the tort since the accomplice need not have detailed knowledge of the terrorist's plan.[45] Indeed, the correct interpretation, and thus the correct reasoning, would have been for the plaintiffs to prove that Twitter provided such knowing and substantial assistance to ISIS that it could be construed as culpable participation in the Istanbul attack, and the defendant, by implication, the opposite.[46]

According to SCOTUS, the plaintiffs failed to prove that Twitter knowingly and substantially aided and abetted the terrorist attack. Concerning the nature of the content and the algorithms, the opinion

[42] *Op. cit.,* p. 8.
[43] *Ibid*.
[44] *Halberstam v. Welch* (1983) 705 F. 2d 472.
[45] *Twitter, Inc. et. al. v. Taamneh et al.* (2023) 598 U.S. ___, p. 19.
[46] *Op. cit.,* p. 21.

highlighted that although ISIS activists and sympathisers were indeed present on the social media platform, and the algorithmic recommendation system did certainly offer ISIS-related content to users whom the algorithm assumed would be interested in such content, the issue of guilt was not proven.[47] This was upheld by the SCOTUS, although, overall, the fact that the platforms, in most cases, did not exercise a (pro)active attitude to prevent the algorithm from filtering out the recommendation of terrorist content was not in dispute.

Judge Thomas drew a particularly significant analogy in this respect between platforms and earlier technologies, namely mobile phones. For example, is a telephone company liable for having brokered several transactions involving illegal substances via mobile phone?[48] The SCOTUS answered the question in the negative, even though there was no doubt that the telephone call facilitated the transaction. The importance of this example, however, is that the plaintiffs ultimately argue that the algorithms' recommendations constitute "active" assistance, which was not the case, as the plaintiffs have failed to prove that Twitter's algorithms intentionally, knowingly and materially recommended ISIS content knowing that it would or could lead to the Istanbul attack. According to SCOTUS, the algorithms are neutrals, and there was no specific outreach connected with the attack or even ISIS. Concerning platform liability, SCOTUS also indicated that the "plaintiffs identify no duty that would require defendants or other communication-providing services to terminate customers after discovering that the customers were using the service for illicit ends".[49] Moreover, even if such an obligation could be identified, proving that the defendant platforms knowingly failed to act with intent to assist in recommending ISIS content to users would again raise concerns.

The SCOTUS also adopted the USCNC's proposal for the Halberstam framework, now applying it correctly. It pointed out that the USCNC erred in its decision to separate the concepts of knowing and substantial, as the awareness of the tech giants that ISIS content was present on their platforms can only be interpreted as general awareness. It cannot be construed as knowledge of and assistance with a specific, individual act of terrorism. The SCOTUS also underlined that the USCNC had misinterpreted the algorithms as technical means, as algorithmic referral systems were not only exclusively

[47] *Op. cit.*, p. 22.
[48] Cf. *Doe v. GTE Corp* (2003) 347 F.3d (CA7).
[49] *Twitter, Inc. et. al. v. Taamneh et al.* (2023) 598 U.S. ___, p. 25.

available to ISIS militants but to the whole general public.[50] In essence, the plaintiffs have alleged that the defendants generally provided available virtual platforms that ISIS used and that the defendants did not stop ISIS despite knowing that it was using those platforms.[51] This allegation was insufficient to establish a credible correlation between the Reina attack and the recommendation systems. The SCOTUS also agreed with the USCNC, which found no credible evidence that Google intentionally supported and aided ISIS by operating its revenue-sharing system. Overall, the SCOTUS in the case found no connection between the defendants and the Reina attack. In light of the above, the SCOTUS reversed the USCNC's judgment.

This detailed description of the Taamneh case also helps to understand the highly terse (only three pages) per curiam opinion of the SCOTUS in the Gonzalez case, given that the decision was essentially based entirely on the Taamneh case. SCOTUS claimed that in the absence of aiding and abetting, the ruling would have been limited to the sole issue of whether Google was responsible for the terrorist actions committed by ISIS through revenue sharing. At the oral hearing on 21 February 2023, the plaintiffs requested to amend their claims. SCOTUS noted in response that it was not its role to grant such requests; however, the SCOTUS judges found and conceded that the plaintiffs' arguments were not supported by either the USCNC or the above Taamneh decision. Consequently, the SCOTUS did not consider the applicability or even possible modification of CDA230 but vacated the judgment and remanded the case to the USCNC to reconsider the plaintiffs' complaint in light of the Taamneh judgment.[52]

4. CONCLUSION

The international legal press and legal blogs were full of such questions after the ruling: Has SCOTUS crashed the internet? Has an all-overriding, game-changing precedent been set? Can algorithms be used to support acts of terrorism? The answer to all three questions was negative. "As much as the SCOTUS judges disliked the fact that social media platforms encourage users to watch ISIS videos, none of them seemed open to holding Google accountable for trying to create the best search engine possible."[53]

[50] Cf.: „Rather, defendants' relationship with ISIS and its supporters appears to have been the same as their relationship with their billion-plus other users: arm's length, passive, and largely indifferent." *Twitter, Inc. et. al. v. Taamneh et al.* (2023) 598 U.S. ___, p. 24.

[51] *Op. cit.*, pp. 28-29.

[52] *Gonzalez et al. v. Google, LLC* (2023) 598 U.S. ___, p. 3.

[53] Jurecic, Q., Rozenshtein, A. Z. and Wittes, B. (2023) *Have the Justices Gotten Cold Feet About 'Breaking the Internet'?* [blog entry] 24 February. Washington DC: Lawfare. Available from: `https://www.lawfaremedia.org/article/have-justices-gotten-cold-feet-about-breaking-internet` [Accessed 13 June 2024].

SCOTUS' reasoning showed that if the same algorithm that was accepted to recommend cooking videos to people based on their search history and interests recommends terrorist content to other people based on the same search history and interests, it was difficult to hold it accountable.

However, regarding CDA230 and the algorithm relationship, the decisions were undoubtedly prominent as SCOTUS evaluated algorithmic recommendation systems as a method, a neutral tool used by platforms[54] rather than a deliberate activity by the platforms. In this respect, the SCOTUS's conservative and nuanced approach to the relationship between algorithms and CDA230 is to be welcomed – regulating algorithms in a comprehensive, separate regulation[55] is more welcome rather than reforming CDA230 just because platforms use algorithms.

The main question is whether these two decisions would lead to the end of the revision of CDA230, i.e., have the Gonzalez and Taamneh cases closed the "twenty-six words question"? The answer is again negative. It is worth highlighting Texas House Bill 20,[56] which aimed to prevent users from being banned or denied access to platforms because of their views and opinions.[57] Although the law came into force in September 2021, the plaintiff in NetChoice v. Paxton asked that the enforcement be denied.[58] The case is currently before the SCOTUS, as the Fifth Circuit Court of Appeals overturned the federal decision by a 2-1 vote, allowing the Texas law to be applied and enforced. The SCOTUS ruling will undoubtedly be an essential step in the evolution of CDA230, so the end is not close.

Article-19 has hailed the Taamneh and Gonzalez decisions as a significant victory for freedom of expression online,[59] as "the Internet has now become one of the principal means by which individuals exercise their right to

[54] Kenneth, T. and Rubinstein, I. (2023) Gonzalez v. Google: The Case for Protecting "Targeted Recommendations". *Duke Law Journal Online*, 72, p. 197. Available from: https://doi.org/10.2139/ssrn.4337584.

[55] In October 2023, Joe Biden signed an Executive Order to address the problems caused by artificial intelligence. Lendvai, G.F. and Gosztonyi, G. (2024) Deepfake y desinformación. ¿Qué puede hacer el derecho frente a las noticias falsas creadas por deepfake? [in press] Submitted to: *IDP. Revista de Internet, Derecho y Política*.

[56] Texas House Bill 20 (HB20), An Act Relating to censorship of or certain other interference with digital expression, including expression on social media platforms or through electronic mail messages.

[57] Robertson, A. (2021) Texas passes law that bans kicking people off social media based on 'viewpoint'. [online] New York: The Verge. Available from: `https://www.theverge.com/2021/9/9/22661626/texas-social-media-law-hb-20-signed-greg-abbott` [Accessed 13 June 2024].

[58] *NetChoice, LLC v. Paxton* (2022) 49 F.4th 439.

[59] ARTICLE 19 (2023) *United States: clear victory for free speech in the Supreme Court decisions*. [online] London: ARTICLE 19. Available from: `https://www.article19.org/resources/united-states-clear-victory-for-free-speech-in-the-supreme-court-decisions/` [Accessed 13 June 2024].

freedom to receive and impart information and ideas",[60] and any restrictions would jeopardise this. While it may seem that the SCOTUS judges were trying to deflect by stating that their ability to consider the complex technical issues involved was limited because they were not Internet experts, they took the correct legal position. They have decided that the legislators cannot use the judicial system as a proxy to solve the problems instead of them. The SCOTUS decision points to the fact that the fate of CDA230 and the "breaking or regulating giant platforms"[61] is in the hands of nothing but legislators.

LIST OF REFERENCES

[1] Albert, K., Armbruster, E., Brundige, E., Denning, E., Kim, K., Lee, L., Yang, Y. (2020) FOSTA in Legal Context. Columbia Human Rights Law Review, 2021, Vol. 52, No. 3.

[2] Allow States and Victims to Fight Online Sex Trafficking Act of 2017

[3] Antiterrorism Act, 18 U.S.C. Chapter 113B

[4] ARTICLE 19 (2023) *United States: clear victory for free speech in the Supreme Court decisions*. [online] London: ARTICLE 19. Available from: https://www.article19.org/resources/united-states-clear-victory-for-free-speech-in-the-supreme-court-decisions/ [Accessed 13 June 2024].

[5] Ballon, i. C. (2020) *E-Commerce and Internet Law: Legal Treatise with Forms*. Los Angeles: Glasser LegalWorks

[6] Barr, W. P. (2020) Letter to the President of the United States. [online] Washington DC: U.S. Department of Justice. Available from: https://www.justice.gov/file/1319346/download [Accessed 13 June 2024]

[7] Birch, K. and Bronson, K. (2022) Big Tech. *Science as Culture*, 31(1). Available from: https://doi.org/10.1080/09505431.2022.2036118.

[8] *Carafano v. Metrosplash.com, Inc.* (2003) 339 F.3d 1119, 1123.

[9] *Cengiz and Others v. Turkey* (2015). Nos 48226/10 and 14027/11, § 49, ECHR 1 December 2015.

[10] Church, P. and Pehlivan, C.N. (2023) The Digital Services Act (DSA): A New Era for Online Harms and Intermediary

[60] *Cengiz and Others v. Turkey* (2015). Nos 48226/10 and 14027/11, § 49, ECHR 1 December 2015.

[61] Jurecic, Q., Rozenshtein, A. Z. and Wittes, B. (2023) *Have the Justices Gotten Cold Feet About 'Breaking the Internet'?* [blog entry] 24 February. Washington DC: Lawfare. Available from: https://www.lawfaremedia.org/article/have-justices-gotten-cold-feet-about-breaking-internet [Accessed 13 June 2024].

Liability. *Global Privacy Law Review*, 4(1). Available from: https://doi.org/10.54648/gplr2023005.

[11] Communications Decency Act Pub. L. No. 104-104 (Tit. V), 110 Stat. 133 (Feb. 8, 1996)

[12] Cox, C. (2020) *The Origins and Original Intent of Section 230 of the Communications Decency Act*. [blog entry] 27 August. Richmond: Journal of Law & Technology. Available from: `https://jolt.richmond.edu/2020/08/27/the-origins-and-original-intent-of-section-230-of-the-communications-decency-act` [Accessed 13 June 2024].

[13] *Cubby, Inc. v. Compuserve Inc.* (1991) 776 F. Supp. 135.

[14] *Delfi AS v. Estonia* (2015). No. 64569/09, ECHR 16 June 2015.

[15] *Doe v. GTE Corp* (2003) 347 F.3d (CA7).

[16] *Enigma Software Grp. U.S.A v. Malwarebytes, Inc.* (2019) 946 F.3d 1040, 1052 (9th Cir. 2019), cert. denied, 141 S. Ct. 13, 208 L. Ed. 2d 197 (2020).

[17] Fenwick, H. (2016). Responding to the ISIS threat: extending coercive non-trial-based measures in the Counter-Terrorism and Security Act 2015. *International Review of Law Computers & Technology*, 30(3). Available from: https://doi.org/10.1080/13600869.2016.1145870.

[18] *Force v. Facebook, Inc* (2019) 934 F.3d 53, 64 (2d Cir. 2019), cert. denied, 140 S. Ct. 2761 (2020).

[19] *Gonzalez et al. v. Google, LLC* (2021) 18-16700.

[20] *Gonzalez et al. v. Google, LLC* (2023) 598 U.S. ___.

[21] Gosztonyi, G.: *Censorship from Plato to Social Media. The Complexity of Social Media's Content Regulation and Moderation Practices*. Cham: Springer Nature Switzerland AG. Available from: https://doi.org/10.1007/978-3-031-46529-1.

[22] *Halberstam v. Welch* (1983) 705 F. 2d 472.

[23] Howe, A. (2023) *'Not, like, the nine greatest experts on the internet': Justices seem leery of broad ruling on Section 230*. [blog entry] 21 February. Bethesda: SCOTUSblog. Available from: `https://www.scotusblog.com/2023/02/not-like-the-nine-greatest-experts-on-the-internet-justices-seem-leery-of-broad-ruling-on-section-230/` [Accessed 13 June 2024].

[24] Jurecic, Q., Rozenshtein, A. Z. and Wittes, B. (2023) *Have the Justices Gotten Cold Feet About 'Breaking the Internet'?* [blog entry]

24 February. Washington DC: Lawfare. Available from: https://www.lawfaremedia.org/article/have-justices-gotten-cold-feet-about-breaking-internet [Accessed 13 June 2024].

[25] Justice Against Sponsors of Terrorism Act, Pub. L. 114-222

[26] Kenneth, T. and Rubinstein, I. (2023) Gonzalez v. Google: The Case for Protecting "Targeted Recommendations". *Duke Law Journal Online*, 72. Available from: https://doi.org/10.2139/ssrn.4337584.

[27] Kosseff, J. (2019) *The 26 Words That Created the Internet*. New York: Cornell University Press. Available from: https://doi.org/10.7591/9781501735783.

[28] Lendvai, G.F. (2023) "Pure Rat Country" – Reflections on Case Decision 2022-001-FB-UA of Facebook Oversight Board (Knin Cartoon Case). *Journal of Digital Technologies and Law*, 19(3).

[29] Lendvai, G.F. and Gosztonyi, G. (2024) Deepfake y desinformación. ¿Qué puede hacer el derecho frente a las noticias falsas creadas por deepfake? [in press] Submitted to: *IDP. Revista de Internet, Derecho y Política*.

[30] Lieberman, A.V. (2017) Terrorism, the Internet, and Propaganda: A Deadly Combination. *Journal of National Security Law & Policy*, 9(1).

[31] *Magyar Tartalomszolgáltatók Egyesulete and Index.hu Zrt. v Hungary* (2016). No. 22947/13, ECHR 2 February 2016

[32] *Marshall's Locksmith Serv. Inc. v. Google, LLC* (2019) 925 F.3d 1263, 1267.

[33] Mazur, J. and Gramblička, B. (2023) New Regulatory Force of Cyberspace: The Case of Meta's Oversight Board. *Masaryk University Journal of Law and Technology*, 17(1). Available from: https://doi.org/10.5817/MUJLT2023-1-1

[34] McKirdy, E., Yan, H. and Lee, Ian (2017) *Istanbul attack: ISIS claims nightclub shooting; killer still at large*. [online] Atlanta: CNN. Available from: https://edition.cnn.com/2017/01/02/europe/turkey-nightclub-attack/index.html [Accessed 13 June 2024].

[35] Millhiser, I. (2023) *The Supreme Court appears worried it could break the internet*. [online] New York: Vox. Available from: https://www.vox.com/politics/2023/2/21/23608851/supreme-court-gonzalez-google-section-230-internet-twitter-facebook [Accessed 13 June 2024].

[36] *NetChoice, LLC v. Paxton* (2022) 49 F.4th 439.

[37] Pacelli, D., Ieracitano, F. and Rumi, C. (2019) The dimensions of fear in the storytelling of European terrorism: the case of Bataclan. In: Baygert, N., Durin, E., Le Moing-Maas, É. and Nicolas, L. (eds.) *La communication européenne, une scène de combats? Positionnements politiques et enjeux médiatiques*. Bruxelles: La Charte Professional Publishing.

[38] Pech, L. (2021) *The Concept of Chilling Effect. Its untapped potential to better protect democracy, the rule of law, and fundamental rights in the EU*. Brussels: Open Society European Policy Institute.

[39] *Pihl v Sweden* (2017). No. 74742/14, ECHR 9 March 2017.

[40] Prado, H. D. (2023) *Gonzalez v Google and the future of an open, free and safe internet*. [blog entry] 12 January. Mountain View: Google. Available from: https://blog.google/outreach-initiatives/public-policy/gonzalez-v-google-and-the-future-of-an-open-free-and-safe-internet/ [Accessed 13 June 2024].

[41] Reynolds, M. (2019) *The strange story of Section 230, the obscure law that created our flawed, broken internet*. [online] San Francisco: Wired. Available from: https://www.wired.co.uk/article/section-230-communications-decency-act [Accessed 13 June 2024].

[42] Riordan, J. (2016) *The Liability of Internet Intermediaries*. New York: Oxford University Press. Available from: https://doi.org/10.1093/oso/9780198719779.003.0012.

[43] Robertson, A. (2021) Texas passes law that bans kicking people off social media based on 'viewpoint'. [online] New York: The Verge. Available from: https://www.theverge.com/2021/9/9/22661626/texas-social-media-law-hb-20-signed-greg-abbott [Accessed 13 June 2024].

[44] Seddiq, O. (2023) *Supreme Court justices aren't the 9 greatest experts on the internet, Elena Kagan said as they heard a major tech case*. [online] New York: Insider. Available from: https://www.businessinsider.com/supreme-court-google-tech-social-media-section-230-justices-internet-2023-2 [Accessed 13 June 2024].

[45] Shehabat, A. and Mitew, T. (2018) Black-Boxing the Black Flag: Anonymous Sharing Platforms and ISIS Content Distribution Tactics. *Perspectives on Terrorism*, 12(1), pp. 81-99.; Lieberman, A.V. (2017) Terrorism, the Internet, and Propaganda: A Deadly Combination. *Journal of National Security Law & Policy*, 9(1).

[46] *Stratton Oakmont, Inc. v. Prodigy Servs.* (1995) N.Y. Sup. Ct. May 24.

[47] *Taamneh et al. v. Twitter, Inc. et al.* (2021) 18-17192.

[48] Texas House Bill 20 (HB20), An Act Relating to censorship of or certain other interference with digital expression, including expression on social media platforms or through electronic mail messages.

[49] *Twitter, Inc. et. al. v. Taamneh et al.* (2023) 598 U.S. ___.

[50] Wakeford, L. and Smith, L. (2020) Islamic State's Propaganda and Social Media: Dissemination, Support, and Resilience. In: Baele, S. J., Boyd, K. A. and Coan, T. G. (eds.) *ISIS Propaganda: A Full-Spectrum Extremist Message, Causes and Consequences of Terrorism*. New York: Oxford University Press. Available from: https://doi.org/10.1093/oso/9780190932459.

[51] Yen, A. C. (2002) Western Frontier or Feudal Society? *Berkeley Technology Law Journal*, 17(4). Available from: https://doi.org/10.2139/ssrn.322522.

MUJLT Official Partner (Czech Republic)

ROWAN LEGAL, advokátní kancelář s.r.o
https://rowan.legal

Cyberspace 2023 Partners

Zákony pro lidi - AION CS
www.zakonyprolidi.cz

ROWAN LEGAL, advokátní kancelář s.r.o
https://rowan.legal

PricewaterhouseCoopers Česká republika
https://www.pwc.com/cz/

Notes for Contributors

Focus and Scope

Masaryk University Journal of Law and Technology (ISSN on-line 1802-5951, ISSN printed 1802-5943) is a peer-reviewed academic journal which publishes original articles in the field of information and communication technology law. All submissions should deal with phenomena related to law in modern technologies (e.g. privacy and data protection, intellectual property, biotechnologies, cyber security and cyber warfare, energy law). We prefer submissions dealing with contemporary issues.

Structure of research articles

Each research article should contain a title, a name of the author, an e-mail, keywords, an abstract (max. 1 500 characters including spaces), a text (max. 45 000 characters including spaces and footnotes) and list of references.

Structure of comments

All comments should contain a title, a name of the author, an e-mail, keywords, a text (max. 18 000 characters) and a list of references.

Structure of book reviews

Each book review should contain a title of the book, a name of the author, an e-mail, a full citation, a text (max. 18 000 characters) and a list of references.

Structure of citations

Citations in accordance with AGPS Style Guide 5th ed. (Harvard standard), examples:

Book, one author: Dahl, R. (2004) *Charlie and the Chocolate Factory*. 6th ed. New York: Knopf.
Book, multiple authors: Daniels, K., Patterson, G. and Dunston, Y. (2014) *The Ultimate Student Teaching Guide.* 2nd ed. Los Angeles: SAGE Publications, pp.145-151.
Article: Battilana, J. and Casciaro, T. (2013) The Network Secrets of Great Change Agents. *Harvard Business Review*, 91(7) pp. 62-68.
Case: *Evans v. Governor of H. M. Prison Brockhill* (1985) [unreported] Court of Appeal (Civil Division), 19 June.
Citation Guide is available from: https://journals.muni.cz/public/journals/36/download/Citationguide.pdf

Formatting recommendations

Use of automatic styles, automatic text and bold characters should be omitted.
Use of any special forms of formatting, pictures, graphs, etc. should be consulted.
Only automatic footnotes should be used for notes, citations, etc.
Blank lines should be used only to divide chapters (not paragraphs).
First words of paragraphs should not be indented.
Chapters should be numbered in ordinary way – example: "5.2 Partial Conclusions".

Submissions

Further information available at
https://journals.muni.cz/mujlt/about

LIST OF ARTICLES

LIST OF COMMENTS