MASARYK UNIVERSITY JOURNAL OF LAW AND TECHNOLOGY

VOLUME **17** | NUMBER **1** | SUMMER **2023** | 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 **17** | NUMBER **1** | SUMMER **2023**

LIST OF ARTICLES

DOI 10.5817/MUJLT2023-1-1

NEW REGULATORY FORCE OF CYBERSPACE: THE CASE OF META'S OVERSIGHT BOARD *

by

JÁN MAZÚR † BARBORA GRAMBLIČKOVÁ ‡

It's been a few years since Facebook (Meta) instituted its Oversight Board as a new quasi-judicial and regulatory body of one of the most important contemporary cyberspaces. It's long established that social media platforms, such as Facebook, pose certain challenges to democracies as they, among other issues, allow for spread of fake news and hate speech, shift our perception of reality, or create echo chambers. In reaction to talks of regulating similar platforms, Meta's self-regulatory attempt of instituting the Oversight Board appears to tackle the issue of content moderation by the platform itself. As the content moderation is one of the main sources of Meta's problematic reputation (taking down posts, pages of various more or less known persons), the board is potentially significant. The paper analyses the board's mandate, governance structure and procedures. We look at standard elements of independence of decision-making bodies (such as courts) to establish whether the Oversight Board is structured in a way conducive to independent decision making. We conclude that that structure of the Oversight Board fulfils some of the elements of the de jure judicial independence, however there is a room for improvement. Independence of the Oversight Board from Meta is a vital element of the institution, however we detect connections and dependencies on Meta (Meta needs to agree on changes of the Charter as well as the Bylaws, Meta was profoundly involved in the initial selection of the members, etc.). The whole structure of Oversight Board is heavily impacted by the private law institutes – trust, company, contracts – which might not be able to fully facilitate all the needs of an independent quasi-judicial body. The private structure, lacking necessary participatory mechanisms, does not permit

* This work was supported by the Slovak Research and Development Agency under the contract No. 16-0553 (project: "Metamorphoses and innovations of the corporations concept under conditions of globalisation").

† Mgr. Ján Mazúr, PhD., EMPA, jan.mazur@uniba.sk, assistant professor, Department of Financial Law, Faculty of Law, Comenius University in Bratislava, Slovakia

‡ JUDr. Barbora Grambličková, PhD., LLM. (née Czókolyová), barbora.czokolyova@uniba.sk, assistant professor, Department of Commercial Law, Faculty of Law, Comenius University in Bratislava, Slovakia

the Oversight Board to gain necessary legitimacy. We also review the Oversight Board's setup in light of the EU's 2022 Digital Services Act (DSA), which represents one of the most comprehensive regulations of the social media platforms, including content moderation issues. We conclude that the Oversight Board would also not be compliant with requirements set forth in the DSA. After the adoption of the DSA, a question of compatibility of the Oversight Board with the out-of-court dispute settlement bodies opened.

KEY WORDS

Social media platforms; regulation of cyberspace; Digital Services Act; Oversight Board; Meta; disinformation; fake news; purpose of the company; quasi-judicial power

1. CONTEXT

It appears to be superfluous to provide excessive evidence of Facebook's or other massively used social media platforms' (SMP) shortcomings and malfunctions in 2022.[1] A lot has been written about platforms in the popular media and academia.[2] Most recently, media has focused on new revelations by whistleblower Frances Haugen, related to the (in)ability of Meta to stop the platform abuse during highly problematic actions, such as 6/1 insurrection in USA or the Stop the Steal groups and conspiracies, but also to Meta's reluctance to act on inadequacies that even Meta itself recognized.[3] It has been revealed that Meta had done very little to prepare for these kinds of crises; in fact, as Meta's own analysis stated: "*We were not able to act on simple objects like posts and comments because they individually tended not to violate, even if they were surrounded by hate, violence, and misinformation.*"[4]

---

1 We use the term „Facebook" to refer to the social media platform and the term "Meta" to refer to the parent company of both social media platforms Facebook and Instagram. We use the term "Meta" to address the Facebook company even before its renaming to Meta. The Meta's policies related to the Oversight Board do not make any relevant distinction between Facebook and Instagram.

2 For reference on media and academic writings since 2019 see for instance our previous take on the subject: Mazúr, J. and Patakyová, M. T. (2019) Regulatory Approaches to Facebook and Other Social Media Platforms: Towards Platforms Design Accountability. *Masaryk University Journal of Law and Technology* 13(2), pp. 219–42. Available from: `https://doi.org/10.5817/MUJLT2019-2-4`.

3 Redacted version of the disclosure is available at: Whistleblower Aid. (2021) Anonymous Whistleblower Disclosure: Re: Supplemental Disclosure of Securities Law Violations by Facebook, Inc. (NASDAQ: FB), SEC TCR #. Available from: `https://drive.google.com/file/d/1WPOaPE6MyWMdMV9f218nsSjGGrmSjnkw/view`.

4 O'Sullivan, D., Subramaniam, T. and Duffy, C. (2021) Not Stopping "Stop the Steal:" Facebook Papers Paint Damning Picture of Company's Role in Insurrection. *CNN*. Available from: `https://edition.cnn.com/2021/10/22/business/january-6-insurrection-facebook-papers/index.html`.

Meta is probably well aware of the fact that it is the very nature of Meta's product mechanics, such as recommendations, optimizing for engagement, which are the root cause of why massive spreading of hate speech and misinformation takes place. According to the leaked documents, Meta has misled the public about the negative effects its platforms have on children and youth.[5] Content moderation budget is not spread evenly or proportionately among individual countries where Facebook's present – 87% of the content moderation budget is spent in USA.[6] As the documents reveal, the platform has been used as a human trafficking tool. Many of these issues pose a serious problem for Meta under the SEC's rules for publicly traded companies.[7] Meta presents itself as a beacon of freedom of expression, yet it willingly chooses growth over safety, by adopting censorship after government's requests.[8]

In reaction to these shortcomings, there have been numerous calls and proposals for regulation and regulatory actions, including by Mark Zuckerberg himself.[9] Some of these proposals include actions and policies in the field of anti-trust, such as the anti-trust lawsuits and policies in order to break up social media[10], proposals to treat parts of Facebook as a network monopoly[11], or general strengthening of competition law framework.[12] There were also proposals to improve the platforms' content moderation[13],

---

5 Subramaniam, T. (2021) Four Takeaways from Facebook Whistleblower's Complaints. *CNN*. Available from: https://edition.cnn.com/2021/10/06/tech/fb-whistleblower-doc-takeaways/index.html.

6 Subramaniam, T. (2021) the Big Takeaways from the Facebook Papers. *CNN*. Available from: https://edition.cnn.com/2021/10/26/tech/facebook-papers-takeaways/index.html.

7 Duffy, C. (2021) Facebook Has Known It Has a Human Trafficking Problem for Years. It Still Hasn't Fully Fixed It. *CNN*. Available from: https://edition.cnn.com/2021/10/25/tech/facebook-instagram-app-store-ban-human-trafficking/index.html.

8 Dwoskin, E., Newmyer, T. and Mahtani, S. (2021) the Case against Mark Zuckerberg: Insiders Say Facebook's CEO Chose Growth over Safety. *The Washington Post*. Available from: https://www.washingtonpost.com/technology/2021/10/25/mark-zuckerberg-facebook-whistleblower/.

9 Zuckerberg, M. (2019) Opinion: Mark Zuckerberg: the Internet Needs New Rules. Let's Start in These Four Areas. *The Washington Post*. Available from: https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html.

10 Kang, C. (2021) the F.T.C. Asks for an Extension to Refile Its Facebook Antitrust Suit. *The New York Times*. Available from: https://www.nytimes.com/2021/07/23/technology/ftc-facebook-antitrust-lawsuit.html.

11 Zingales, L. (2021) Don't Break Up Social Media, Bifurcate It. *Project Syndicate*. Available from: https://www.project-syndicate.org/commentary/social-media-separate-network-infrastructure-from-editorial-role-by-luigi-zingales-2021-08.

12 This is the case of the recent EU's Digital Services Act package.

13 Electronic Frontier Foundation. (2021) *The Santa Clara Principles on Transparency*

of proposals to open Facebook's and other SMPs' data to researchers.[14] Even more ambitions proposals called for creation of a new regulatory agency with overarching mandate.[15] Perhaps the most prominent and overarching was the long-discussed European Commission's proposal for the Digital Services Act, which became the law in October 2022.[16]

Through the political and academic debates, one proposal related to content moderation issues was actually adopted by Meta itself: the creation of an ultimate content moderator for Facebook and Instagram – the Oversight Board. The Oversight Board is tasked with no lesser purpose but "*to promote free expression by making principled, independent decisions regarding content on Facebook and Instagram and by issuing recommendations on the relevant Facebook Company Content Policy.*"[17] Through this purpose the Oversight Board should effectively serve as the "Supreme Court" of Facebook and Instagram, two of the most important and widely used social media platforms (owned by the parent company Meta).[18] As such, the Oversight Board should provide impartial judgements in some of the wickedest content moderation decisions issued by the platforms.[19] Taking into consideration the number of users of Facebook and Instagram and the fact that the board's jurisdiction is territorially not restricted, it represents seemingly the ultimate quasi-judicial body of the cyberspace, certainly the ultimate content moderator of the largest global public space.

This paper provides an analysis of the jurisdiction of the Oversight Board, its governance structure, including its corporate composition and inner quasi-judicial structure. We undertake a corporate law analysis to discuss

---

and Accountability in Content Moderation. Available from: https://santaclaraprinciples.org.

[14] Hegelich, S. (2020) Facebook Needs to Share More with Researchers. *Nature* 579(7800), pp. 473–473. Available from: https://doi.org/10.1038/d41586-020-00828-5.

[15] Wheeler, T., Verveer, P. and Kimmelman, G. (2020) New Digital Realities; New Oversight Solutions in the U.S. The Case for a Digital Platform Agency and a New Approach to Regulatory Oversight. *The Shorenstein Center on Media, Politics and Public Policy*. Available from: https://shorensteincenter.org/wp-content/uploads/2020/08/New-Digital-Realities_August-2020.pdf.

[16] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). *Official Journal of the European Union* (L277) 19 October. Available from: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX\%3A32022R2065 (hereinafter the "DSA").

[17] Oversight Board. (2022) *The Charter*. Available from: https://oversightboard.com/governance/.

[18] For an in-depth look into the board's origins, see: Klonick, K. (2020) the Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression. *Yale Law Journal* 129, pp. 2418–2499.

[19] Unless stated otherwise in the text, the obligations of the Oversight Board relate to Facebook as well as Instagram, even though we explicitly mention only Facebook.

strengths and vulnerabilities of the structure and compare the structure with typical features of well-functioning judiciary.

The paper is structured as follows. Section 1 deals with the Oversight Board's mission, jurisdiction and powers, wherein we find that the current jurisdiction and capacities remain very limited, following a setup favoring niche decision making (of potentially significant cases). Section 2 provides an overview of the board's governance structure, including its creation and membership. The structure, although clearly setup to minimize Meta's influence on the board's functioning and primarily on its decision making, shows some vulnerabilities, which are discussed in detail. Section 3 deals with the board's decision making and the Meta's undertaking to implement the board's decisions. In the final section 4, we review the interaction of the board's mandate and governance structure with the presumed expectations from similar reviewing bodies as laid out in the DSA.

2. MISSION, JURISDICTION AND POWERS

When discussing the Oversight Board's mission, jurisdiction and powers, it is useful to clearly delineate what the Oversight Board claims to be, what it is and what it does not even have an ambition to be. As the board's charter states the board's overall mission includes promotion of free expression through the means of making decisions regarding content on Facebook and issuing recommendations on the company's content policy. As the board's mandate implies Meta's giving away some of its power over content policing, we may naturally ask what motivates Meta. Several explanations emerge.

First, from idealistic perspective, Meta may seek greater legitimacy of its content policies and reassuring its users that a third (semi-)independent body examines its decisions. Meta may also be interested in enforcing more stringent human rights standards. Second, by establishing a way of self-regulation, Meta may be attempting to stave off potential government regulation. Third, in a more cynical fashion, Meta may also attempt to use the board as a cheap way to achieve public relations points, feeding on the legitimacy of the board members' CVs.[20] Fourth, Meta outsources controversial decisions out of the company, which is not only beneficial from the legitimacy perspective, but also safeguards the company as it may always use the board as a scapegoat.[21]

[20] Applying Max Weber's conceptualization of legitimacy, one could conclude that the Oversight Board's legitimacy is based on the charismatic authority of its members in contrast to legal authority of an institution. See: Weber, M. (2004) the Vocation Lectures. Indianapolis: Hackett Publishing Company. p. 34.

[21] Douek, E. (2019) Facebook's "Oversight Board:" Move Fast with Stable Infrastructure

The board is free to choose cases from those submitted to the board by Meta's platforms' users, but it also hears cases submitted by Meta. Once it reaches a decision Meta's bound to implement it. The board is also tasked to provide recommendations to Meta on its content policy, either upon Meta's request or on its own initiative.

This mandate closely resembles a mandate of judicial body conducting judicial review of administrative decisions in typical functioning democracies.[22] The board's jurisdiction includes Meta's leading cyberspace platforms, Facebook, and Instagram, leaving out private messaging platforms, such as WhatsApp, Messenger, and Instagram Direct.[23] As for geographic outreach, the board's jurisdiction is global, not restricted to any specific region or country.[24]

The board has discretion to choose from requests for review, yet the board is mandated to consider emblematic cases that have the greatest potential to guide future decisions and policies of Meta.[25] The board's discretion is shaped by substantial criteria for selection, a priori set and publicly issued by the board itself.[26]

These criteria include the following: (i) cases that raise important issues pertaining to respect for freedom of expression and other human rights and/or the implementation of Facebook's (platform specific) Community Standards;[27] (ii) cases of critical importance to public discourse, directly or indirectly affecting a substantial number of individuals, and/or raising questions about Meta's policies; (iii) cases reflecting the platforms' user base, ensuring regional and linguistic diversity.[28] (iv) There are also negative eligibility criteria; the board does not review content posted through

---

and Humility. *North Carolina Journal of Law & Technology* 21(1), p. 17; Klonick, K. (2020) *op. cit.*, p. 2426.

22 Jaffe, L. L. (1958) the Right to Judicial Review. *Harvard Law Review* 71(3), p. 401.

23 Also, less known service Oculus is left out of review.

24 As is shown further, this does not mean the board decides cases according to local laws.

25 Oversight Board. (2022) *Op. cit*. The Oversight Board met with exceptionally high demand for appeals from Facebook's users within the first period of the Oversight Board's existence (from October 2020 until December 2021) – over a million requests for review were received by the Oversight Board during this period. See Oversight Board. (2021) *Annual Report*, p. 5.

26 Most recently, the Oversight Board issued its Overarching Criteria for Case Selection in October 2022. The board's priorities include: (i) elections and civic space; (ii) crisis and conflict situations; (iii) gender; (iv) hate speech against marginalized groups; (v) government use of Meta's platforms; (vi) treating users fairly; (vii) automated enforcement of policies and curation of content. See: `https://www.oversightboard.com/governance/`.

27 Meta. *Facebook Community Standards*. Available from: `https://transparency.fb.com/en-gb/policies/community-standards/`.

28 Oversight Board. (2022) *op. cit*.

marketplace, fundraisers, Facebook dating, messages, and spam, nor does it review content on platforms other than aforementioned.

There are also formal (eligibility) criteria set by more detailed Bylaws of the Oversight Board, resembling classic eligibility criteria of typical judicial proceedings:[29] (i) appeals must come from an active account holder, whether from the original poster of content or person who submitted content for review; (ii) Meta must have already reviewed its initial decision; (iii) appeals must be submitted within 15 days from the time Meta sends an update about its final content policy decision.[30]

Furthermore, the review must not be in contradiction with country-specific laws (i. e. country of residence of particular user, or country from which the content was posted) and/or must not potentially trigger a criminal liability or regulatory sanctions of Meta, the board, or its individual members.[31] The same restriction applies when keeping the content could lead to criminal liability or adverse governmental action against Meta, Meta employees, administration or board's members. The review is also not available when the content has been blocked by a valid report of illegality, or where the content is criminally unlawful in a jurisdiction with a connection to the content. The case selection is done by a majority vote of the board's case selection committee.[32]

When critically reviewed, these restrictions do not hold. Douek has argued that Meta follows local rules in content moderation as they may result from legitimate legislative processes within any country.[33] Yet, there have been several instances where Meta yielded to local norms to the detriment of freedom of speech[34] and other instances where Meta overruled local norms by its own moral norms, also to the detriment of freedom of speech.[35] In these cases, Meta prioritized continuation

[29] See also: https://oversightboard.com/appeals-process/.

[30] Art. 3, Sec. 1.1 of the Oversight Board's Bylaws.

[31] Art. 3, Sec. 1.2.2 of the Oversight Board's Bylaws.

[32] In November 2020, the board issued its first rulebook, which is a non-binding, but practical guidance to the board members and administrative staff to facilitate selection of cases for review and make the process more accessible, transparent and predictable. This Rulebook was revised in October 2022. Oversight Board. (2020) *Rulebook for Case Review and Policy Guidance*. Available from: https://oversightboard.com/sr/rulebook-for-case-review-and-policy-guidance.

[33] Douek, E. (2020) *op. cit.*, p. 38.

[34] Pearson, J. (2020) Exclusive: Facebook Agreed to Censor Posts after Vietnam Slowed Traffic - Sources. *Reuters*. Available from: https://www.reuters.com/article/us-vietnam-facebook-exclusive/exclusive-facebook-agreed-to-censor-posts-after-vietnam-slowed-traffic-sources-idUSKCN2232JX.

[35] Jacobs, J. (2019) Will Instagram Ever "Free the Nipple"? *The New York Times*. Available from: https://www.nytimes.com/2019/11/22/arts/design/instagram-free-the-nipple.html.

of its service although it meant censoring political or cultural speech – Meta's commitments to business are reliable, while clearly its commitments to freedom of political or cultural speech are not when they endanger the business interests. Without substantive review of local norms and their alignment with international legal norms following local rules becomes highly problematic and appears to be business-motivated decision to avoid legal problems.[36]

The board is tasked to interpret Meta's Community Standards and other relevant content policies to review the cases and "*determine if decisions were made [by Facebook] in accordance with Facebook's stated values and policies.*"[37] It is clear from the board's founding documents that the venture point of the board's mission is promotion of freedom of expression (on social media). It may at times come at odds with other values, such as authenticity, safety, privacy and dignity. The board is tasked to balance them out, in light of human rights norms protecting free expression.

In its first Annual Report, the Oversight Board stipulated a new challenge in applying international human rights standards to content moderation.[38] The Oversight Board identified that among the sources of authority guiding the Oversight Board's decisions, the Article 19 of the International Covenant on Civil and Political Rights (ICCPR) was the most cited. The ICCPR is a global human rights treaty that Meta voluntarily pledged to respect in its Corporate Human Rights Policy.[39] Thus, the Oversight Board states that the basis of its decisions are not only Meta's rules but international human rights norms as well. Moreover, the Oversight Board already dealt with the case of conflict between Meta's content policies and Meta's human rights responsibilities. The Oversight Board overturned Meta's decision based on its human rights responsibilities, even though the removal of the content in question was in line with the Meta's rules. In the Annual Report, the Oversight Board pledges to prioritize human rights if a conflict emerges between Meta's content policies and its human rights responsibilities.[40]

Moreover, with the adoption of the DSA, the link between the Meta's content policies (incl. Community Standards) and the core EU human rights document – the Charter of Fundamental Rights of the EU – becomes

[36] Facebook's own Community Standards refer to international human rights standards when making judgements regarding moderation of free speech. See: `https://transparency.fb.com/en-gb/policies/community-standards/`.
[37] Oversight Board. (2022) *op. cit.*, Art. 2, p. 4.
[38] Oversight Board. (2021) *op. cit.*, p. 43.
[39] *Op. cit.*, p. 44.
[40] *Op. cit.*, p. 46.

even stronger.[41] The DSA requires in the article 14(4) that the platforms act diligently, objectively and proportionately in applying and enforcing any restrictions in relation to policies, procedures, measures and tools used for content moderation, with due regard to the applicable fundamental rights stipulated by the Charter of Fundamental Rights. In practice, this would require the board to assess content moderation cases in light of the EU human rights law. Similarly, the DSA also provides additional room to draw up relevant codes of conduct in accordance with the Union law, especially in relation to illegal content, but also in other contexts (systemic risks).[42]

Based on the above-mentioned, both the Oversight Board's commitments to apply international human rights norms to content moderation as well as the perspective requirements of the EU to assess content moderation cases in light of the EU human rights laws, put international human rights norms in the center of the decision-making processes of the Oversight Board.

The board decides whether Meta should keep or remove specific content ("*instruction to allow or remove content*"). The board may also instruct Meta to "*uphold or reverse a designation that led to an enforcement outcome.*"[43] The board issues decisions that are binding upon Meta unless their implementing could violate law.[44] It may moreover issue specific recommendations on the Meta's content policies, whether from its own initiative or upon Meta's request.[45] Meta may also ask further questions and seek advice from the board. The charter is very explicit about limiting powers of the board to decision making and recommendations.[46] In course

[41] The DSA makes multiple direct references to the Charter (further as the Charter of Fundamental Rights): recitals 3, 9, 32, 34, 36, 39-41, 47, 51-52, 59, 63, 81, 109, 115, 127, 153, 155, art. 9 (orders to act against illegal content), art. 14 (alignment of platform's terms and conditions with the charter) art. 34 (risk assessment especially in relation to negative effects on fundamental rights in the charter), art. 35 (mitigation of risks on very large online platforms), or art. 36 and 48 (use of crisis protocols must be in line the charter).

[42] Art. 45 of the DSA. This follows up on the previous soft regulations of codes of conduct, such as the 2018 Code of Practice on Disinformation and most recently the 2022 Strengthened Code of Practice on Disinformation. Even though the DSA understands the codes as voluntary self-regulation, the regular monitoring and review of the achievements of the codes' objectives should trigger potential reviews of policies (art. 45(4) of the DSA).

[43] Oversight Board. (2022) *op. cit.*

[44] Based on the Oversight Board's first Annual Report, in 2021, the Oversight Board published 20 decisions, from which 14 decisions of Meta were overturned and 6 upheld. Moreover, from these 20 cases 16 were submitted by the users and 4 by Meta. Oversight Board. (2021) *op. cit.*, p. 22.

[45] Based on the Oversight Board's first Annual Report, in 2021, the Oversight Board made 86 recommendations to Meta and for 2/3 of these recommendations Meta either demonstrated implementation or reported progress. While Meta committed to implement most of the recommendations, the Oversight Board stipulated a new challenge to ensure that Meta turns these commitments into actions. *Op. cit.*, p. 5, p. 54.

[46] Oversight Board. (2022) Art. 1 Sec. 4: „The board will have no authority or powers beyond those expressly defined by this charter."

of reaching decisions, the board may also reasonably request additional information from Meta.

The board is explicitly asked to review Meta's decisions and policies for consistency. The charter provides for precedential value of previous decisions of the board when there are factual similarities of cases and applicability of policies is similar. Although the board has the power to set precedents in reviewing content decisions, the board has no power or direct mandate to *change policies a priori*. It may merely advise, and recommend Meta to change its policies, but the board itself cannot change the law, nor is it allowed to *choose the law*, which would not be in comfort with the Meta's policies. The corporate policy governs the content moderation.

We argue that the board's mandate and jurisdiction are insufficient to deal with complexity of the platforms. Correcting content moderation alone cannot serve as a panacea for the platforms' ills. Even internal documents of Meta recognized that dealing with isolated issues such as individual posts or comments helps little in solving massive spreading of fake news or hoaxes on the platforms and other types of abuses, as they individually do not violate content policies.[47]

Including content policies advisory and recommendations is a nice gesture but does not compare to the real necessity of controlling or at least reviewing the true corporate golden egg: algorithms and overall architecture of the platform. Only by allowing a (semi-)independent body to review the platform's algorithms and architecture, based on independently reviewed data on the platform's use, can there be a proper discussion on how to balance corporate interests in high-traffic of low quality content without alignment to truth, and values of democracy, such as dignity. Clearly, the board has no mandate to deal with these topics, which is its main shortcoming.[48]

3. GOVERNANCE STRUCTURE

This section deals with governance structure of the Oversight Board. We recognize that one of the most important factors of the board's institutional setup is its independence (on Meta, and third parties). Independence of court-like structure is important to achieve legitimacy of its decision-making authority. If two parties wish to have their dispute or conflict resolved, a third party – a judge or arbiter – must be neutral, impartial, and independent on the parties but also on other, external interests. Factual *and* perceived impartiality and independence may lead to legitimacy

[47] O'Sullivan, D., Subramaniam, T. and Duffy, C. (2021) *op. cit.*

[48] Douek, E. (2019) *op. cit.*, p. 74; Klonick, K. (2020) *op. cit.*, p. 2475.

of the whole resolution framework, be it private (arbitration courts) or public (traditional state-administered courts).[49] Consequently, legitimacy is necessary for sustainable existence of the courts and the acceptance of their resolutions by the parties and perspective parties.[50]

We therefore consider internationally recognized structural elements of *de jure* judicial independence to establish whether the governance structure of the Oversight Board favors its independence.[51]

The elements include primarily the following: (i) Institutional stability, stability of the court's powers, allocation of competences and procedures to change them (who decides what powers courts have; how easy it is to change these rules). The more complicated the procedure to change the institutional setup of a court, the more stable the institutional setup of the court is. Such institutional stability leads to independence. (ii) Procedures to appoint judges (who appoints judges; how diverse or monolithic are persons selecting the judges etc.). The more diverse (in numbers, in representation), the more independent judges may be. (iii) Term of the judges (tenure, term, renewable terms etc.) – longer terms or tenures may be better for independence of judges as it makes them less dependent on other branches for re-election for next term. (iv) Remuneration of judges (who sets the remuneration; how comparable to market standard it is; how easy it is to cut the salary) – decent salary is a basic protection against outside influence (e. g. corruption). (v) Inference of other branches into decision making power of courts should be minimized. (vi) Distribution of cases should be based preferably on random draws. (vii) Requirements of transparency – publishing decisions – are conducive for public debate, which may decrease pressures of other branches on judiciary. We consider these elements individually.

The governance structure of the Oversight Board was designed to facilitate its independence from Meta and to enable a mechanism through which content may be brought for independent review. The Oversight Board's Charter was considered to become a constitution-like document[52], which

[49] Shapiro, M. (1981) *Courts. A Comparative and Political Analysis*. Chicago: the University of Chicago Press.

[50] Similarly, higher levels of legitimacy are typically awarded to arbitration courts setup by rather neutral entities, such as attorneys (bar association) or organizations with wider groups of constituents (interest organizations). It is difficult to forego the elements of neutrality and participation.

[51] We draw mainly from: Voigt, S., Gutmann, J. and Feld, L. P. (2015) Economic Growth and Judicial Independence, a Dozen Years on: Cross-Country Evidence Using an Updated Set of Indicators. *European Journal of Political Economy* 38, p. 197–211. Available from: https://doi.org/10.1016/j.ejpoleco.2015.01.004.

[52] Klonick, K. (2020) *op. cit.*, pp. 2457-2458.

would establish the framework for creating this *institution* and lay out the relationship between Meta, the Oversight Board and the Trust.[53] The Charter may be amended only if approved by the simple majority of individual trustees of the Trust, the simple majority of the Oversight Board and once approved by Meta. The most recent update to the Charter added to this rule, that any amendment increasing the obligations or duties of any individual trustee, corporate trustee, or manager of the LLC, shall not be effective without the approval of said party (individual trustee, corporate trustee or manager of the LLC).[54] The requirement for Meta's approval to any changes to the Charter is logical for Meta, which safeguards its "investment" in the board, yet it is problematic from the perspective of independence of Meta, as it gives Meta – the 'controlled' – the power to block any meaningful changes to the Charter, which governs the controlling process.[55]

The Charter makes a direct reference to the Bylaws, which outline the Oversight Board's operational procedures.[56] Moreover, the Charter makes a reference to other documents, such as LLC Agreement, Trust Agreement, Member contracts, Code of Conduct, and Service Provider Contract. To further assess respective elements of judicial independence, we explore the Oversight Board's governance and its main elements (the Trust, the Company and the Oversight Board and its members) through the analysis of the main documents (the Charter, the Bylaws, the LLC Agreement and the Trust Agreement).[57] We follow the structure of the Oversight Board, which consists of a Delaware limited liability company – Oversight Board LLC (the Company) and a non-charitable purpose trust – Oversight Board Trust (the Trust).

---

[53] The final version of the Charter was released on September 17, 2019. It is a nine-page documents divided into seven articles covering the matters of: members, authority to review, procedures of review, implementation, governance, amendments and bylaws and compliance with the law. The most recent version of the Charter was released on February 2023, which is referred to in this paper unless stated otherwise.

[54] Oversight Board. (2022) *op. cit.*, Art. 6 Sec. 1.

[55] Amendment of the Charter thus relies on the approval from Meta, which was criticized in the past. See: Klonick, K. (2020) *op. cit.*, pp. 2457-2466.

[56] The Bylaws were most recently revised in February 2023 and this revision introduced new rules for their amendment in Art. 5 Sec. 5 of the Bylaws. Each area of the Bylaws has a specific procedure for its amendment, with designated entities and stipulated quorums required for the consent on the amendment.

[57] In the process of writing this paper, the core documents of the Oversight Board were revised. In the paper, we refer to the core documents from the following dates: February 2023 Charter, February 2023 Bylaws October 2022 Rulebook. If necessary, we address the changes from the previous versions of documents directly in the paper.

3.1. THE TRUST

Independence from Meta as a key element of the Oversight Board's governance structure cannot be enabled without financial independence. The Trust Agreement was signed between Meta as settlor and Brown Brothers Harriman Trust Company of Delaware as corporate trustee in October 2019 in order to create Delaware non-charitable purpose trust with a name: Oversight Board Trust. The purpose of the Trust is specified in Section 2 of the Trust Agreement: "*The purpose of the Trust is to facilitate the creation, funding, management, and oversight of a structure that will permit and protect the operation of an Oversight Board, the purpose of which is to protect free expression by making principled, independent decisions about important pieces of content and by issuing policy advisory opinions on Facebook's content policies.*"[58] Additionally, the vital role of the Trust is to protect the independent judgment of the Oversight Board and their ability to fulfil their purpose especially via proper administration and structure.[59]

Moreover, the Trust Agreement states, that in order to assist to fulfil the Trust's purpose, the trustees shall form and fund a limited liability company of which the Trust will be the sole member through its trustees. The purpose of the limited liability company shall be to establish, administer, and attend to the ongoing operation of the group of individuals who make up the Oversight Board members. The trustees shall serve as managers of the limited liability company and the corporate trustee shall either serve as corporate manager of the limited liability company or appoint the corporate manager.[60]

The main aim of the Trust is to ensure governance and accountability of the Board and at the same time to control the Oversight Board's adherence to the stated purpose of its existence.[61] The responsibility of the trustees is to confirm the future board members and ensure that the Board operates in line with its purpose and governing documents.[62] Moreover, one of the main duties of the trustees is to remove the members of the Oversight Board if they breach the Code of Conduct. The purpose of the Trust is to maintain the administration and to provide oversight, thus, the trustees are responsible for the safeguarding of the assets in the Trust. In concrete, the trustees oversee the annual review and approval

---

[58] Oversight Board Trust Agreement, Sec. 2 Subsec. 2.1.
[59] *Op. cit.*, Sec. 2 Subsec. 2.2.
[60] *Op. cit.*, Sec. 2 Subsec. 2.1 and 2.3.
[61] Art. 5 Sec. 2 Oversight Board. (2022) *op. cit.*, Art. 5 Sec. 2. and *Oversight Board Bylaws.* Meta Oversight Board. Available from: `https://transparency.fb.com/sr/oversight-board-charter-2023`, Art. 4 Sec. 1.
[62] Oversight Board Bylaws, Art. 4 Sec. 1 Subsec. 1.2.

of the Oversight Board's budget, including member compensation.[63] The trustees do not have any competence in reviewing cases and independent judgment of the Oversight Board members.[64]

Moreover, it is necessary to address the relation of the Trust and Meta as settlor. The Meta is funding the Trust and is appointing independent trustees, who shall act in line with their fiduciary duties.[65] In order to enable the independence of the Trust and in order to avoid frustrating the independent judgement of the Oversight Board, Meta as settlor has relinquished its authority over the Trust except for exceptional provisions and circumstances stated in the Trust Agreement.[66]

Three alternatives were discussed how to provide financial independence of Oversight Board. The first alternative was a model of an annual funding provided from Meta, which will create unwanted financial dependence, the second alternative was to make the Oversight Board self-sufficient in funding, this alternative was considered to be risky if the project fails, the last alternative was a creation of irrevocable fund in an amount that will be enough to fund the operations of the Oversight Board for six years (two terms).[67] The last alternative was agreed upon and an initial trust estate in an amount of $130 million was transferred to the Trust by Meta.

The Trust is composed of at least three and maximum of eleven individual trustees and one corporate trustee selected by Meta as settlor. Individual trustees serve a five-year term[68] with an annual compensation of $200.000.[69]

[63] *Op. cit.*, Art. 4 Sec. 2.
[64] *Op. cit.*, Art. 4 Sec. 1 Subsec. 1.2.
[65] Oversight Board. (2022) *op. cit.*, Art. 5 Sec. 2.
[66] Oversight Board. (2021) *op. cit.*, Sec. 2 Subsec. 2.2.
[67] Klonick, K. (2020) *op. cit.* p. 2469.
[68] Oversight Board. (2021) *op. cit.* subsec. 6.2.2 (b).
[69] *Op. cit.*, subsec. 6.7. As of March 15, 2022, there are five individual trustees. See also: `https://oversightboard.com/governance/`.

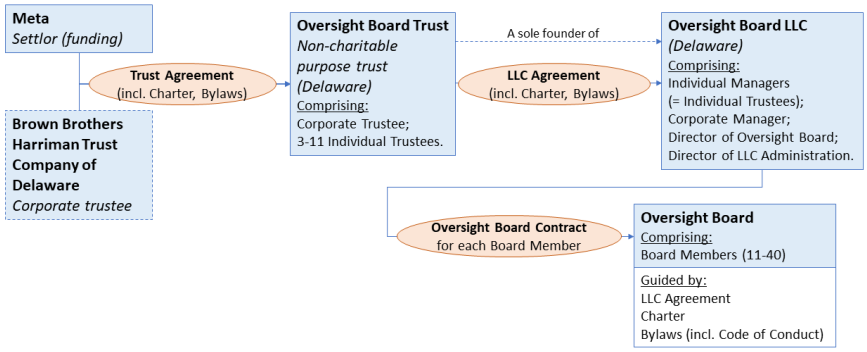

Figure 1: Governance Structure of the Oversight Board*
* Source: Meta published corporate documents, authors' design

3.2. THE COMPANY

The limited liability company, Oversight Board LLC (Company), was formed and funded by the Trust, thus, the Trust is the sole-member of this Company. The Company is a Delaware limited liability company, which was made effective as of October 17, 2019. The Company facilitates the functioning of the Board and its administration. The purpose of the Trust as a sole-member of the Company is defined in Article 2, Section 2.2 of the LLC Agreement and repeats the purpose already defined in the Trust Agreement. The Company facilitates the contractual relationships with the Oversight Board members as well as with the full-time administration stuff. As mentioned above, the individual trustees of the Trust shall serve as individual managers of the Company and the corporate trustee of the Trust shall either serve as corporate manager or appoint the corporate manager of the Company.[70] Based on the LLC Agreement, business and affairs of the Company are managed in sole and absolute discretion by individual managers (individual trustees) and one of more of their powers may be delegated to director of Oversight Board (Director of Oversight Board).[71] Director of Oversight Board shall be appointed by individual managers in order to assist in carrying out duties of managers as (for example)

[70] Oversight Board. (2019) *Oversight Board LLC Agreement*. Subsec. 2.2. Available from: `https://about.fb.com/wp-content/uploads/2019/12/LLC-Agreement.pdf`.
[71] *Op. cit.*, Subsec. 5.1 (a).

entering into board member contracts, service and employment contracts, dealing with expenses and compensations.[72] Moreover, Director of LLC Administration may be appointed by the corporate manager to assist in carrying out its duties[73] (managing finances, paying service providers, etc.).[74] It can be summed up that the Company is a tool which formally incorporated the Oversight Board.[75]

3.3. THE OVERSIGHT BOARD AND ITS MEMBERS

The Oversight Board is composed of a diverse set of members. The minimum number of members is eleven and if fully staffed it may have up to forty members. As to the board composition and member qualification the Charter states: "*Members must not have actual or perceived conflicts of interest that could compromise their independent judgment and decision-making. Members must have demonstrated experience at deliberating thoughtfully and as an open-minded contributor on a team; be skilled at making and explaining decisions based on a set of policies or standards; and have familiarity with matters relating to digital content and governance, including free expression, civic discourse, safety, privacy and technology.*"[76]

The term of the members is a three-year term and one member can serve up to three terms. The renewability of terms is prone to problems with independence. The compensation of the members is based on the fulfilment of their duties but will not be conditioned or withheld based on the outcome of the decisions of the Oversight Board.[77] Responsibilities and duties of the members are stipulated in their contracts (with the Company) and in the Code of Conduct.

The Code of Conduct, which represents an annex to the Bylaws, includes typical elements of professional codes of conduct (ethical codes), such as requirements on independence and impartiality, professionalism and integrity, or confidentiality. It regulates the board members' conduct when selecting and deciding cases. The structure and governance of the Oversight Board determine institutional aspects and the extent of institutional independence of the board, while the rules in the Code of Conduct determine personal independence safeguards, impartiality of individual board members and their integrity. The Code of Conduct is thus

---

72 *Op. cit.*, Subsec. 5.3 (a).
73 *Op. cit.*, Subsec. 5.2 (a).
74 *Op. cit.*, Subsec. 5.3 (b).
75 Klonick, K. (2020) *op. cit.* p. 2469.
76 Oversight Board. (2022) *Op. cit.*, Art. 1 Sec. 2.
77 *Op. cit.*, Art. 1 Sec. 5.

necessary to set standards of behavior of respective members, which must also be enforced through disciplining and/or removal from office.

The Oversight Board's operation is supported by administration; however, administration cannot interfere with the board's independent judgment on substantive content issues[78], the same applies to the trustees. Some of the members of the Oversight Board will serve as co-chairs, who will operate as liaisons to the administration, lead committees. Moreover, co-chairs will carry out management responsibilities as well especially in connection with membership and case selection.[79]

It is stated in the Charter, that Meta undertakes commitments to (i) provide information reasonably required for the Oversight Board to make its decisions, (ii) request the Oversight Board's review of content, (iii) seek policy advisory opinions from the Oversight Board and commit to taking action on the board's decisions and recommendations, (iv) support the Oversight Board to the extent that requests are technically and operationally feasible and consistent with a reasonable allocation of Meta's resources.[80]

Crucial element of Oversight Board's independence is the selection and removal of its members. It is stated in the Charter, that the initial formation of the Oversight Board will be supported by Meta, as well as selection of co-chairs. Indeed, this initial procedure was increasingly held by Meta and as Klonick states: "*It is unclear if this precedent of Facebook's initial involvement will forever taint the process and put in place long-term mechanisms that compromise members' ability to fairly adjudicate.*"[81]

After the initial formation, the Charter's mechanism stipulates, that co-chairs and Meta will jointly select candidates for the remainder of the board seats based on a review of the candidates' qualifications and a screen for disqualifications.[82] Following the selection, the trustees will formally appoint those members to the Oversight Board. Meta and the public may propose candidates to serve as members of the Oversight Board.

Herein lies a major deficit of the board's governance, specifically of the composition of the board. Although the public may propose candidates, it does not participate on the selection procedures anymore (at least in a structured and predictable manner). Coming back to the concept of legitimacy, an important part of legitimacy is participation, as noted

[78] Oversight Board Bylaws, Art. 4 Sec. 1 Subsec. 1.2.
[79] Oversight Board. (2022) *Op. cit.*, Art. 1 Sec. 7.
[80] *Op. cit.*, Art. 5 Sec. 3.
[81] Klonick, K. (2020) *Op. cit.*. p. 2465.
[82] Oversight Board. (2022) *Op. cit.*, Art. 1 Sec. 8.

in the past.[83] It would be advisable for Meta and the Oversight Board to introduce mechanisms to include various organized public interest groups or organizations (watchdogs, anti-conspiracy organizations, consumer protection organizations etc.) into the selection procedure in a structured way, especially with voting or nomination rights for certain board's members.

As mentioned previously, the trustees may remove a member of the Oversight Board before the expiration of their term for violations of the Code of Conduct, however, a member of the Oversight Board shall not be removed due to content decisions they have made.[84] The Bylaws stipulate that, at all times the Oversight Board must include a globally diverse set of members, in order to facilitate the needs of panel composition and in particular, this means that members of the Oversight Board should encompass the following regions: United States and Canada; Latin America and the Caribbean; Europe; Sub-Saharan Africa; Middle East and North Africa; Central and South Asia; and Asia Pacific and Oceania.[85] Although representation of various regions on the board is necessary, these regions naturally include thousands of respective cultures and societies with specific contexts to assess content moderation cases in – none of which is feasible with even a few dozens of board members.

4. DECISION MAKING AND IMPLEMENTATION

The third section deals with decision making and implementation of the board's decisions by Meta. It is useful to discuss who makes decisions, what process takes place to reach decisions, but also what basis is used to inform decision making.

The board reaches decisions in panels, which are composed of five board members with at least one member from the region of the content's origin. The panels are supposed to be gender diverse. The panels are established by random choice and their composition may remain anonymous to maintain safety and independence of the members of the panels.[86]

Decision making process is based on the information and statements provided by Meta, and the posting or reporting person. The board's charter claims high levels of accessibility and promises that *"posting person or the reporting person will have the opportunity to submit relevant and informed written statements to the board."*[87] The board may also gather or request

[83] Smith, R. W. (1970) the Concept of Legitimacy. *A Journal of Social and Political Theory* 35. p. 26.
[84] Oversight Board. (2022) *Op. cit.*, Art. 1 Sec. 8.
[85] Oversight Board Bylaws. Art. 1 Sec. 1.4 Subsec. 1.4.1.
[86] Meta's proprietary software, Case management Tool, is used for these random draws. See: Oversight Board Bylaws, Sec. 3.1.
[87] Oversight Board. (2022) *Op. cit.*, Art. 3 Sec. 3.

additional information, translations, or expert opinions to facilitate decision making. So far there has not been any tangible report on the use of expert opinions, yet they provide a potentially useful tool to mitigate the lack of fully contextualized decision making. As mentioned above, it may be difficult for individual board members to properly understand true meanings of messages in specific cultural contexts, opinions of recognized experts from countries or cultures of the origin of disputed message. Reliance on local, yet independent experts, sensitive to cultural nuances, may improve legitimacy of decisions. Additionally, the board is now allowed to accept additional written submissions by individuals and groups regardless of their direct relationship to the case.[88]

To offset this lack of knowledge of local contexts, individuals and organizations can submit comments to the Oversight Board during the decisions process. The Oversight Board stated that these public comments were key element for their understanding of the language, culture, politics and human rights specificities. As stated in its Annual Report, the Oversight Board received almost 10.000 public comments from individuals and organizations around the world, which helped shape the board's decisions and recommendations – in any case though, 97% of these public comments related to the decision on the former President Trump's suspension.[89] The Oversight Board pledges its commitment to build a global network of regional consultants to encourage people to submit appeals and public comments in their respective regions and language of the content in question.[90]

The Oversight Board's Bylaws require that the panels seek consensual decisions if possible. Yet if it is not possible, majority of the panelists resolve the case. Similar to dissenting opinions in court rulings, panelists are free to provide any reasons for divergence from the panel's decision, reservations or concerns.

Each decision should include a determination on the content, i. e. a resolution to allow or remove the content from Facebook or Instagram. The board can thus either uphold Meta's decision or reverse its decision. The board may also uphold or reverse any specific messaging (designation) that Meta may have decided to require prior to allowing the content (e. g. displaying a warning screen). The decision should also include

---

88 Ibid., Compare with the previous version of the Charter where the individuals or groups submitting their statements had to qualify as being "immediately depicted or impacted by the content in question".

89 Oversight Board. (2021) *Annual Report*, p. 51.

90 *Op. cit.*, p. 67.

explanation of the argumentation behind the decision, and, alternatively, also recommendations formulated by the board.

Transparency appears to be one of the guiding principles of the board's decision making.[91] The board is required to publish not only procedures on submission and the board's requirements for review[92], decisions and rationale behind decisions are also made publicly available, including within a publicly available database.[93] The board further publishes annual report (which is first approved by majority vote), including certain data on the volumes of cases submitted, considered and decided, broken down into regions, sources of referral and platform, as well as the analysis of the impact on the human rights standards.[94] The board should also include a report on the timeliness of Meta's implementation and response to board decisions and recommendations. The names of the board members are public, including their brief CVs.[95] The principle of transparency extends beyond board to Meta, which must disclose the actions it takes in response to the board's decisions.

There are four specific types of process the board may consider: (i) standard appeals process, which is the most common process dealing with overruling or upholding Meta's decisions; (ii) board re-review, which is a special procedure under which a decision is sent to all board members who may decide by a majority vote to submit the decision for a re-review by a new panel of the board (re-review must be decided before the decision is published); (iii) expedited review, which is undertaken under specific time-constrained circumstances as it may have imminent real-world consequences; under the most recent update of the Charter in February 2023, the expedited review is not automatic anymore and the co-chairs will decide whether to accept Meta's referral[96]; (iv) request for policy advisory opinions by Meta – Meta may specifically request clarification of a previous decision of the board or advisory and recommendation regarding possible changes to its content policies.[97]

Standard appeals process starts with a submission by user (original

---

[91] Oversight Board Bylaws. *Op. cit.*, Art. 1 Sec. 4.

[92] Note that the art. 3 Sec. 1.2.1 of the Oversight Board Bylaws requires the that users who submit a request for review can track the process online and get notifications about the request procedures and milestones.

[93] See: `https://oversightboard.com/decision/`.

[94] The first Annual Report was published in June 2022.

[95] See: `https://oversightboard.com/meet-the-board/`.

[96] Oversight Board. (2022) *Op. cit.*, Art. 3 Sec. 7 Subsec. 7.2. Additionally, also the co-chairs have the right to initiate an expedited review of a selected case, albeit with the consent of Meta (see Subsec. 2.1.2 of the Bylaws).

[97] *Op. cit.*, Art. 3 Sec. 7 Subsec. 7.3.

poster or reporting person, i. e. petitioner) or by Meta. Users are required to provide reasoning as to why the board should deal with the case and why the original Meta's decision was wrong. At first, the board's staff prepares a longlist of eligible cases for in-depth review. This first selection is done by the administrative staff of the board, i. e. The Case Selection Team. The longlist is then presented to the Case Selection Committee, composed of 5+ board members (on a rotating basis), and a sub-committee of the board, which prepares a shortlist of cases. This shortlist gets reviewed by the Meta's legal team to check for legality of review (legally risky cases are not considered).[98] The Case Selection Committee votes on the remaining cases to make a list of cases for review (simple majority vote suffices if there is no consensus reached). Once the panels are randomly formed and panelists familiarize with cases, panelists must declare conflicts of interest. Afterwards, the panel privately deliberates the case and prepare draft decision, which is reviewed by the whole board. Moreover, panelists may, by a majority vote, decide that a case requires plenary board deliberation. Next, the decision is published and implemented by Meta.

At times the board may decide to issue supplementary policy advisory opinions to Meta (previously policy guidance)[99]. In such cases, once the request for policy advisory opinion is approved by majority of board members, a panel is formed, typically constituted of five members, based on regional diversity, gender representation, expertise, availability, and interest. Following, the panel will have a preliminary meeting to agree on the following matters: (i) the lead drafter of the policy advisory opinion; (ii) questions to Meta and written requests for additional information; (iii) research tasks for the Oversight Board administration to undertake and/or commission from external experts.[100] Under the new Rulebook for Case Review and Policy Guidance 2022, public comments, research findings

[98] Based on the Annual Report, the 278 cases considered by the Case Selection Committee through December 2021 covered more than 70 countries, ranging from Fiji to Chad, and Trinidad & Tobago. 130 cases were shortlisted by the Oversight Board up until December 2021 and from among these cases Meta identified 51 occasions where its original decision on the content was incorrect. As stipulated by the Oversight Board, "this high error rate raises wider questions both about the accuracy of Meta's content moderation and the appeals process Meta applies before cases reach the Board." Oversight Board. (2021) *Annual Report*, p. 21.

[99] The most recent update of the Charter in February 2023 records the change of policy guidance into seemingly softer "policy advisory opinions". Similarly, policy advisory opinions were referred to in Rulebook for Case Review and Policy Guidance 2020 as "policy guidance" under much simpler procedure of adaption as the policy advisory opinions under Rulebook for Case Review and Policy Guidance 2022.

[100] Oversight Board. (2022) *Rulebook for Case Review and Policy Guidance*. Step 5. Available from: `https://oversightboard.com/sr/rulebook-for-case-review-and-policy-guidance`.

and stakeholder inputs are taken into account in the process of deliberation on the policy advisory opinion.[101] First the panel and next the board provide feedback on the draft policy advisory opinion prepared by the lead drafter. The draft policy advisory opinion may be approved by a single majority of both the panel and the board.[102] If the policy advisory opinion is approved by the panel and the board, it is sent to Meta for privacy legal review and then follows its publication and translation.[103]

The decisions of the board are binding upon Meta, which must implement them promptly, in a matter of days after the release of the decision (except for policy advisory opinions and recommendations).[104] Meta is also required to respond to all board decisions and provide information regarding the implementation of each decision. It also has 60 days to provide response to any policy advisory provided by the board.

5. THE OVERSIGHT BOARD IN LIGHT OF THE DSA

The DSA features several regulatory elements similar to the Oversight Board and its functions. It may be therefore useful to review the compatibility of the board's mission and setup with these elements in the DSA.[105]

The regulation requires the platforms to provide their users with an easy and effective way to contest decisions of platforms that negatively affect them.[106] In specific, the platforms should be required to provide for easily accessible, user-friendly *internal* complaint-handling systems delivering outcomes in a non-discriminatory and non-arbitrary manner, and out-of-court dispute settlement framework by *external independent* certified bodies.[107] While the former option is envisioned as an internal and therefore dependent review system, the latter should rely on external independent and impartial arbiter, almost akin to arbitration court. None of these options should limit the possibility to contest platform decisions in a regular court – the last resort for the users or petitioners, yet from the regulatory point of view the least preferred option as it is expensive, lengthy and out-of-reach for many.

The internal complaint-handling system, as laid out in the art. 20 of the DSA, represents the first go-to option for the users (petitioners), typically after the platform limits or removes their content or profile,

[101] *Op. cit.*, Step 6.
[102] *Op. cit.*, Step 7.
[103] *Ibid.*
[104] Oversight Board. (2022) *Op. cit.*, Art. 4.
[105] We do not attempt to review or assess other elements of the regulation included within the DSA.
[106] Art. 16(1) of the DSA.
[107] See *op. cit.* art. 20 and 21.

or after they unsuccessfully attempted to limit someone else's content or profile. Specifically, reviewable are decisions taken by the platforms on the grounds that a user provided information on the platform that is illegal or incompatible with the platforms' terms and conditions. Petitioners have 6 months to lodge a complaint against decisions, electronically and free of charge. Anyone should be able to lodge a complaint and have their complaint reviewed in a timely and diligent manner.

This review system is internal; therefore, the review cannot be "independent" or "impartial" – the reviews are supposed to be made by the platform itself (e. g. by the employees, or contractor(s)). Nonetheless the complaints are supposed to be handled objectively, resulting in either upholding the decision or reversing it. Automated means of reviewing are permissible as well, but only if the review is not based solely upon them. The review output should provide petitioners with information on the options of additional out-of-court dispute settlement and other redress options.

Under the out-of-court dispute settlement system, users should have the right to select any out-of-court dispute settlement body certified by the EU Members States to settle disputes relating to decisions issued by the platforms (incl. those not resolved by the internal complaint-handling system).[108] The out-of-court settlement system is therefore based on external reviewer of the platforms' decisions, who must fulfill specific criteria to get certified. The logic of the system is similar to online dispute resolution systems – an independent and impartial, yet sufficiently knowledgeable neutral reviews disputes and issues decisions. The platforms and their users (petitioners) should be treated equally.[109] The decisions taken by the out-of-court settlement system are not binding on the parties though, which leaves the parties with the option to seek judicial redress.[110]

The certification requirements include further requirements indicating the structure of the dispute settlement system: (i) the settlement body must be impartial and independent of online platforms and users; (ii) the settlement body must possess necessary expertise to review the platform decisions; (iii) the remuneration of the settlement body's members is not linked to the outcome of the procedure; (iv) the system must be accessible electronically, and must be produce swift, efficient, and cost-effective

[108] *Op. cit.*, Art. 21.

[109] A minor deviation from this principle is in the distribution of fees under art. 21(5) of the DSA, under which if the platform loses it reimburses reasonable expenses of the petitioner, whereas if the platform wins the dispute, there is no reimbursement of the platform's costs.

[110] *Op. cit.*, Art. 21(2); see also recital 59 of the DSA.

reviews; (iv) the resolution system must be based on clear and fair rules of procedure.[111]

Considering the mission and the setup of the Oversight Board, it stands somewhere in the middle of these two review systems, presumably closer to the out-of-court dispute settlement. First, the Oversight Board it is not an internal body of Meta, and although not ideal, its dependence on Meta has been structurally weakened. Thus, it differs widely from the internal complaint-handling system, yet as the analysis provided in this paper shows, it cannot be considered completely independent as well. It remains to be seen how the digital services coordinators will interpret the requirement of independence under the art. 21(3) of the DSA (and whether detailed delegated legislation would be required to further specify these requirements).

Second, the board does not review all the platform's decisions, but only a fraction, as mentioned above.[112] Although anyone can submit a request for review to the board, the board has a broad discretion to select *emblematic* cases. It is not structured as a regularly approached entity (as both the internal complaint-handling and out-of-court dispute settlement systems are), but rather a last resort, selective reviewer, whose decisions are meant to have wider impact.

Third, the board's review process is currently fully covered by Meta's bulk payment to the trust, whereas the out-of-court dispute settlement is paid for by the losing side and/or online platforms. As such, these fees, although supposed to be reasonable, would deter a proportion of users, yet unlikely those with strong case against the platform. An interesting part of the DSA consists of requirement that the fees charged by the dispute settlement body should not exceed the costs of the dispute settlement, indicating its limited commercial potential. The internal complaint-handling system should be free of charge.

Fourth, the Oversight Board, but also the internal complaint-handling system, have clearly a global scope, whereas the out-of-court settlement system has a localization aspect to it. As the certification of settlement bodies is done at the level of Member States, there is some expectation these bodies will have a knowledge of local circumstances. In fact, a distributed network of certified local settlement bodies may be able to offset the lack of knowledge of local contexts when reviewing cases by the board.

Fifth, the DSA imposes strong transparency requirements on the platforms,

[111] *Op. cit.*, Art. 21(3).
[112] See Section 1: mission, jurisdiction and powers. See also note 75.

which is also one of the guiding principles of the board's mission.[113] The DSA requires that platforms publish regular, accessible, and easily comprehensible reports on content moderation platforms engaged in during previous reporting period. The reports should include categorized statistics on content moderation by the platform, including orders issued by the Member States' authorities (under the art. 9 and 10 of the DSA), categorized by the type of illegal content concerned, time frames it took to act, also detailed and categorized information on the number of disputes the platform engaged in at its own initiative, handled through the internal complaint-handling systems or submitted to the out-of-court dispute settlement bodies, the outcomes and the average time needed for completing the dispute. Very large online platforms, i. e. platforms with over 45 million users[114], would be in addition obliged to undertake and publish among other issues audit report and audit implementation report (based on the art. 37(4) of the DSA).[115] The reporting obligations under the DSA are wider than the reports provided by the Oversight Board, which deal primarily with the cases submitted to it for review. Nonetheless, the board's reports may be potentially deeper as they have ambition to provide human rights impact assessments (in relation to content moderation).[116]

Sixth, the obligation to undertake an independent audit relates marginally to the policy-oriented recommendations the Oversight Board may provide Meta. There are no specific requirements on the audits and recommendations provided by the Oversight Board in its governing documents, the board enjoys and sometimes uses a wide discretion to comment on Meta's policies and actions. On the other hand, the DSA requires that very large online platforms procure an independent audit from an auditor with proven expertise in the area of risk management, technical competence and capabilities.[117] Such auditor must be independent and objective and governed by professional ethics. The audit concerns the obligations set out in chapter III of the DSA (Chapter III Due diligence obligations for a transparent and safe online environment). The audit also reviews the platforms' performance when it comes to their commitments pursuant to the codes of conduct (under the art. 45-46 of the DSA) and the crisis protocols (under the art. 48 of the DSA). The audits must include

[113] See Art. 15, 24, 39 and 42 of the DSA.
[114] *Op. cit*, Art. 33.
[115] *Op. cit.*, Art. 42.
[116] See Section 3: decision making and implementation. Additionally, the Oversight Board itself highlighted the Meta's transparency as one of their significant concerns. Oversight Board. (2021) Annual Report, p. 8.
[117] Art. 37(3) of the DSA.

enumeration of the elements audited, methodology, findings, auditors' opinion on compliance and operational recommendations on measures to achieve compliance, but also a declaration of conflicts of interest.

In summary, the Oversight Board's present setup will not be compliant with the DSA, even though it resembles out-of-court dispute settlement system. It differs in several key aspects, primarily its semi-independent position, the breadth of its scope, yet the limitations of its capacity to hear cases, or global approach in contrast to requirement to consider local contexts.

The Oversight Board's mission is clearly different to the mission envisioned for the out-of-court dispute settlement bodies – the question of reconciliation of these missions is now open as the DSA was adopted in October 2022. Meta is not bound by the decisions taken by the out-of-court dispute settlement bodies, which provides the Oversight Board some attractivity. The Oversight Board may become an alternative for in-depth reviews of the out-of-court dispute settlements. The board would have to change its mission and structure (and comply with the requirements under the DSA). Another approach could involve a possible transformation of the Oversight Board into an out-of-court dispute settlement body, becoming additional redress venue, competing with certified out-of-court dispute settlement bodies. A major problem with the out-of-court dispute settlement bodies' mandate under the DSA relates to their non-binding nature of decision making; if Meta continues to make a credible promise to abide by the board's decisions, the board may have niche here. Therefore, there seems to be certain additional value in transforming the Oversight Board into a settlement body. Although the board's decisions are mandatory on Meta (with certain caveats)[118], there may come into play other qualitative parameters in competition of these two systems, such as admission rate for review, fees, quality of decisions, reputation etc.

6. CONCLUSION

The Oversight Board's mandate is purposefully limited to reviewing content decisions by Meta. This limited mandate does not include more problematic issues for review, such as the overall architecture and design of the platforms, including algorithms used to spread information on the social media. Arguing that regulating specific instances of problematic speech on the platform would suffice is like arguing that regulating *merely* individual banks is sufficient to prevent the next financial crisis. As the previous financial crises revealed, it is essential to understand

[118] The enforceability of the board's decisions is questionable should Meta decide to ignore them; such enforcement appears to rest only on potential reputation losses of Meta.

underlying connections between individual banks and other financial institutions, that lead to systemic risks – the same applies to algorithmically spreading fake information wildfires, as even the DSA accepts.

Although it is surely appealing for corporate PR to outsource some of the difficult content decisions on a semi-independent quasi-judicial body, the Oversight Board, it is way more important for the quality of democracies to independently review the channels, algorithms, and platform design than individual decisions. Still, the problem may lie in the contradiction of the corporate profit-maximizing purpose with protection of democratic values. Moreover, even though the board's governance is structured to account for majority of typical judicial independence elements, there are some structural weaknesses, such as short terms of the board members, or reliance on trustees to execute important decisions (yet the trustees also play an important role of enforcing accountability). Even the Oversight Board itself admits certain limitations to its scope for decision-making and independent institutional setup in its recent Annual Report.

As our paper suggests, the board suffers from legitimacy deficit, which comes from lack of participation on its composition, governing rules but also from lack of pure legal legitimacy. This deficit may be mitigated by legislative action – by outlining legal requirements (e. g. by the EU in case of the DSA) for the out-of-court dispute settlement systems, similar to the Oversight Board. Yet, the Oversight Board in its current form is a different animal as stipulated by the DSA. The Oversight Board may be a useful part of the overall platforms' regulatory framework, once it enhances the participation, strengthens its legitimacy towards the platforms' users and improves its systematic appreciation of local contexts.

LIST OF REFERENCES

[1] Douek, E. (2019) Facebook's "Oversight Board:" Move Fast with Stable Infrastructure and Humility. *North Carolina Journal of Law & Technology* 21(1).

[2] Duffy, C. (2021) Facebook Has Known It Has a Human Trafficking Problem for Years. It Still Hasn't Fully Fixed It. *CNN*. Available from: `https://edition.cnn.com/2021/10/25/tech/facebook-instagram-app-store-ban-human-trafficking/index.html`.

[3] Dwoskin, E., Newmyer, T. and Mahtani, S. (2021) the Case against Mark Zuckerberg: Insiders Say Facebook's CEO Chose Growth over Safety. *The Washington Post*. Available from: `https://www.washingtonpost.com/technology/2021/10/25/mark-zuckerberg-facebook-whistleblower/`.

[4] Electronic Frontier Foundation. (2021) *The Santa Clara Principles on Transparency*

and Accountability in Content Moderation. Available from: https://santaclaraprinciples.org.

[5] Hegelich, S. (2020) Facebook Needs to Share More with Researchers. *Nature* 579(7800), pp. 473–473. Available from: https://doi.org/10.1038/d41586-020-00828-5.

[6] Jacobs, J. (2019) Will Instagram Ever "Free the Nipple"? *The New York Times*. Available from: https://www.nytimes.com/2019/11/22/arts/design/instagram-free-the-nipple.html.

[7] Jaffe, L. L. (1958) the Right to Judicial Review. *Harvard Law Review* 71(3).

[8] Kang, C. (2021) the F.T.C. Asks for an Extension to Refile Its Facebook Antitrust Suit. *The New York Times*. Available from: https://www.nytimes.com/2021/07/23/technology/ftc-facebook-antitrust-lawsuit.html.

[9] Klonick, K. (2020) the Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression. *Yale Law Journal* 129, pp. 2418–2499.

[10] Mazúr, J. and Patakyová, M. T. (2019) Regulatory Approaches to Facebook and Other Social Media Platforms: Towards Platforms Design Accountability. *Masaryk University Journal of Law and Technology* 13(2), pp. 219–42. Available from: https://doi.org/10.5817/MUJLT2019-2-4.

[11] Meta. *Facebook Community Standards*. Available from: https://transparency.fb.com/en-gb/policies/community-standards/.

[12] O'Sullivan, D., Subramaniam, T. and Duffy, C. (2021) Not Stopping "Stop the Steal:" Facebook Papers Paint Damning Picture of Company's Role in Insurrection. *CNN*. Available from: https://edition.cnn.com/2021/10/22/business/january-6-insurrection-facebook-papers/index.html.

[13] Oversight Board. *Appeals process*. Available from: https://oversightboard.com/appeals-process/.

[14] Oversight Board. *Governance*. Available from: https://www.oversightboard.com/governance/.

[15] Oversight Board. *Meet the Board*. Available from: https://oversightboard.com/meet-the-board/.

[16] Oversight Board. (2020) *Rulebook for Case Review and Policy Guidance*. Available from: https://oversightboard.com/sr/rulebook-for-case-review-and-policy-guidance.

[17] Oversight Board. (2022) *The Charter*. Available from: https://oversightboard.com/governance/.

[18] Oversight Board. (2023) Oversight Board Bylaws. Available from:

https://transparency.fb.com/sr/oversight-board-charter-2023.

[19] Pearson, J. (2020) Exclusive: Facebook Agreed to Censor Posts after Vietnam Slowed Traffic - Sources. *Reuters*. Available from: https://www.reuters.com/article/us-vietnam-facebook-exclusive/exclusive-facebook-agreed-to-censor-posts-after-vietnam-slowed-traffic-sources-idUSKCN2232JX.

[20] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). *Official Journal of the European Union* (L277) 19 October. Available from: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32022R2065.

[21] Shapiro, M. (1981) *Courts. A Comparative and Political Analysis*. Chicago: the University of Chicago Press.

[22] Smith, R. W. (1970) the Concept of Legitimacy. *A Journal of Social and Political Theory* 35.

[23] Subramaniam, T. (2021) Four Takeaways from Facebook Whistleblower's Complaints. *CNN*. Available from: https://edition.cnn.com/2021/10/06/tech/fb-whistleblower-doc-takeaways/index.html.

[24] Subramaniam, T. (2021) the Big Takeaways from the Facebook Papers. *CNN*. Available from: https://edition.cnn.com/2021/10/26/tech/facebook-papers-takeaways/index.html.

[25] Voigt, S., Gutmann, J. and Feld, L. P. (2015) Economic Growth and Judicial Independence, a Dozen Years on: Cross-Country Evidence Using an Updated Set of Indicators. *European Journal of Political Economy* 38. Available from: https://doi.org/10.1016/j.ejpoleco.2015.01.004.

[26] Weber, M. (2004) the Vocation Lectures. Indianapolis: Hackett Publishing Company.

[27] Wheeler, T., Verveer, P. and Kimmelman, G. (2020) New Digital Realities; New Oversight Solutions in the U.S. The Case for a Digital Platform Agency and a New Approach to Regulatory Oversight. *The Shorenstein Center on Media, Politics and Public Policy*.

[28] Whistleblower Aid. (2021) Anonymous Whistleblower Disclosure: Re: Supplemental Disclosure of Securities Law Violations by Facebook, Inc. (NASDAQ: FB), SEC TCR #. Available at: https://drive.google.com/file/d/1WPOaPE6MyWMdMV9f218nsSjGGrmSjnkw/view.

[29] Zingales, L. (2021) Don't Break Up Social Media, Bifurcate It. *Project Syndicate*. Available from: https://www.project-syndicate.org/

commentary/social-media-separate-network-infrastructure-from-editorial-role-by-luigi-zingales-2021-08.

[30] Zuckerberg, M. (2019) Opinion: Mark Zuckerberg: the Internet Needs New Rules. Let's Start in These Four Areas. *The Washington Post*. Available at: https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html.

DOI 10.5817/MUJLT2023-1-2

ON SOVEREIGNTY *

by

DAN SVANTESSON † SAMULI HAATAJA ‡
DANIELLE IRELAND-PIPER § KUAN-WEI CHEN ¶

The concept of sovereignty is more important than ever in the cyber context, yet it is poorly understood. With this article, we seek to contribute towards a shared understanding of the concept of sovereignty by succinctly addressing the following six, interrelated, questions:

1. *Who can claim to have sovereignty;*
2. *Over what can one have sovereignty;*
3. *What are the consequences of having sovereignty over something;*
4. *Who can violate sovereignty;*
5. *What is the threshold for violating sovereignty; and*
6. *What are the consequences of violating sovereignty?*

However, this article is not limited to a descriptive account of the law as it stands today. A purely descriptive account would not provide a full picture of the complex concept of sovereignty, and we have felt it appropriate to enter the territory of law reform options in parts of the discussion. While sovereignty is a technology-neutral concept and the article addresses it as such, particular attention is directed at sovereignty in the cyber context.

KEY WORDS

Sovereignty, Cyberspace, Cyberconflict, International law, Cyberwar

* This research was supported by the Australian Government through a grant by the Australian Department of Defence. The views expressed herein are those of the authors and are not necessarily those of the Australian Government, the Australian Department of Defence, or the universities or other institutions the authors are affiliated with.

† dasvante@bond.edu.au, Professor, Faculty of Law, Bond University, Australia

‡ s.haataja@griffith.edu.au, Senior Lecturer, Griffith Law School, Griffith University, Australia

§ Danielle.Ireland-Piper@anu.edu.au, Associate Professor, National Security College, Australian National University and Honorary Adjunct Associate Professor, Faculty of Law, Bond University, Australia

¶ kuan-wei.chen@student.bond.edu.au, Senior Research Assistant/PhD Candidate, Faculty of Law, Bond University, Australia

1. INTRODUCTION

The topic of sovereignty is currently gaining an enormous amount of attention, not least in the cyber context. Yet, there seems to be little, or no, progress in our understanding of this key concept. In fact, it may be the case that the increased use of the term is resulting in an even lower level of shared understanding of what sovereignty is and does.

This discrepancy between increase in attention on the one hand, and lacking increase in understanding on the other hand, is both remarkable and unusual. It is also a major obstacle for a productive discourse on the topic. On the cyber arena, we see this e.g., in the form of imprecise – slogan-like – calls for cyber sovereignty, data sovereignty, digital sovereignty, information sovereignty, and the like.

To move towards a shared understanding of the concept of sovereignty, it seems essential to address, at the minimum, the following six, interrelated, questions:

1. Who can claim to have sovereignty;
2. Over what can one have sovereignty;
3. What are the consequences of having sovereignty over something;
4. Who can violate sovereignty;
5. What is the threshold for violating sovereignty; and
6. What are the consequences of violating sovereignty?

In this article, we seek to address these questions with the aim of providing an accessible overview of the concept of sovereignty. Hopefully, by addressing these important questions we may help to facilitate a shared understanding of sovereignty. However, this article is not limited to a descriptive account of the law as it stands today.

The reality is that there are fundamental disagreements on key aspects of sovereignty. Thus, a purely descriptive account would not provide a full picture of the complex concept of sovereignty, and we have felt it appropriate to enter the territory of law reform options in parts of the discussion. Great care has, however, been taken to clearly indicate to the reader what is our proposals and what is established law.

Put simply, it may be said that there are, at least, five problems with the current concept of sovereignty:

1. It is often approached in an unstructured manner;
2. It is vague and abstract;
3. It is anchored in territoriality;

4. It is binary; and
5. As a component of international law, its enforcement is difficult.

To give the reader an idea of what to expect from this article, it is appropriate to make a few comments about which of these problems the article seeks to address. It is hoped that this article will go some way towards providing a structured lens through which to discuss sovereignty, not least by breaking down the concept into the six questions outlined above.

However, it is less likely that the article manages to address the second problem; that of the concept of sovereignty being vague and abstract. Indeed, the proposal of anchoring sovereignty in the concept of State dignity may admittedly make sovereignty even more vague and abstract. Compared to conventional conceptions of sovereignty, one anchored in State dignity has potential to offer a more honest and transparent way to accommodate for flexibility in the international relations of States.

By anchoring sovereignty in the concept of State dignity, this article seeks to address problems three and four. However, it is not our ambition to reform the overall operation of international law, and the reality is that whether sovereignty is anchored in territoriality, or as we propose in State dignity, enforcing sovereignty is always going to be difficult.

As to the structure, the article commences with some brief and general observations about sovereignty and how sovereignty is discussed today, with emphasis on how it is discussed today in relation to the Internet. It then addresses the six highlighted questions one-by-one. In doing so, no attempt has been made to divide the attention equally between those questions. The first four are relatively straightforward, while the latter two are highly controversial. This is reflected in how we address them. The article concludes with some observations about the uncertain future of the concept of sovereignty, and of the environment in which it will operate.

While sovereignty is a technology-neutral concept and the article addresses it as such, particular attention is directed at sovereignty in the cyber context.

2. SOVEREIGNTY TODAY

Sovereignty as a concept has been taken for granted as being absolute and as being the foundation of the international legal order.[1] The concept of sovereignty is understood and manifested in a number of ways,[2] and it is "both a source of international law and international-law based".[3]

Sovereignty is a key concept in relation to several of the world's biggest current challenges such as Russia's invasion of Ukraine,[4] environmental challenges,[5] and China's aspiration to the so-called 'reunification' of Taiwan.[6] Without exaggeration, it may be said that the degree to which the concept of sovereignty instils stability in international law impacts all these challenges and how well we can handle them. Yet, we are remarkably far from a clear consensus on how the concept of sovereignty operates.

However, there is one matter on which there is agreement; while it has not always been so,[7] today, it is uncontroversial to suggest that sovereignty applies online.[8] This is important, but the value of this consensus is

---

1 See e.g. Jackson, J. H. (2003) Sovereignty-Modern: A New Approach to an Outdated Concept. American Journal of International Law, 97 (4), pp. 782-802; and Simonovic, I. (2002) Relative Sovereignty of the Twenty First Century. *Hastings International & Comparative Law Review*, 25, p. 371. Cf. Louis Henkin who does not find it useful to perpetuate the 'myth' of and use of the term sovereignty: Henkin, L. (1994) The Mythology of Sovereignty. In: RStJ Macdonald (ed.) *Essays in Honour of Wang Tieya*. Martinus Nijhoff: Dordrecht, pp. 353-355. See also Waldron, J. (2011) Are Sovereigns Entitled to the Benefit of the International Rule of Law? European Journal of International Law, 22 (2), p. 328.

2 Crawford, J. (2006) The Creation of States in International Law. 2nd ed. Oxford: Oxford University Press, p. 32. See also Svantesson, D. et al (2021) *The developing concept of sovereignty: considerations for defence operations in cyberspace and outer space*, Technology and Jurisdiction Research Team, Bond University, p. 19; and Klabbers, J. (1998) Clinching the Concept of Sovereignty: Wimbledon Redux. *Austrian Review of International and European Law*, 3 (1), p. 346.

3 Besson, S. (April 2011) Sovereignty. In: *Max Planck Encyclopedias of International Law*, paragraph 113.

4 See e.g. Kremlin. (2015) *Article by Vladimir Putin "On the Historical Unity of Russians and Ukrainians"*. [online] Moscow: Kremlin. Available from: `http://en.kremlin.ru/events/president/news/66181` [Accessed 7 November 2022].

5 See Paris Agreement, 12 December 2015, 3156 UNTS (entered into force 4 November 2016), art 13(3).

6 *The Taiwan Question and China's Reunification in the New Era* (2022). [online] Beijing: Taiwan Affairs Office of the State Council and The State Council Information Office of the People's Republic of China. Available from: `https://english.www.gov.cn/atts/stream/files/62f34db4c6d028997c37ca98` [Accessed 7 November 2022].

7 Barlow, J. A. (1996) *Declaration of the Independence of Cyberspace*. [online] Electronic Frontier Foundation: San Francisco. Available from: `https://www.eff.org/cyberspace-independence` [Accessed 7 November 2022].

8 Consider e.g. UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (24 June 2013) UN Doc A/68/98, and Open-ended working group on developments in the field of information and telecommunications in the context of international security, "Final

superficial indeed given that those who say that sovereignty applies online generally do not engage with the considerably more difficult question of how sovereignty applies online.

Perhaps this suggests that the only reason why we have a consensus on that sovereignty applies online is because we can answer that question while turning a blind eye to the 'how question'. The very prospect of this being the case shows the primitive level we currently are at and how strong the need is for more expertise being directed at this question.[9]

It is this combination of the central importance of the concept of sovereignty, and its current relatively primitive level of understanding, that made us write this article even though there already is a wealth of literature on the topic, and indeed, on the application of international law to cyber conflicts more broadly.[10] In other words, the nature of the current discussions is such that further works, such as this article, are justified, and this article is of course by no means the last word on this important topic. Much work lies ahead.

3. WHO CAN CLAIM TO HAVE SOVEREIGNTY?

On the surface, the question of who can claim to have sovereignty is uncontroversial; the answer is that States can claim to have sovereignty. Of course, the question then is what a State is, and fortunately international law provides answers to that question.

The State is the primary[11] subject or legal person of international law which possesses "the totality of international rights and duties recognized by international law".[12] Laying down the widely-accepted criteria of statehood,[13] the 1933 Montevideo Convention on the Rights and Duties of States provides that a State "*should* possess the following qualifications: (a)

Substantive Report" (10 March 2021), [online] New York: UN Office of Disarmament Affairs. Available from: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf [Accessed 7 November 2022].

9 See further: Svantesson, D. (2020) Is International Law Ready for the (Already Ongoing) Digital Age? Perspectives from Private and Public International Law. In: Busstra, M. et al (eds.) *International Law for a Digital World*. T. M. C. Asser Press: The Hague, 147, pp. 113-155.

10 For an excellent recent contribution to this debate, in this specific journal, see: Osula, A.-M., Kasper, A. and Kajander, A. (2022) EU Common Position on International Law and Cyberspace. *Masaryk University Journal of Law and Technology*, 16 (1), p. 89.

11 Higgins, R. (2000) *Problems and Process: International Law and How We Use It*. Oxford: Clarendon, p. 39. See also Klabbers, J. (1998) Clinching the Concept of Sovereignty: Wimbledon Redux. (1998) *Austrian Review of International and European Law*, 3 (1), p. 367.

12 *Reparation for Injuries Suffered in the Service of the United Nations (Advisory Opinion)*, [1949] ICJ Rep 174, p. 180; and *Legality of the Use by a State of Nuclear Weapons in Armed Conflict (Advisory Opinion)* [1996] ICJ Rep 66, paragraph 25.

13 Higgins, R. (2000) *Problems and Process: International Law and How We Use It*. Oxford: Clarendon, p. 39; and Cançado Trindade, A. A. (2013) *International law for humankind: towards a new jus gentium*. 2nd ed. Leiden: Brill, pp. 166-167. See also 'Draft Declaration on Rights

a permanent population; (b) a defined territory; (c) government; and (d) capacity to enter into relations with the other States". [14]

The criteria for statehood is prescriptive, for the seemingly objective criteria of what makes a State a State "have always been interpreted and applied flexibly, depending on the circumstances and the context in which the claim of statehood is made".[15] Divorced from the political (and often politicised) matter of the recognition of States,[16] various examples of 'States' demonstrate that despite lacking one or more of the component elements of statehood does not prevent them from being considered a member of the international community.[17] For example, as the Vatican and the Federated States of Micronesia demonstrate, there is no minimum requirement to satisfy the criteria of either territory or permanent population.

Further, the capacity to enter into relations with other States, according to Crawford, "is no longer, if it ever was, an exclusive State prerogative".[18]

---

and Duties of States with Commentaries' [1949] *Yearbook of the International Law Commission* 287, p. 289, paragraph 49.

[14] *Convention on the Rights and Duties of States*, signed 26 December 1933, 165 LNTS 19 (entered into force 26 December 1934), art I (emphasis added).

[15] Higgins, R. (2000) *Problems and Process: International Law and How We Use It*. Oxford: Clarendon, 39. See also Cançado Trindade, A. A. (2013) *International law for humankind: towards a new jus gentium*. 2nd ed. Leiden: Brill, ch VII; and Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo, Advisory Opinion [2010] ICJ Rep 403, paragraph 51.

[16] See *Convention on the Rights and Duties of States*, signed 26 December 1933, 165 LNTS 19 (entered into force 26 December 1934), art 3. See also Oppenheim, L. and Roxburgh, R. (2005) *International Law: A Treatise, Vol I: Peace*. 3rd ed. The Lawbook Exchange: Clark, p. 136, paragraph 72; and p. 373, paragraph 209. See generally, International Law Association (2018) I, Sydney Conference. [online] London: International Law Association. Available from: `https://www.ila-hq.org/en_GB/documents/conference-report-sydney-2018-6` [Accessed 7 November 2022]. For instance, Taiwan is (for lack of a better term) an entity that fulfils all objective criteria of statehood: see generally Crawford, J. (2006) *The Creation of States in International Law*. 2nd ed. Oxford: Oxford University Press, pp. 198-219. More recently, Russian President Vladimir Putin unilaterally claimed that 'Ukraine never had a tradition of genuine statehood': Reuters. (2022) *Extracts from Putin's speech on Ukraine*. [online] London: Reuters. Available from: `https://www.reuters.com/world/europe/extracts-putins-speech-ukraine-2022-02-21/` [Accessed 7 November 2022]. This assertion is overwhelmingly refuted by the international community: see e.g. UNGA, *Territorial integrity of Ukraine: defending the principles of the Charter of the United Nations*, GA Res ES-11/4, UN Doc A/RES/ES-11/4 (12 October 202) (143 in favour, 5 against, 35 abstentions).

[17] International Law Association (2018) *Recognition/Non-Recognition in International Law*, Sydney Conference. [online] London: International Law Association. Available from: `https://www.ila-hq.org/en_GB/documents/conference-report-sydney-2018-6` [Accessed 7 November 2022], p. 6.

[18] Crawford, J. (2006) The Creation of States in International Law. 2nd ed. Oxford: Oxford University Press, p. 61. See also *Recognition/Non-Recognition in International Law*, proceedings from the Sydney Conference of the International Law Association (2018), p. 5. [online] London: International Law Association. Available from: `https://www.ila-hq.org/en_GB/documents/conference-report-sydney-2018-6` [Accessed 7 November 2022].

Instead, independence, or "sovereignty in the relation between States",[19] is considered the "central criterion for statehood".[20] And here our quest to map out who can claim to have sovereignty arguably ends up in a degree of circularity; that is, having sovereignty is a criteria for being a State, and being a State is a criteria for having sovereignty.[21] Put in a more favourable light, it may perhaps instead be said that, this points to a link between, on the one hand, the question of how sovereignty may be established, and on the other hand, the question of who can claim to have sovereignty.

At any rate, it might now be tempting to conclude that we have successfully answered the first question. However, that is not quite the case. For example, the concept of 'data sovereignty' is frequently discussed in the context of indigenous populations, which highlights that sovereignty is not strictly speaking limited to States in all its meanings.[22] That, however, is a topic we do not pursue further here.

4. OVER WHAT CAN ONE HAVE SOVEREIGNTY?

A State is said to be sovereign over "a portion of the surface of the globe", meaning that it enjoys the "the right to exercise therein, to the exclusion of any other State, the functions of a State".[23] This clearly anchors the concept of sovereignty in the type of territoriality thinking that increasingly is recognised as incompatible with the online environment. Further, territorial sovereignty, in short, is the "exclusive competence of the State in regard to its own territory",[24] and respect for such territorial sovereignty "is an essential foundation of international relations".[25] A violation of territorial sovereignty would be in breach of the principle of sovereignty equality and non-intervention,[26] and constitute an internationally wrongful act. There are, however, obvious difficulties in applying this to the cyber domain.

The fact that our thinking of territoriality in the context of sovereignty

---

[19] *Island of Palmas Case (the Netherlands v. United States of America)* (1928) 2 RIAA 829, p. 838. See also *Customs Regime between Germany and Austria (Protocol of March 19th, 1931), Advisory Opinion*, PCIJ (ser A/B) No 41, p. 57 (per Judge Anzilotti).

[20] Crawford, J. (2006) *The Creation of States in International Law*. 2nd ed. Oxford: Oxford University Press, p. 62.

[21] See also Koskenniemi, M. (2005) *From Apology to Utopia: the Structure of International Legal Argument*. Cambridge: Cambridge University Press, pp. 224-302.

[22] See further: Hummel P., et al. (2021), Data sovereignty: A review. *Big Data & Society*, p. 12.

[23] *Island of Palmas Case (the Netherlands v. United States of America)* (1928) 2 RIAA 829, p. 838.

[24] *Ibid*, p. 838.

[25] *Corfu Channel (United Kingdom v Albania)* [1949] ICJ Rep 4, p. 35. See also *Case Concerning Military and Paramilitary Activities in and against Nicaragua* [1986] ICJ Rep 14, paragraph 202. See also Jackson, J. H. (2003) Sovereignty-Modern: A New Approach to an Outdated Concept. *American Journal of International Law*, 97 (4) 782, p. 790.

[26] *Case Concerning Military and Paramilitary Activities in and against Nicaragua* [1986] ICJ Rep 14, paragraph 212.

has evolved over time, can be seen in that territorial sovereignty is now not limited to the landmass of the Earth that is said to be within the physical confines of a State. It also extends over territorial waters,[27] which spans up to 12 nautical miles from territory of the coastal State.[28] A coastal State is also said to exercise certain sovereign rights to explore and exploit natural resources in the exclusive economic zone[29] and on the continental shelf that adjoins its territorial waters.[30] Further, a State is said to enjoy "complete and exclusive sovereignty" over the airspace above its territory,[31] which has been confirmed as "firmly established and longstanding tenets of customary international law".[32] This means that any human-made object (for instance an aircraft or spacecraft) wishing to transit through sovereign airspace must obtain authorisation from the overflown State.[33] In contrast, despite there being no universally accepted demarcation line between airspace and outer

---

[27] *Corfu Channel (United Kingdom v Albania)* [1949] ICJ Rep 4, p. 30. See also United Nations Convention on the Law of the Sea, signed on 10 December 1982, 1833 UNTS 3 (entered into force 16 November 1994), art 2(1).

[28] *United Nations Convention on the Law of the Sea*, signed on 10 December 1982, 1833 UNTS 3 (entered into force 16 November 1994), art 3; and *Convention on International Civil Aviation*, 7 December 1944, 15 UNTS 295, ICAO 7300/9 (entered into force 4 April 1947), art 2.

[29] *United Nations Convention on the Law of the Sea*, signed on 10 December 1982, 1833 UNTS 3 (entered into force 16 November 1994), art 55; art 57.

[30] *Ibid*, art 77; and art 76. See also*North Sea Continental Shelf Cases (Germany v. Denmark; Germany v. the Netherlands)* [1969] ICJ Rep 3; and Continental Shelf (Libyan Arab Jamahiriya v. Malta) [1985] ICJ Rep 13.

[31] *Convention on International Civil Aviation*, 7 December 1944, 15 UNTS 295, ICAO 7300/9 (entered into force 4 April 1947), art 1. Though the upper limit of sovereignty over airspace is unsettled, it is accepted that sovereignty over airspace ends where outer space begins, for there can be no claim of sovereignty over outer space: *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*, 27 January 1967, 610 UNTS 205 (entered into force 10 October 1967), art II. Some States have set an arbitrary height of 100km as where outer space begins, see e.g. Denmark, *Law on Activities in Outer Space* [online], L 128 (2016). Available from: `https://www.ft.dk/RIpdf/samling/20151/lovforslag/L128/20151_L128_som_vedtaget.pdf` (in Danish), paragraph 4(4); Kazakhstan, *Outer Space Activities Act (2012)*, art 1(6),

[32] *Case Concerning Military and Paramilitary Activities in and against Nicaragua* [1986] ICJ Rep 14, paragraph 212.

[33] *Convention on International Civil Aviation*, 7 December 1944, 15 UNTS 295, ICAO 7300/9 (entered into force 4 April 1947), art 5. See also *International Air Services Transit Agreement*, 7 December 1944, 84 UNTS 387 (entered into force 30 January 1945), art 1, Section 1(1). For a space object, see Canada: Claim Against the Union of Soviet Socialist Republics for Damage Caused by Soviet Cosmos 954 (1979), Annex A: Statement of Claim. International Legal Materials, 18 (4), p. 899, paragraph 21; and UNCOPUOS, *Questionnaire on possible legal issues with regard to aerospace objects: replies from Member States*, UN Doc A/AC.105/635/Add.7 (2003); UNCOPUOS, *Questionnaire on possible legal issues with regard to aerospace objects: replies from Member States*, UN Doc A/AC.105/635/Add.8E (2003), reply of the Netherlands; UNCOPUOS, *Questionnaire on possible legal issues with regard to aerospace objects: replies from Member States*, UN Doc A/AC.105/635/Add.7 (2003), replies of Costa Rica; Czech; Ecuador; Mexico; South Africa; and Turkey.

space, it is universally agreed that outer space and celestial bodies are areas beyond territorial sovereignty.[34] Further, the right to carry out remote sensing of natural resources without the consent of the targeted state is also generally accepted as customary international law.[35]

Given these expansions of how territoriality is viewed in the context of sovereignty, it may be argued that it would be illogical if we felt restrained from allowing it to expand also in response to the realities of cyberspace. Or as we argue, better still, it may be argued that this persistent need to evolve and expand the way in which we apply territoriality in the context of sovereignty finally has reached a breaking point created by cyberspace and that the time, thus, has come to adopt an approach to sovereignty that is not anchored in territoriality.

In terms of objects, on the high seas, it is said that "a ship [...] is assimilated to the territory of the State of the flag it flies",[36] while an aircraft bears the nationality of the State that registers the aircraft.[37] Similarly, a space object launched into Earth orbit or beyond is considered an extension of the territory of the State that registers the object, over which that State may exercise jurisdiction and control.[38] This is referred to as quasi-territorial jurisdiction.[39]

Territorial sovereignty, however, cannot be claimed over the global commons, which include the high seas,[40] Antarctica,[41] outer space as well as the Moon and other celestial bodies.[42] Notably, however, the United

[34] *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*, 27 January 1967, 610 UNTS 205 (entered into force 10 October 1967), art II.

[35] Jakhu, R. S. and Freeland, S. (2016) The Relationship between the Outer Space Treaty and Customary International Law. *Proceedings of the International Institute of Space Law*, 59, p. 186.

[36] *S.S. Lotus, (France v. Turkey)*, (1927) PCIJ Ser. A, No. 10, p. 25.

[37] *Convention on International Civil Aviation*, 7 December 1944, 15 UNTS 295, ICAO 7300/9 (entered into force 4 April 1947), art 17.

[38] *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*, 27 January 1967, 610 UNTS 205 (entered into force 10 October 1967), art VIII; and *Agreement among the Government of Canada, Governments of the Member States of the European Space Agency (ESA), the Government of Japan, the Government of the Russian Federation and the Government of the United States of America Concerning Cooperation on the Civil International Space Station*, 29 January 1998, 80 Stat 271, 1 USC 113 (entered into force 27 March 2001), art 5

[39] See Cheng, B. (1965) The Extra-Territorial Application of International Law. *Current Legal Problems*, 18 (1), p. 135.

[40] *United Nations Convention on the Law of the Sea*, signed on 10 December 1982, 1833 UNTS 3 (entered into force 16 November 1994), art 89.

[41] *Antarctic Treaty*, signed on 1 December 1959, 402 UNTS 7 (entered into force 23 June 1961), art IV(2). Territorial claims advanced by Argentina, Australia, Chile, France, the United Kingdom, New Zealand, and Norway have been 'frozen' as a result of the Treaty.

[42] *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*, 27 January 1967, 610 UNTS 205 (entered into

Nations Convention on the Law of the Sea provides that all States enjoy traditional freedoms of navigation, overflight, scientific research and fishing on the high seas, provided they cooperate with other States in managing living resources.[43] Arguably, this principle could also apply in other global commons, subject to the relevant *lex specialis*.

At least dating back to Menthe's pioneering work in 1998, commentators have periodically tried to argue that cyberspace is another of these global commons.[44] However, while doing so is useful in the sense of emphasising the need for everyone to take responsibility for avoiding a so-called 'tragedy of the commons' for cyberspace, the problems associated with such an approach are well-documented.[45]

5. WHAT ARE THE CONSEQUENCES OF HAVING SOVEREIGNTY OVER SOMETHING?

There are obvious (and less obvious) political, social, economic consequences of sovereignty. However, our focus is on those consequences of sovereignty that are a legal construct and linked with statehood. Statehood entails both rights and responsibilities.[46] Put simply, traditionally, under international law a State enjoys the ultimate entitlements of sovereignty to shoulder rights and obligations,[47] and the freedom to determine its own affairs free from intervention.[48] In other words, notions of sovereignty and the legal rights and responsibilities of statehood are interconnected concepts.

Under international law, jurisdiction is a manifestation of State sovereignty[49] and is an expression of a State's authority to make and/or

---

force 10 October 1967), art II; and *Agreement governing the Activities of States on the Moon and Other Celestial Bodies*, signed on 5 December 1979, 1363 UNTS 3 (entered into force 11 July 1984), art 11(2).

43 See generally, *United Nations Convention on the Law of the Sea*, signed on 10 December 1982, 1833 UNTS 3 (entered into force 16 November 1994).

44 Menthe, D.C. (1998) Jurisdiction in Cyberspace: A Theory of International Spaces. *Michigan Telecommunications and Technology Law Review* 4, p. 69.

45 See e.g., Svantesson, D. (2006) Borders on, or border around – the future of the Internet. *Albany Law Journal of Science & Technology*, 16 (2), pp. 343-381.

46 See e.g. Annan, K. (2005) "In Larger Freedom": Decision Time at the UN. *Foreign Affairs* (May/June 2005).

47 *Reparation for Injuries Suffered in the Service of the United Nations (Advisory Opinion)*, [1949] ICJ Rep 174, p. 180.

48 See Haass, R. N. (2003) *Sovereignty: Existing Rights, Evolving Responsibilities*. [online] Washington D.C: US Department of State. Available from: `https://2001-2009.state.gov/s/p/rem/2003/16648.htm` [Accessed 7 November 2022]. Cf. Jackson, J. H. (2003) Sovereignty-Modern: A New Approach to an Outdated Concept. *American Journal of International Law*, 97 (4) 782, p. 790; and Simonovic, I. (2002) Relative Sovereignty of the Twenty First Century. *Hastings International & Comparative Law Review*, 25, 371, p. 374.

49 *Island of Palmas Case (or Miangas) (United States v the Netherlands)*, (1949) II RIAA 829, p. 838.

enforce rules binding on natural or juridical persons, and objects.[50] Such exercise of jurisdiction can be territorial, or in the case of natural or juridical persons based on nationality.[51] As yet another attribute of sovereignty, a State may exercise discretion whether to secure the protection of a national who has been injured by another State.[52]

5.1. RIGHTS AS A CONSEQUENCE OF SOVEREIGNTY

As a consequence of sovereignty, a State is entitled to enjoy respect for its territorial sovereignty,[53] the equality of States,[54] and the right to be free from intervention in matters "which are essentially within the domestic jurisdiction of any State".[55] The latter encompasses the entitlement to freely determine the choice of political, economic, social, and cultural governance of the State,[56] and enjoying the right to formulate and conduct foreign

---

[50] See *Nationality Decrees Issued in Tunis and Morocco [French Zone], Advisory Opinion*, [1923] PCIJ Rep (Ser B) No 4, p. 24; and S.S. Lotus, (France v. Turkey), (1927) PCIJ Ser. A, No. 10, pp. 18-19.

[51] *Nationality Decrees Issued in Tunis and Morocco* [1923] PCIJ (ser 8) No B4, p. 24; *Nottebohm (Liechtenstein v. Guatemala)*, [1955], ICJ Rep 4, p. 20. See also *Convention on Certain Questions relating to the Conflict of Nationality Laws*, 12 April 1930, 179 LNTS 89 (entered into force 1 July 1937), art 1.

[52] *Mavrommatis Palestine Concessions* [1924] PCIJ (ser A) no 2, p. 1; *Nottebohm (Liechtenstein v. Guatemala)*, [1955], ICJ Rep 4, p .24; *Barcelona Traction, Light and power Company* [1970] ICJ Rep 3, paragraphs 78-79. See also International Law Commission, *Draft Articles on Diplomatic Protection*, UN Doc A/CN.4/L.684 and Corr.1-2, UN Doc A/61/10.

[53] *Case Concerning Military and Paramilitary Activities in and against Nicaragua* [1986] ICJ Rep 14, paragraphs 202, 213, 251; and *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)* [2005] ICJ Rep 168, paragraph 165. Further, as a result of sovereignty, diplomatic and consular staff enjoy diplomatic immunity, while consular premises are inviolable: see *Vienna Convention on Consular Relations*, signed on 24 April 1963, 596 UNTS 261 (entered into force 19 March 1967). See also *Case Concerning United States Diplomatic and Consular Staff in Tehran (Iran v. United States of America)* [1980] ICJ Rep 3, paragraph 77.

[54] *Charter of the United Nations*, 24 October 1945, 1 UNTS XVI, art 2(1). See also *Draft Declaration on Rights and Duties of States*, UNGAOR 4th Sess, UN Doc A/RES/375 (1949), art 5; and UNGA, *Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations*, UN Doc A/RES/2625 (XXV) (1970), Annex.

[55] *Charter of the United Nations*, 24 October 1945, 1 UNTS XVI, art 7. See also *Draft Declaration on Rights and Duties of States*, UNGAOR 4th Sess, UN Doc A/RES/375 (1949), art 3; *Convention on the Rights and Duties of States*, signed 26 December 1933, 165 LNTS 19 (entered into force 26 December 1934), art 8; and UNGA, *Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty*, UNGAOR 20th Sess, UN Doc A/RES/2131(XX) (1965), paragraph 1. See also *Case Concerning Military and Paramilitary Activities in and against Nicaragua* [1986] ICJ Rep 14, paragraphs 202, 205, 251, 288.

[56] *Case Concerning Military and Paramilitary Activities in and against Nicaragua* [1986] ICJ Rep 14, paragraph 263. See also UNGA, *Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations*, UN Doc A/RES/2625 (XXV) (1970), Annex.

policy.[57] In addition, sovereignty entails also the entitlement to exploit natural resources on its territory,[58] enforce laws in its territorial jurisdiction, and over objects and nationals within its territory,[59] and to not be the injured by another State.[60] More recent rights that have evolved as a result of decolonisation and emergence of newly independent States include the right to pursue economic and social development in a way it desires,[61] and the right to "benefit from the advances and development in science and technology".[62] Fundamentally, sovereignty also entails the right to self-preservation, which is the fundamental right to exist and the right to resort to self-defence when the State's survival is threatened.[63]

5.2. RESPONSIBILITIES RELATED TO SOVEREIGNTY

Responsibilities that arise as a consequence of sovereignty and statehood include human rights obligations owed to individuals, and relatedly, legal obligations not to engage in internationally wrongful acts. The issue of State responsibility as a consequence of sovereignty is discussed in further detail under heading 8 below. For now, on the specific consequence of owing human rights obligations, it is worth noting that international human rights

---

[57] *Case Concerning Military and Paramilitary Activities in and against Nicaragua* [1986] ICJ Rep 14, paragraph 265.

[58] *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)* [2005] ICJ Rep 168, paragraph 244; and *East Timor (Portugal v. Australia)* [1995] ICJ Rep 90, paragraph 19. See also UNGA, *Permanent sovereignty over natural resources*, UN Doc A/RES/3171 (1973), paragraphs 2-3; and UNGA, *Charter of Economic Rights and Duties of States*, UN Doc A/RES/3281(XXIX) (1974), art 2. Such rights extend also to exploit resources found in the territorial sea and exclusive economic zone: see fn 29 above.

[59] See *Convention on the Rights and Duties of States*, signed 26 December 1933, 165 LNTS 19 (entered into force 26 December 1934), art 9; and UNGA, *Draft Declaration on Rights and Duties of States*, GA Res 375(IV), UN Doc A/RES/375(IV) (1949), art 2. See also *S.S. Lotus, (France v. Turkey)* (1927) PCIJ Ser. A, No. 10, pp. 18-19. To a limited extend, a State also enjoys the right to assert jurisdiction over nationals places outside of its territory, which Bin Cheng calls 'jurisaction', which is the 'enjoyment' of State jurisdiction beyond its territory: see Cheng, B. (1965) The Extra-Territorial Application of International Law. *Current Legal Problems*, 18 (1), pp. 135-136.

[60] E.g. *Corfu Channel (United Kingdom v Albania)* [1949] ICJ Rep 4, p. 22. See also *Trail Smelter Case (United States, v Canada) (Decision of 11 March 1941)* [1949] III RIAA 1905, p. 1965. It may be noted that, injury does not necessarily need to result from an internationally wrongful act (consider e.g. transboundary pollution).

[61] See generally UNGA, *Charter of Economic Rights and Duties of States*, UN Doc A/RES/3281(XXIX) (1974), art 4; art 5; art 7; art 10; and art 12(1). This should be read in conjunction with the right to be free from political or economic coercion that results in the 'subordination of [...] sovereign rights': see UNGA, *Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations*, UN Doc A/RES/2625 (XXV) (1970), Annex.

[62] UNGA, *Charter of Economic Rights and Duties of States*, UN Doc A/RES/3281(XXIX) (1974), art 13(1)

[63] *Legality of the Use by a State of Nuclear Weapons in Armed Conflict (Advisory Opinion)* [1996] ICJ Rep 66, paragraph 96.

law, along with international criminal law, "recognises individual persons as the subject of rights and duties both between themselves and with respect to their relationship with a relevant State".[64] This links sovereignty with the relationship between States and citizens, as well between States and persons with State control. What amounts to a 'relevant State' may not always be clear in the cyber environment.

As a starting point, the Charter of the United Nations opens with a commitment to "reaffirm faith in fundamental human rights, in the dignity and worth of the human person, in the equal rights of men and women and of nations large and small".[65] This language was subsequently adopted in the Preamble of Universal Declaration of Human Rights (UDHR) in 1948.[66]

However, human rights obligations as a result of sovereignty and statehood are not limited to the geographic notions of sovereignty but can also extend to notions of effective sovereignty and power. In short, human rights obligations can apply "extraterritorially". This is the case when a State has "effective control" of a territory or a person, even if that person is outside sovereign territory. In its Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory Advisory Opinion, the International Court of Justice (ICJ) held that State parties to the International Covenant on Civil and Political Rights should be bound to comply with its provisions, even when exercising jurisdiction outside national territory.[67] This clearly has implications when applying the concept of sovereignty online.

By way of further example, in Al-Skeini and Others v the United Kingdom,[68] the European Court of Human Rights found that that the obligations of the United Kingdom (UK) under the European Convention on Human Rights (ECHR) applied in Iraq. In failing to investigate the circumstances of the killings of Iraqi civilians by UK soldiers, the UK had breached its obligations under the ECHR. An analogous reasoning could arguably be applied in relation to Internet-based situations.

In sum, consequences of sovereignty are political and legal, linked with notions of statehood, and include both sovereign rights and sovereign

[64] Freeland S. and Ireland-Piper, D. (2021) Space Law, Human Rights and Corporate Accountability. *UCLA Journal of International Law and Foreign Affairs*, 26(1), p. 6.

[65] *Ibid*.

[66] *Ibid*.

[67] *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory (Advisory Opinion)*, [2004] ICJ Rep 136, paragraph 109. See also *Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda)*, [2005] ICJ Rep 168, paragraph, 216; and *Case Concerning Application of the International Convention on the Elimination of All Forms of Racial Discrimination (Georgia v Russian Federation) (Request for the Indication of Provisional Measures)* [2008] ICJ Rep 353, paragraph 109. Note also *Bankovic v. Belgium*, 52207/99 [2001] ECHR 2001-XII.

[68] *Al-Skeini and Others v United Kingdom*, 55721/07 [2011] 1093.

responsibilities that extend beyond physical borders. This is of great significance as we move forward since it supports ideas of a sovereignty concept relying less on territoriality than the traditional notions of sovereignty have done.

6. WHO CAN VIOLATE SOVEREIGNTY?

Before seeking to canvass who can violate sovereignty, it must be admitted that not everyone agrees that sovereignty is something that can be violated. The debate about whether sovereignty is itself a binding rule of international law, or rather a principle of international law that guides State interactions but does not dictate results under international law, has been discussed in a multitude of publications,[69] including in this journal.[70] That topic will consequently not be re-visited in detail here.

But put briefly, most of the States that have expressed a view on the matter seem to have sided with the proposition that sovereignty is indeed a binding rule of international law, rather than merely a principle. Examples of States falling into this category now include the Netherlands,[71] France,[72]

[69] See e.g.: Ginsburg, T. (2017) Introduction to Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0. *American Journal of International Law Unbound*, 111, pp. 205-206, and Svantesson, D. et al (2021) *The developing concept of sovereignty: considerations for defence operations in cyberspace and outer space*, Technology and Jurisdiction Research Team, Bond University.

[70] Svantesson, D. (2018) 'Lagom jurisdiction' – What Viking drinking etiquette can teach us about Internet jurisdiction and Google France. *Masaryk University Journal of Law and Technology*, 12 (1), pp. 29-47.

[71] *Letter from the Government of the Kingdom of the Netherlands, Minister of Foreign Affairs to Parliament* (July 2019), p. 2. [online] United Nations Office for Disarmament Affairs: New York. Available from: `https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/02/appendix-Internaional-law-in-cyberspace-kingdom-of-the-netherlands.pdf` [Accessed 7 November 2022].

[72] UNGA, *Developments in the Field of Information and Telecommunications in the Context of International Security: Report of the Secretary-General*, UN Doc A/74/120 (24 June 2019) 22-6.

Austria,[73] the Czech Republic,[74] Finland,[75] Iran,[76] Japan,[77] Norway,[78] and, Germany.[79] Indeed, Osula et al correctly concluded that "there seems to be a broad agreement among 23 [European Union Member States] regarding the interpretation of sovereignty as a standalone rule, entailing both rights and obligations".[80] However, it must be noted that this apparent consensus is superficial indeed since the respective positions adopted amongst these

[73] Austria maintained that "a violation of the principle of State sovereignty constitutes an internationally wrongful act". *Comments by Austria, Pre-Draft Report of the OEWG – ICT* (31 March 2020). [online] New York: United Nations Disarmament Office. Available from: https://front.un-arm.org/wp-content/uploads/2020/04/comments-by-austria.pdf [Accessed 7 November 2022].

[74] The Czech Republic noted that it considers "the principle of sovereignty as an independent right and the respect to sovereignty as an independent obligation". *Statement by Richard Kadlčák at Open-ended Working Group on developments in the field of information and telecommunications in the context of international security of the First Committee of the General Assembly of the United Nations* (11 February 2020). [online] Prague: National Cyber and Information Security Agency, Czech Republic. Available from: https://www.nukib.cz/download/publications_en/CZ\%20Statement\%20-\%20OEWG\%20-\%20International\%20Law\%2011.02.2020.pdf [Accessed 7 November 2022].

[75] According to Finland, sovereignty is "a primary norm of public international law, a breach of which amounts to an internationally wrongful act and triggers State responsibility". Ministry for Foreign Affairs, Finland, *Finland published its positions on public international law in cyberspace* (15 October 2020). [online] Finnish Ministry of Foreign Affairs: Helsinki. Available from: https://valtioneuvosto.fi/en/-/finland-published-its-positions-on-public-international-law-in-cyberspace [Accessed 7 November 2022].

[76] See *Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace* (July 2020) [online] Tehran: Nour News. Available from: https://nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat [Accessed 7 November 2022].

[77] *Basic Position of the Government of Japan on International Law Applicable to Cyber Operations* (28 May 2021). [online] Ministry of Foreign Affairs of Japan: Tokyo, p. 3. Available from: https://www.mofa.go.jp/files/100200935.pdf [Accessed 7 November 2022].

[78] Norway in UNGA, *Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266*, UN Doc A/76/136 (2021), p. 67; and *International Law Applied to Operations in Cyberspace: Paper shared by France with the Open-ended working group established by resolution 75/240* (December 2021), p.2. [online] New York: United Nations Office of Disarmament Affairs. Available from: https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf [Accessed 7 November 2022].

[79] *On the Application of International Law in Cyberspace* (March 2021), p. 4. [online] Berlin: Ministry of Foreign Affairs, Germany. Available from: https://www.auswaertiges-amt.de/blob/2446304/2ae17233b62966a4b7f16d50ca3c6802/on-the-application-of-international-law-in-cyberspace-data.pdf [Accessed 7 November 2022].

[80] Osula, A.-M., Kasper, A. and Kajander, A. (2022) EU Common Position on International Law and Cyberspace. *Masaryk University Journal of Law and Technology*, 16 (1), p. 114.

states differ, or are silent, on the circumstances in which sovereignty is in fact violated.

The main proponents for sovereignty to be viewed as a principle rather than a rule are UK and at one stage the United States (US).[81] For example, the UK has articulated the position that sovereignty is "fundamental to the international rules-based system" but that there is no "specific rule or additional prohibition" for cyber activities that fall below the use of force and intervention thresholds,[82] and that "there is no such rule as a matter of current international law".[83] Furthermore, according to a 2017 US Department of Defense memo, the law does not presently support the proposition that "sovereignty acts as a binding legal norm" relevant to cyber activities.[84] Yet other States have managed to adopt both of the views noted above.[85]

Authoritarian States have a history of using sovereignty as a shield against foreign criticism of what they see as purely domestic affairs.[86] Thus, while most States have noted that certain cyber activities may violate State sovereignty, China has asserted that "[s]overeignty in cyberspace is the internal supremacy and external independence that States enjoy".[87]

Having made these important observations, we can now turn to the question of who can violate sovereignty, assuming sovereignty can be violated. While under international law, sovereignty attaches to States, sovereignty can be violated by States as well as non-State actors alike. Conduct that is directed or controlled by a State can be attributed to that

---

[81] See further Heller, K. J. (2021) In Defense of Pure Sovereignty in Cyberspace. *International Law Studies*, 97, p. 1436.

[82] Wright, J. (2018) *Cyber and International Law in the 21st Century.* Speech, Chatham House, Royal Institute of International Affairs. [online] London: Government of the United Kingdom. Available from https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century [Accessed 7 November 2022].

[83] *Ibid.*

[84] O'Connor, J. M. 'International Law Framework for Employing Cyber Capabilities in Military Operations' (Memorandum, 19 January 2017), p. 3.

[85] *The Application of International Law to State Activity in Cyberspace* (1 Dec 2020). [online] New Zealand Foreign Affairs & Trade: Wellington. Available from: `https://dpmc.govt.nz/sites/default/files/2020-12/The\%20Application\%20of\%20International\%20Law\%20to\%20State\%20Activity\%20in\%20Cyberspace.pdf` [Accessed 12 December 2022].

[86] Österdahl traces back the origin of "information sovereignty" to a former Soviet concept implying "that the State has a right to control the dissemination of information within its territory. The State according to this doctrine has the right to control the news flowing out of the country and the news coming in". Østerdahl, I. (1992) *Freedom of Information in Question: Freedom of information in international law and the calls for a New World Information and Communication Order (NWICO).* Uppsala: Iustus Förlag AB, p. 137.

[87] See China, *China's Views on the Application of the Principle of Sovereignty in Cyberspace* (2022), submitted to the Open-ended Working Group on security of and in the use of information and communications technologies, sec I and sec III.

State, and thereby cause a violation of other States' sovereignty.[88] Conduct of private persons that is acknowledged and adopted by a State as its own can also violate the sovereignty of another State.[89] Of course, in such a situation, an argument could be made that it then is the State acknowledging and adopting the conduct of private persons that conducts the violation. That, however, is a discussion into which we need not enter here.

The situations that generally are easiest to assess are violations by States. A State, by virtue of its acts, can violate the sovereignty of another. Thus, for example, in allowing its satellite to crash on Canadian territory, the Soviet Union was said to violate Canada's sovereignty and interfere "with the sovereign right of Canada to determine the acts that will be performed on its territory".[90]

Often, the difficulty – especially online – is the issue of attribution. Under international law, acts carried on by governmental agencies are directly attributable to the State,[91] and this includes any person or entity which has that status in accordance with the internal law of the State.[92] The conduct of soldiers and the armed forces are clearly attributable to the State.[93] As under international law a State is not responsible for conduct of individuals or private entities, for acts of non-governmental entities to be violative of sovereignty, the act must be attributable to that State.

Sovereignty also entails a corollary duty "to protect within the territory the rights of other States".[94] Thus, in Corfu Channel, the ICJ held that it is "every State's obligation not to allow knowingly its territory to be used for

[88] UNGA, *Responsibility of States for Internationally Wrongful Acts*, 53 UN GAOR Supp, UN Doc A/56/83 (2002), Annex, art 8. See *Case Concerning Military and Paramilitary Activities in and against Nicaragua* [1986] ICJ Rep 14, paragraphs 86, 115 ["effective control"]; cf. The Prosecutor v. Dusko Tadić, IT-94-1-AR72, Appeals Chamber, Decision, 2 October 1995, paragraph 120 ["overall control"]; see also and *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)*, [2007] ICJ Rep 43, paragraphs 406-407; *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda)*, [2005] ICJ Rep 168, paragraph 160.

[89] UNGA, *Responsibility of States for Internationally Wrongful Acts*, 53 UN GAOR Supp, UN Doc A/56/83 (2002), Annex, art 11. See also *United States Diplomatic and Consular Staff in Tehran*, [1980] ICJ Rep 3, paragraph 74.

[90] *Canada: Claim Against the Union of Soviet Socialist Republics for Damage Caused by Soviet Cosmos 954* (1979), Annex A: Statement of Claim. International Legal Materials, 18 (4), paragraph 21.

[91] UNGA, *Responsibility of States for Internationally Wrongful Acts*, 53 UN GAOR Supp, UN Doc A/56/83 (2002), Annex, art 4. See *Difference Relating to Immunity from Legal Process of a Special Rapporteur of the Commission on Human Rights, Advisory Opinion* [1999] ICJ Rep 62, paragraph 62; and *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)*, [2007] ICJ Rep 43, paragraph 385.

[92] UNGA, *Responsibility of States for Internationally Wrongful Acts*, 53 UN GAOR Supp, UN Doc A/56/83 (2002), Annex, art 4(2).

[93] *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)* [2005] ICJ Rep 168, paragraphs 213-214.

[94] *Island of Palmas Case (the Netherlands v. United States of America)* (1928) 2 RIAA 829, p. 839.

acts contrary to the rights of other States".[95] Such violations of sovereignty may be caused by activities undertaken by the State itself, or by entities or persons under the jurisdiction and control of the State. A State may therefore find itself held responsible for allowing transboundary pollution to injure the interests of other States.[96] Similarly, where a State allows its territory to be used for cyber attacks on another state, it may be in violation of international law.[97]

The UN Charter provides that States must "refrain [...] from the threat or use of force against the territorial integrity or political independence of any State".[98] Therefore, a State can violate the sovereignty of another State, typically through use of the armed forces. However, *Nicaragua* demonstrates that *contras*, or irregular forces or armed bands can also violate sovereignty.[99] Indeed, the Friendly Relations Declaration obliges States "to refrain from organizing or encouraging the organization of irregular forces or armed bands including mercenaries, for incursion into the territory of another State".[100] This may have implications for cyber operations involving what may be seen as 'irregular forces' such as some forms of 'cyber militia'; be as it may that the definition of 'incursion' may be critical in the cyber context.

The UN Charter foresees the potential violations of sovereignty and empowers the Security Council to act to threats to the peace, breaches of the peace and acts of aggression.[101] Thus, the Security Council may employ "measures not involving the use of armed force"[102] or "take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security".[103] However, as seen in relation to the Russian aggression in Ukraine, the value of this power is limited when the aggressor is a member of the Security Council.

---

[95] *Corfu Channel (United Kingdom v Albania) [1949] ICJ Rep 4, p. 22. See also Trail Smelter Case (United States, v Canada)* (Decision of 11 March 1941), [1949] III RIAA 1905, p. 1965; and *Pulp Mills on the River Uruguay (Argentina v. Uruguay)*, [2010] ICJ Rep 14, paragraph 101.

[96] *Trail Smelter Case (United States v Canada)* (Decision of 11 March 1941), [1949] III RIAA 1905.

[97] See Coco, A. and de Souza Dias, T. (2021) "Cyber Due Diligence": A Patchwork of Protective Obligations in International Law. *European Journal of International Law* 32 (3), p. 771.

[98] *Charter of the United Nations*, 24 October 1945, 1 UNTS XVI, art 2(4).

[99] *Case Concerning Military and Paramilitary Activities in and against Nicaragua* [1986] ICJ Rep 14, paragraphs 251-252.

[100] UNGA, *Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations*, UN Doc A/RES/2625 (XXV) (1970), Annex, paragraph 1. See also UNGA, *Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations*, UN Doc A/RES/42/22 (1988), I, paragraph 5. See also *Case Concerning Military and Paramilitary Activities in and against Nicaragua* [1986] ICJ Rep 14, paragraphs 195, 228.

[101] *Charter of the United Nations*, 24 October 1945, 1 UNTS XVI, art 2(7).

[102] *Ibid*, art 41.

[103] *Ibid*, art 42.

Finally, it may be noted that humanitarian interventions in Kosovo, Haiti and Bosnia Herzegovina suggest that sovereignty violations by a "coalition of the willing" to prevent widespread human rights abuses and stem the breaches of humanitarian law in conflict situations may legitimatise what otherwise would be a violation.[104] Put differently, most international lawyers would say that what occurred in those instances was, technically, a violation of the prohibition on the use of force (and thus an unlawful intervention and violation of sovereignty) but that it was 'legitimate' given it was done for humanitarian reasons.[105] This may be seen as a developing area of international law in relation to which the cyber implications have not yet fully been canvassed. However, one thing is clear, it certainly points to a degree of flexibility.

7. WHAT IS THE THRESHOLD FOR VIOLATING SOVEREIGNTY?

As already noted, there are those who take the view that sovereignty is not of a nature to be 'violated' and for them, the question of what may be the threshold for violating sovereignty is of course nonsensical. Here, we will proceed on the basis that sovereignty may indeed be the object of violation. We first outline what may be seen as the standard views on the topic of the threshold for violating sovereignty, and then proceed to provide details about a possible future direction; it is in relation to this crucial question we have concentrated our law reform proposals.

7.1. THE CURRENT STANDARD POSITION

In the cyber context, it may be said that there are two bases on which a violation of sovereignty can be established. First, where there is a violation of a State's territorial integrity; and second, where there is interference or usurpation of inherently governmental functions. This approach originated from the Tallinn Manual, and a number of States have expressed support for this approach.[106] Violations of territorial sovereignty are predominantly determined based on the significance of the effects caused by the cyber

[104] Simonovic, I. (2002) Relative Sovereignty of the Twenty First Century. H*astings International & Comparative Law Review*, 25, p. 373.

[105] However, in Corfu Channel, the ICJ warned against the "alleged right of intervention", which in the past has "given rise to the most serious abuses" by particularly the "most powerful States and might easily lead to perverting the administration of international justice itself": *Corfu Channel (United Kingdom v Albania)* [1949] ICJ Rep 4, pp. 34-35. See also Henkin, L. (1994) The Mythology of Sovereignty. In: RStJ Macdonald (ed.) *Essays in Honour of Wang Tieya*. Martinus Nijhoff: Dordrecht, p. 358).

[106] Schmitt, M. (ed.) (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd ed. Cambridge: Cambridge University Press, p. 20.

operation, and generally this requires physical effects to occur. Violations of sovereignty on the second basis can occur irrespective of the nature of the effects caused by the cyber operation, provided it involves interference with or usurpation of inherently governmental functions.

7.1.1 Violations of territorial sovereignty

In relation to the first basis, the Tallinn Manual experts agreed that cyber operations causing physical effects in the territory of another State would constitute a violation of sovereignty.[107] However, the experts were divided on the threshold at which cyber operations causing loss of functionality would violate sovereignty on this basis. Here they agreed that disruptions requiring repair or replacement of hardware components would be sufficient (this was likened to physical damage), but there was no consensus about disruption requiring reinstallation of software.[108] The experts could not reach consensus on whether cyber operations that do not damage hardware or disrupt the functionality of systems would amount to a violation of territorial sovereignty.[109]

This is important not least in that it highlights just how limited agreement there is on this topic; far from all States embrace the Tallinn Manual, and even in the Group of Experts drafting it, there was significantly divergent opinions on key matters such as this.

A number of States have adopted the position that cyber operations can violate territorial sovereignty where significant effects are caused. For example, according to the Czech Republic, cyber operations that cause significant physical damage or harm to individuals, and those that damage or disrupt the operation of cyber or other infrastructure where it has a "significant impact on national security, economy, public health or environment" will constitute violations of sovereignty.[110] Similarly, Germany

[107] This was likened to a non-consensual physical presence on a State's territory and was considered to be "consistent with object and purpose of principle of sovereignty, which clearly protects territorial integrity against physical violation". *Ibid*, p. 20.

[108] *Ibid*, p. 21.

[109] *Ibid*, p. 21. Those who argued that these cyber operations would violate territorial sovereignty provided the examples of cyber operations that cause another State's cyber infrastructure or programs to operate differently; cyber operations that involve altering or deleting data; the installation of malicious software or backdoors; and DdoS attacks causing temporary but significant disruptions to the functioning of systems. This argument was premised on the object and purpose of sovereignty as a principle, and the notion that States have the right to full access and control over cyber activities on their territory.

[110] *Statement by Richard Kadlčák at Open-ended Working Group on developments in the field of information and telecommunications in the context of international security of the First Committee of the General Assembly of the United Nations* (11 February 2020). [online] Prague: National Cyber and Information Security Agency, Czech Republic. Available

maintains that a cyber operation that causes "physical effects and harm" in another State's territory will violate sovereignty, as well as disruptive cyber operations particularly where they cause "substantive secondary or indirect physical effects" in another State's territory.[111] Norway gives the example of a cyber operation causing physical damage, such as a fire at a petrochemical plant, and one causing a loss of functionality, such as encrypting the data of systems that renders them "unusable for a substantial period of time".[112] Canada also provides that a cyber operation must "rise above a level of negligible or de minimis effects" and cause "significant harmful effects within the territory of another State without that State's consent" for a violation of sovereignty to occur.[113]

A minority of States consider cyber operations below the threshold of significant effects or loss of functionality to violate territorial sovereignty. According to France, a cyber operation that involves the "unauthorised penetration" of its computer systems may constitute a violation of its sovereignty.[114] Iran similarly maintains that any unlawful intrusions into its cyber infrastructure constitute violations of its sovereignty.[115] However, most other States require cyber operations to cause significant physical effects to constitute violations of sovereignty on this basis, though there remains some uncertainty about the precise threshold.

---

from: https://www.nukib.cz/download/publications_en/CZ\%20Statement\%20-\%20OEWG\%20-\%20International\%20Law\%2011.02.2020.pdf [Accessed 7 November 2022]

[111] *On the Application of International Law in Cyberspace* (March 2021), p. 4. [online] Berlin: Ministry of Foreign Affairs, Germany. Available from: https://www.auswaertiges-amt.de/blob/2446304/2ae17233b62966a4b7f16d50ca3c6802/on-the-application-of-international-law-in-cyberspace-data.pdf [Accessed 7 November 2022].

[112] *Norwegian positions on selected questions of international law relating to cyberspace* (May 2021), p. 3. [online] Oslo: Government of Norway. Available from https://www.regjeringen.no/contentassets/a8911fc020c94eb386a1ec7917bf0d03/norwegian_positions.pdf [Accessed 7 November 2022].

[113] *International law applicable in cyberspace* (4 April 2022). [online] Ottawa: Global Affairs Canada, paragraph 15. Available from: https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng [Accessed 7 November 2022].

[114] United Nations Secretary-General, I, UN Doc A/74/120 (24 June 2019), p. 22. Some scholars have expressed support for a similar position: see Buchan, R. (2018) *Cyber Espionage and International Law*. Oxford: Hart, p. 54; and Delerue, F. (2020) *Cyber Operations and International Law*. Cambridge: Cambridge University Press, p. 214.

[115] *Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace* (July 2020) [online] Tehran: Nour News. Available from: https://nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat [Accessed 7 November 2022].

7.1.2 Violations of sovereignty on the basis of interference or usurpation of government functions

In relation to the second basis, the Tallinn Manual experts maintained that a violation of sovereignty occurs where a cyber operation interferes with or usurps inherently governmental functions. In this context they argued that there is no need for a threshold of physical effects or disruption to the functionality of systems.[116] As examples of cyber operations that interfere with inherently governmental functions, the Tallinn Manual experts said that this occurs where a State "changes or deletes data such that it interferes with the delivery of social services, the conduct of elections, the collection of taxes, the effective conduct of diplomacy, and the performance of key national defence activities" in another State.[117] In relation to usurpation of inherently governmental functions, the Tallinn Manual experts gave the example of exercising law enforcement functions without the State's consent.[118]

Recently, a growing number of States have adopted the position that a violation of sovereignty can also occur on this basis. Canada maintains that cyber operations with "significant harmful effects on the exercise of inherently governmental functions" violate international law "regardless of whether there is physical damage, injury, or loss of functionality".[119] It outlines inherently government functions to include "health care services, law enforcement, administration of elections, tax collection, national defence and the conduct of international relations, and the services on which these depend".[120] A violation of sovereignty could occur on this basis where a cyber operation "interrupts health care delivery by blocking access to patient health records or emergency room services, resulting in risk to the health or life of patients".[121]

Norway also adopts the Tallinn Manual approach that a violation of sovereignty can occur on this basis, and this is irrespective of "whether

[116] Schmitt, M. (ed.) (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd ed. Cambridge: Cambridge University Press, pp. 21-22.
[117] *Ibid*, p. 22.
[118] The example given in this context is where a state conducts a law enforcement operation against a botnet in order to gather evidence in a criminal prosecution: Schmitt, M. (ed.) (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd ed. Cambridge: Cambridge University Press, p. 22.
[119] *International law applicable in cyberspace* (4 April 2022). [online] Ottawa: Global Affairs Canada, paragraph 18. Available from: `https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng` [Accessed 7 November 2022]
[120] *Ibid.*
[121] *Ibid.*

physical damage, injury, or loss of functionality has resulted".[122] It maintains that the precise threshold is not settled, and this will be assessed on a case-by-case basis. But Norway does provide examples of situations where a violation would occur. These include "altering or deleting data or blocking digital communication between public bodies and citizens so as to interfere with the delivery of social services, the conduct of elections, the collection of taxes, or the performance of key national defence activities".[123] Further, it provides that a violation would occur where a cyber operation manipulates "police communications so that patrol cars are unable to communicate with police dispatch/operation centres".[124] The Czech Republic maintains that a violation of sovereignty occurs on this basis where there is a significant disruption to inherently government functions.[125] It gives the example of "distributing ransomware which encrypts the computers used by a government and thus significantly delaying the payment of retirement pensions".[126]

A number of other States, including New Zealand,[127] the Netherlands,[128] Switzerland,[129] and Sweden,[130] also maintain that a violation of sovereignty

[122] *Norwegian positions on selected questions of international law relating to cyberspace* (May 2021), p. 4. [online] Oslo: Government of Norway. Available from https://www.regjeringen.no/contentassets/a8911fc020c94eb386a1ec7917bf0d03/norwegian_positions.pdf [Accessed 7 November 2022].

[123] *Ibid*.

[124] *Ibid*.

[125] *Statement by Richard Kadlčák at Open-ended Working Group on developments in the field of information and telecommunications in the context of international security of the First Committee of the General Assembly of the United Nations* (11 February 2020), p. 3 [online] Prague: National Cyber and Information Security Agency, Czech Republic. Available from: https://www.nukib.cz/download/publications_en/CZ\%20Statement\%20-\%20OEWG\%20-\%20International\%20Law\%2011.02.2020.pdf [Accessed 7 November 2022].

[126] *Ibid*.

[127] The Application of International Law to State Activity in Cyberspace (1 Dec 2020), paragraph 11. [online] New Zealand Foreign Affairs & Trade: Wellington. Available from: https://dpmc.govt.nz/sites/default/files/2020-12/The\%20Application\%20of\%20International\%20Law\%20to\%20State\%20Activity\%20in\%20Cyberspace.pdf [Accessed 12 December 2022].

[128] *Letter from the Government of the Kingdom of the Netherlands, Minister of Foreign Affairs to Parliament* (July 2019), p. 3. [online] New York: United Nations Office for Disarmament Affairs. Available from: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/02/appendix-Internaional-law-in-cyberspace-kingdom-of-the-netherlands.pdf [Accessed 7 November 2022].

[129] *Switzerland's position paper on the application of international law in cyberspace* (2021), p. 3. [online] Bern: Federal Department of Foreign Affairs, Switzerland. Available from: https://www.eda.admin.ch/content/dam/eda/en/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_EN.pdf [Accessed 7 November 2022].

[130] *Position Paper on the Application of International Law in Cyberspace* (2022), p. 2. [online] Stockholm: Government of Sweden. Available from: https://www.regeringen.

can occur on this basis but do not provide further detail on their positions or examples of situations where this may occur. The Swiss and Swedish positions provide that this is assessed on a case-by-case basis depending on the nature and effects of the incident.[131] Accordingly, many States have expressed support for the Tallinn Manual's approach to violations of sovereignty either on the basis of territorial sovereignty where the effects are significant, or on the basis of interference or usurpation of inherently governmental functions irrespective of whether there are physical effects or not.

Importantly, the above shows that there is already a degree of detachment between sovereignty and territoriality. That is, while violations of sovereignty can occur through effects equivalent to a physical intrusion into a State's territory, many States are also recognising that sovereignty can be violated where cyber operations without physical effects interfere with or usurp government functions. This may arguably be seen to support the feasibility of our proposal below.

7.2. A POSSIBLE PATH FORWARD

While we hasten to acknowledge that just about everything we have said so far lacks worldwide consensus, it nevertheless represents a viable description of what may be viewed as the closest thing we have to a consensus position. In the remaining discussion in this section, we turn our focus to a possible law reform option. In doing so we build on an idea first canvassed in 2017,[132] and that has been elaborated upon in an, at the time of writing, forthcoming book chapter. We here aim to take that proposal one step further by providing additional clarifications and some views of its practical application.

---

se/4a1ce0/contentassets/2bf3882c23bb4fdfb935310b03d562a1/swedens-position-paper-on-the-application-of-international-law-in-cyberspace.pdf [Accessed 7 November 2022].

[131] *Switzerland's position paper on the application of international law in cyberspace* (2021), p. 3. [online] Bern: Federal Department of Foreign Affairs, Switzerland. Available from: https://www.eda.admin.ch/content/dam/eda/en/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_EN.pdf [Accessed 7 November 2022]; *Position Paper on the Application of International Law in Cyberspace* (2022), p. 2. [online] Stockholm: Government of Sweden. Available from: https://www.regeringen.se/4a1ce0/contentassets/2bf3882c23bb4fdfb935310b03d562a1/swedens-position-paper-on-the-application-of-international-law-in-cyberspace.pdf [Accessed 7 November 2022].

[132] Polcak, R. and Svantesson, D. (2017) *Information Sovereignty – Data Privacy, Sovereign Powers and the Rule of Law*. Cheltenham: Edward Elgar Publishing, p. 64.

7.2.1 Briefly about the proposal

As noted in the introduction, one key problem with sovereignty in the cyber context, and specifically with attempts at canvassing a threshold for violations of sovereignty, is the fact that sovereignty – under the conventional thinking – is largely grounded in a territoriality thinking. As is now widely accepted, this territoriality thinking is a poor fit with the online environment.[133] Relatedly, due to the focus on a territoriality thinking, the traditional notion of sovereignty is – to a great extent – something binary, and also this is a poor fit with what we are dealing with in the concept of sovereignty.

In an attempt to address these weaknesses, it is suggested that we can anchor sovereignty in the concept of 'State dignity':

> an infringement of sovereignty would only result in legal consequences where it impacts the dignity of the state in question. In this sense, the reference to dignity would work like a filter, sorting actions according to the level of infringement in which they result. In other words, the function would be similar to how the requirement of actual harm filters the severity of actions in relation to certain torts (such as injurious falsehood).[134]

As infringements of State dignity may be assessed as a matter of degree,

[133] See further Svantesson, D. (2017) *Solving the Internet Jurisdiction Puzzle*. Oxford: Oxford University Press; Handl, G. et al. (eds.) (2012) *Beyond Territoriality*, The Hague: Martinus Nijhoff; Mills, A. 'Rethinking Jurisdiction in International Law', 84(1) *British Yearbook of International Law* (2014) pp. 187-239; Slaughter, A. 'The Future of International Law Is Domestic (or, The European Way of Law)', 47(2) *Harvard International Law Journal* (2006) pp. 327-352; Schiff Berman, P. (2014) Global Legal Pluralism: A Jurisprudence of Law beyond Borders, Cambridge: Cambridge University Press; Oster, J. 'Rethinking Shevill. Conceptualising the EU private international law of Internet torts against personality rights', 26(2-3) *International Review of Law, Computers & Technology* (2012) pp. 113-128; Schultz, T. 'Carving up the Internet: Jurisdiction, Legal Orders, and the Private/ Public International Law Interface', 19(4) *European Journal of International Law* (2008) pp. 799-839; Cooper, D. and C. Kuner, C. 'Data Protection Law and International Dispute Resolution', 382 R*ecueil des Cours of the Hague Academy of International Law* (2017) pp. 1-174; C. Ryngaert, C. and Zoetekouw, M. 'The End of territory? The e-emergence of community as a principle of jurisdictional order in the Internet era', in Kohl, U. (ed.) (2017) *The Net and the Nation State: Multidisciplinary Perspectives on Internet Governance*, Cambridge: Cambridge University Press, pp. 185-201; Keyes, M. (2005) *Jurisdiction in International Litigation*, Sydney: The Federation Press, p. 181; Ubertazzi, B. (2012) Exclusive Jurisdiction in Intellectual Property, Tübingen: Mohr Siebeck; Cooper, D. et al. (eds.) 'Data protection law and international dispute resolution', 382 *Recueil des Cours of the Hague Academy of International Law* (2017); and Orakhelashvili, A., 'State Jurisdiction in International Law: Complexities of a Basic Concept', in Orakhelashvili, A. (ed.) (2015), *Research Handbook on Jurisdiction and Immunities in International Law*, Cheltenham: Edward Elgar Publishing, Chapter 1

[134] Polcak, R. and Svantesson, D. (2017) *Information Sovereignty – Data Privacy, Sovereign Powers and the Rule of Law*. Cheltenham: Edward Elgar Publishing, p. 64.

we can steer away from sovereignty as something binary when anchoring sovereignty in State dignity. In more detail, while an act either does, or does not, take place on a given State's territory (binary), a State's dignity may be assessed as negligibly or severely impacted or anything in between (a matter of degree). Importantly then, when working with the State dignity concept we need to maintain this characteristic of it being a matter of degree rather than be seen as a distinct threshold for sovereignty infringements; otherwise, it ends up being as binary as the current – territoriality-based – approach to sovereignty. This clearly has implications for how we approach the consequences of sovereignty infringements.

Further, infringements of State dignity need not be assessed from the traditional perspective tied to territoriality, so by anchoring sovereignty in State dignity, we can free it from its territoriality focus. Admittedly, without more, we are still confronted with a vague test that is little more than a 'wet finger in the air' type test whereby one abstract concept is traded for another. Yet the practical advantages over the current conception of sovereignty – in particular the move from a largely binary concept anchored in territoriality to a nuance-recognising concept free from territoriality – should not be underestimated.

Furthermore, it is possible to point to an important ideological basis for the proposed change. As the world has become increasingly 'civilised', it should be natural to undertake a shift from sovereignty as a territoriality-focused concept based on physical control (strengths) to a more sophisticated normative concept based on mutual respect and the rules of international law (rights).[135]

[135] As noted by Khan:

> [I]n recent years there are increasing signs that the traditional and rather categorical symbiosis between territory and power may no longer lay a legitimate claim for exclusivity. This is hardly deplorable since from an international law perspective, possession and transfer of territory have never been considered an end in itself. *L'obsession du territoire* of modern States was always meant to serve people, not vice versa.

Khan, D.E. (2012) Territory and Boundaries. In: Fassbender, B. and Peters, A. (eds.) *The Oxford Handbook of The History of International Law*. Oxford: Oxford University Press, p. 248 (footnote omitted). But given the direction the world is heading, we understand the point of view of those who would argue that perhaps we have missed the window of opportunity for this change and increased sophistication.

7.2.2 A demonstration of the proposal

Imagine that State A undertakes a cyber-attack with serious societal implications – important research data is deleted, and patient records manipulated making it impossible to safely carry out medical procedures – in the victim state (State B). Under the conventional approach to sovereignty, we would presumably start by asking whether the affected cyber infrastructure was located on the territory of State B. For example, as noted by Heller, Switzerland asserts that "State sovereignty protects information and communication technologies (ICT) infrastructure on a State's territory against unauthorised intrusion or material damage," including "computer networks systems and software supported by the ICT infrastructure, regardless of whether the infrastructure is private or public".[136] Thus, the physical location of the ICT infrastructure becomes central.

In contrast, under the State dignity focused approach, it would not matter whether State B had used local cyber infrastructure or a cloud-based structure wholly or partly abroad – attention would be placed on the degree to which State A's action infringes State B's dignity. Another advantage is that the proposed structure also recognises that an attack on 100 small 'soft targets' may be a serious attack even if none of those targets individually meet the threshold of e.g., being critical infrastructure on the territory of the victim State.[137]

The idea of anchoring sovereignty in the concept of State dignity may also be used to explain some of the "anomalies" in how sovereignty operates.

---

[136] Heller, K. J. (2021) In Defense of Pure Sovereignty in Cyberspace. *International Law Studies*, 97, p. 1459, referring to Directorate of International Law, Federal Department of Foreign Affairs, Switzerland's Position Paper on the Application of International Law in Cyberspace, UN GGE 2019/2021 (2021), annex at 2. [online] Switzerland Federal Department of Foreign Affairs: Bern. Available from: https://www.eda.admin.ch/dam/eda/en/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_EN.pdf [Accessed 7 November 2022].

[137] In this respect there are similarities to the so-called "accumulation of events doctrine": see further: Kudláčková, I., Wallace, D. and Harašta, J. Cyber Weapons Review in Situations Below the Threshold of Armed Conflict. In Jančárková, T. et al (Eds.) *20/20 Vision: The Next Decade*. Tallinn: NATO CCDCOE Publications. Available from: https://ccdcoe.org/uploads/2020/05/CyCon_2020_6_Kudlackova_Wallace_Harasta.pdf [Accessed 20 April 2023]; Delerue, F. (2020) *Cyber Operations and International Law*. Cambridge: Cambridge University Press, pp. 334-5; Francisco Lobo, J. (2018) One Piece at a Time: The 'Accumulation of Events' Doctrine and the 'Bloody Nose' Debate on North Korea. [online] Lawfare Blog. Available from: https://www.lawfareblog.com/one-piece-time-accumulation-events-doctrine-and-bloody-nose-debate-north-korea [Accessed 20 April 2023]; and McLaughlin, M. (2023) Deterring the Next Invasion: Applying the Accumulation of Events Theory to Cyberspace. [online] Opinio Juris. Available from: http://opiniojuris.org/2023/03/02/deterring-the-next-invasion-applying-the-accumulation-of-events-theory-to-cyberspace/) [Accessed 20 April 2023].

For example, as discussed above, current thinking on international law may seek to explain the humanitarian interventions in Kosovo, Haiti, and Bosnia Herzegovina as instances that, technically, were violations of sovereignty but that were 'legitimate' given the humanitarian reasons. However, arguably a better explanation is that these humanitarian interventions – given their context – did not violate any State dignity. Thus, while some commentators no doubt will point to the risk of the flexibility of the State dignity concept being exploited, it may equally well be argued that this flexibility is already in place and that anchoring sovereignty in the concept of State dignity is merely a more honest and transparent way to accommodate this flexibility.

Indeed, in some ways anchoring sovereignty in the concept of State dignity may provide a degree of rigour where there is none today. As noted above, authoritarian States have a history of using sovereignty as a shield against foreign criticism of what they see as purely domestic affairs. Imagine, for example, that a certain State (State C) mistreats a domestic minority in violation of their fundamental human rights, and that State C imposes a ban on information about the human rights violations being communicated to the citizens of State C. Under the current thinking on sovereignty, State C may argue that any other State communicating such information to the citizens of State C violates State C's sovereignty. Such misuse of sovereignty would not be possible if we adopt the idea of anchoring sovereignty in the concept of State dignity since it is State C's own conduct that undermines its dignity rather than the information that brings the human rights violations into the spotlight.

7.2.3 More about State dignity

While adding some clarifying examples, the above has mainly summarised what has already been proposed elsewhere. However, we will here seek to add to the picture painted so far by exploring further the concept of State dignity in some detail. In this context, it should be noted that we seek to draw upon a broad range of sources that deal with the concept of State dignity (and indeed dignity more broadly). Thus, we make no claim that all these sources ought to be authoritative for how we understand the concept of State dignity. We do, however, see all these sources as informative for how we understand the concept of State dignity.

The dignity, honour, or prestige of a State[138] or nation has been "described

[138] *Case concerning the difference between New Zealand and France concerning the interpretation or application of two agreements, concluded on 9 July 1986 between the two States and which related to the problems arising from the Rainbow Warrior Affair*, (1990) XX RIAA 215, paragraphs 108-109.

as a fundamental endowment of a sovereign and equal subject".[139] As a related concept to State sovereignty, there have been many instances where States have explicitly invoked or referenced the notion of State or national dignity.

For example, after the downing of a Russian Sukhoi Su-24M attack aircraft in 2015, Russia imposed economic sanctions on Turkey, to which Turkey's President Erdogan responded that such actions were not "in line with 'State dignity'".[140] Former Iranian president Rouhani invoked "protecting national dignity and standing against world powers",[141] while China recently underscored support "safeguarding [Iran's] sovereignty and national dignity".[142] When Kiribati and the Solomon Islands decided to recognise the People's Republic of China, the government of Taiwan terminated diplomatic relations "with immediate effect to uphold national dignity".[143] The Democratic People's Republic of Korea often invokes the "dignity and sovereignty of the state"[144] when defending against what

[139] Fitzgerald, J. (2006) The Dignity of Nation. In: Chien, S. Y. S. and Fitzgerald, J. (eds.) *The dignity of nations: equality, competition, and honor in East Asian nationalism*. Hong Kong: Hong Kong University Press, pp. 1, 3. This notion of dignity should be distinguished from the obligation of the receiving State to protect consular premises against impairment of the 'dignity' of consular premises under the Vienna Convention on Consular Relations: see *Vienna Convention on Consular Relations*, signed on 24 April 1963, 596 UNTS 261 (entered into force 19 March 1967), arts 31, 59. See also *Case Concerning United States Diplomatic and Consular Staff in Tehran (Iran v. United States of America)* [1980] ICJ Rep 3, paragraph 77.

[140] Al Arabia. (2 December 2015) *Turkey won't retaliate against Russia's sanctions*. [online] Dubai: Al Arabia. Available from: `https://english.alarabiya.net/News/middle-east/2015/12/02/Erdogan-vows-no-retaliation-against-Russian-sanctions` [Accessed 7 November 2022].

[141] *President at the inauguration ceremony of direct reduction plant: Iranian nation unsanctionable/We'll negotiate anywhere necessary for nation's interests*, press statement (11 November 2019). [online] Tehran: Ministry of Foreign Affairs of the Islamic Republic of Iran. Available from: `https://en.mfa.gov.ir/portal/NewsView/568055` [Accessed 7 November 2022].

[142] *President Xi Jinping Meets Iranian President Ebrahim Raisi* (16 September 2022). [online] Beijing: Ministry of Foreign Affairs of the People's Republic of China. Available from: `https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/202209/t20220916_10766906.html` [Accessed 7 November 2022].

[143] *The R.O.C. (Taiwan) government terminates diplomatic relations with Solomon Islands with immediate effect to uphold national dignity* (16 September 2019). [online] Taipei: Ministry of Foreign Affairs of the Republic of China (Taiwan). Available from: `https://en.mofa.gov.tw/News_Content.aspx?n=1330&sms=274&s=34155` [Accessed 7 November 2022]; and *The R.O.C. (Taiwan) government terminates diplomatic relations with Republic of Kiribati with immediate effect to uphold national dignity* (20 September 2019). [online] Taipei: Ministry of Foreign Affairs of the Republic of China (Taiwan). Available from: `https://en.mofa.gov.tw/News_Content.aspx?n=1330&s=34156` [Accessed 7 November 2022].

[144] See e.g. *Statement of Spokesman for DPRK Foreign Ministry* (5 November 2022). [online] Pyongyang: Ministry of Foreign Affairs of the Democratic People's Republic of Korea. Available from: `http://www.mfa.gov.kp/view/article/16089` [Accessed 7 November 2022]; and *Country-Specific "Special Rapporteur" Mechanism Must Be Abolished Immediately* (17 October 2022). [online] Pyongyang: Ministry of Foreign Affairs of the

it sees as interference with its domestic affairs. Further, in response to sanctions imposed as a result of the treatment of Uyghurs in Xinjiang, the Ministry of Foreign Affairs of China expressed that China vows to "take forceful measures to firmly defend its own interests and dignity",[145] while Chinese Communist Party Chairman Xi Jinping defended accelerating military development as being necessary for the "rejuvenation of the Chinese nation' and to 'safeguard China's dignity and core interests".[146]

Damage to State dignity or reputation has not just been referenced by the State that feels such emotional attributes have been violated. In 2021, while accusing the Chinese Ministry of State Security of carrying out cyber-attacks to steal intellectual property, then Australian Home Affairs Minister underscored that the public attribution of such attacks means "significant reputational damage to China".[147]

It has been said that "[r]eferences to national dignity usually surface when [S]tates have little to fall back on but their dignity", and this is particularly the case for regimes that feel threatened by (real or imaginary) external elements or pressure.[148] However, it is unclear whether these assertions have been made based on legal, historical or political grounds.[149]

Democratic People's Republic of Korea. Available from: http://www.mfa.gov.kp/view/article/15966 [Accessed 7 November 2022].

[145] *Foreign Ministry Spokesperson Zhao Lijian's Regular Press Conference on June 2, 2022* (2022). [online] Beijing: Ministry of Foreign Affairs of the People's Republic of China. Available from: https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2511_665403/202206/t20220602_10698118.html [Accessed 7 November 2022]. See also Sydney Morning Herald (27 May 2021) *Chinese foreign minister tells Germans 'you know what genocide looks like'*. [online] Sydney: Sydney Morning Herald. Available from: https://www.smh.com.au/world/europe/chinese-foreign-minister-tells-germans-you-know-what-genocide-looks-like-20210526-p57vdy.html [Accessed 7 November 2022] [per the Chinese Foreign Minister Wang Yi 'When those EU sanctions were launched, the Chinese people were reminded of the days when we were bullied by European imperialists. We have our national dignity to uphold']

[146] Al Jazeera. (16 October 2022) *Xi vows to strengthen China's military as Party Congress begins*. [online] Doha: Al Jazeera. Available from: https://www.aljazeera.com/news/2022/10/16/xi-touts-zero-covid-policy-as-communist-party-congress-begins [Accessed 7 November 2022].

[147] Sydney Morning Herald. (20 July 2021) *'Illicit gain': Australia accuses China of criminal cyber attacks*, [online] Sydney: Sydney Morning Herald. Available from: https://www.smh.com.au/politics/federal/illicit-gain-australia-accuses-china-of-criminal-cyber-attacks-20210720-p58b6s.html [Accessed 7 November 2022].

[148] Fitzgerald, J. (2006) The Dignity of Nation. In: Chien, S. Y. S. and Fitzgerald, J. (eds.) *The dignity of nations: equality, competition, and honor in East Asian nationalism*. Hong Kong: Hong Kong University Press, pp. 3-4. State dignity is cited as an expression of nationalism particularly in the East Asian context: Ibid, p. 6; and Sung-Won Yoon (2008) Sovereign Dignity, Nationalism and the Health of a Nation: A Study of China's Response in Combat of Epidemic. *Studies in Ethnicity and Nationalism* 8 (1), p. 85.

[149] China's insistence on sovereign dignity may be attributed to its historical experience of what the Chinese government terms the 'century of humiliation': see generally, Chan, P. (2014)

There is a clear and important pattern in this, and it is a pattern that provides an additional impetus for the idea of anchoring sovereignty in the concept of State dignity. The pattern suggests that, authoritarian States, in particular, are seeking to 'hijack' the concept of State dignity so as to use it as a shield against criticism by the international community. But just like an individual criminal should not have the avenue to argue that being prosecuted is against her human dignity, States should not have the option to use State dignity as such a shield against their obligations under international law, including under human rights law.

Thus, by adopting and giving meaning to the concept of State dignity in the manner advocated here, we may not only help develop sovereignty, but we can also prevent the attempt by authoritarian States to hide behind a twisted interpretation of the concept of State dignity in a manner undermining the international system.

From the perspective of international law, injury to dignity may arguably be approached in the light of the law governing reparations for damage arising from internationally wrongful acts.[150] Damage may be material (pecuniary) or moral,[151] and *Lusitania* held "there can be no doubt" that there is an entitlement to compensation "for an injury inflicted resulting in mental suffering, injury to his feelings, humiliation, shame, degradation, loss of social position or injury to his credit or to his reputation".[152] That seminal case specifically referenced the afflictions suffered by individuals

China's Approaches to International Law since the Opium War. *Leiden Journal of International Law*, 27 (4), p. 859; and Sung-Won Yoon (2008) Sovereign Dignity, Nationalism and the Health of a Nation: A Study of China's Response in Combat of Epidemic. *Studies in Ethnicity and Nationalism* 8 (1), 93. Similarly, such escape from humiliation and attainment of dignity can be traced to the modern histories of Korea, Taiwan and Japan: see Fitzgerald, J. (2006) The Dignity of Nation. In: Chien, S. Y. S. and Fitzgerald, J. (eds.) *The dignity of nations: equality, competition, and honor in East Asian nationalism*. Hong Kong: Hong Kong University Press, p. 13.

[150] *Factory at Chorzów*, [1928], PCIJ, Ser A, No 17, p. 29. See also *Reparation for Injuries Suffered in the Service of the United Nations (Advisory Opinion)*, [1949] ICJ Rep 174, p. 184. See also UNGA, *Responsibility of States for Internationally Wrongful Acts*, 53 UN GAOR Supp, UN Doc A/56/83 (2002), Annex, art 31(1). Reparations should 'as far as possible, wipe out the illegal act and re-establish the situation which would, in all probability, have existed' had the internationally wrongful act not been committed: Factory at Factory at Chorzów, [1928], PCIJ, Ser A, No 17, p. 47; and Pirim, C. Z. (2020) Reparation by Pecuniary Means of Direct Moral Damages Suffered by States as a Result of Internationally Wrongful Acts. Journal of International Dispute Settlement 11, pp. 258-259.

[151] *Opinion in the Lusitania Cases (United States v Germany)* (1956) VII RIAA 32, p. 34 et seq. Sometimes, it is referred to as 'political damage': see ILC, *Second report on State responsibility, by Mr. Gaetano Arangio-Ruiz, Special Rapporteur*, UN Doc A/CN.4/425 & Corr.1 and Add.1 & Corr.1 (1989), p. 5, paragraph 13.

[152] *Opinion in the Lusitania Cases (United States v Germany)* (1956) VII RIAA 32, p. 40. See also UNGA, *Responsibility of States for Internationally Wrongful Acts*, 53 UN GAOR Supp, UN Doc A/56/83 (2002), Annex, art 36(2); and also Pirim, C. Z. (2020) Reparation by Pecuniary Means

who have feelings and emotions, and who enjoy certain social standing or reputation. As States are "deprived of any feelings", the notion that a State can suffer pain, humiliation, or injury to reputation may no doubt be termed "problematic".[153]

Even so, the matter of moral injury to the State was discussed at length by Special Rapporteur on the draft articles on State responsibility Gaetano Arangio-Ruiz.[154] A distinction was made between moral damage to natural or legal persons of a State, and "non-material damage which the offended State sustains more directly as an effect of an internationally wrongful act".[155] The latter has been termed "direct moral damage",[156] and consists of "infringement of the State's right per se" and "injury to the State's dignity, honour or prestige", which are considered an integral part of the State's personality.[157] These two elements of moral damage should be considered one and the same, for the "mere infringement of the injured State's right [...] is felt by that State as an offence to its dignity, honour or prestige".[158]

Indeed, there has been a long line of cases whereby legal persons are said to suffer moral damage.[159] As both States and entities such as corporations "are both abstract legal entities which cannot feel pain",[160] the idea that non-pecuniary damage cannot be awarded to legal persons which do not

---

of Direct Moral Damages Suffered by States as a Result of Internationally Wrongful Acts. *Journal of International Dispute Settlement* 11, p. 245.

[153] Pirim, C. Z. (2020) Reparation by Pecuniary Means of Direct Moral Damages Suffered by States as a Result of Internationally Wrongful Acts. *Journal of International Dispute Settlement* 11, pp. 242-243. See also Annacker, C. (1994) Part Two of the International Law Commission's Draft Articles on State Responsibility. *German Yearbook of International Law*, 37, p. 227.

[154] ILC, *Second report on State responsibility, by Mr. Gaetano Arangio-Ruiz, Special Rapporteur*, UN Doc A/CN.4/425 & Corr.1 and Add.1 & Corr.1 (1989).

[155] *Ibid*, p. 5, paragraph 13. Pirim, C. Z. (2020) Reparation by Pecuniary Means of Direct Moral Damages Suffered by States as a Result of Internationally Wrongful Acts. *Journal of International Dispute Settlement* 11, p. 248.

[156] Pirim, C. Z. (2020) Reparation by Pecuniary Means of Direct Moral Damages Suffered by States as a Result of Internationally Wrongful Acts. *Journal of International Dispute Settlement* 11, p. 246.

[157] ILC, *Second report on State responsibility, by Mr. Gaetano Arangio-Ruiz, Special Rapporteur*, UN Doc A/CN.4/425 & Corr.1 and Add.1 & Corr.1 (1989), p. 6, paragraph 14. Claudia Annacker, however, distinguishes between moral damage and legal damage: see Annacker, C. (1994) Part Two of the International Law Commission's Draft Articles on State Responsibility. *German Yearbook of International Law*, 37, p. 231.

[158] ILC, Second report on State responsibility, by Mr. Gaetano Arangio-Ruiz, Special Rapporteur, UN Doc A/CN.4/425 & Corr.1 and Add.1 & Corr.1 (1989), p. 6, paragraph 14.

[159] See e.g. *Comingersoll S.A. v. Portugal* [2000], App no 35382/97, ECHR 2000-IV, paragraph 35; and *Dispute Concerning Responsibility for the Deaths of Letelier and Moffitt (United States v Chile)* (1992) 25 RIAA 1, p. 16; and *Case Concerning Ahmadou Sadio Diallo (Republic of Guinea v Democratic Republic of the Congo)* [2010 ICJ Rep 639, paragraph 18.

[160] Pirim, C. Z. (2020) Reparation by Pecuniary Means of Direct Moral Damages Suffered by States as a Result of Internationally Wrongful Acts. *Journal of International Dispute Settlement* 11, p. 254.

have any feelings must be refuted.[161] It has also been said that the purposes of reparations for moral damage is aimed at "covering the losses suffered in moral values because of the offences committed to their reputation and at sending a message to the international community that States' dignity, honour and prestige should be respected".[162]

In *Rainbow Warrior*, it was held that the infringement of "non-material interests, such as acts affecting the honor, dignity or prestige of a State" entitle the affected State to receive "adequate reparation".[163] Though the unilateral removal of French agents responsible for blowing up a ship in the harbour of Auckland from the island of Hao caused no material damage to New Zealand, the Tribunal held that the damage to New Zealand is "of a moral, political and legal nature, resulting from the affront to the dignity and prestige" of New Zealand itself and the injured State's judicial and executive authorities.[164] Further, in *LaGrand*, Germany claimed that it "suffered moral and political damage by the fact alone that its rights and the rights of its nationals were violated by the United States"[165] when German nationals were executed despite an order by the ICJ not to do so pending final judgement in the case.[166] It may also be noted that in *M/V 'Saiga' (No 2)*, compensation was granted for "violation of [a State's] rights in respect of ships flying its flag".[167]

Satisfaction (discussed further below) is a form of reparation reserved for injuries arising from moral or legal damage that are not financially assessable.[168] There is ample jurisprudence whereby courts and tribunals

---

[161] *Ibid*, p. 254. Note however, it 'is undeniable that measuring direct moral damages suffered by States is difficult, subjective and variable': Ibid, p. 259.

[162] Ibid, p. 261. It may be no surprise that in *Lusitania*, the umpire noted:

> as between sovereign nations the question of the right and power to impose penalties, unlimited in amount, is political rather than legal in its nature.

ILC, *Second report on State responsibility, by Mr. Gaetano Arangio-Ruiz, Special Rapporteur*, UN Doc A/CN.4/425 & Corr.1 and Add.1 & Corr.1 (1989), p. 34, paragraph 114. See also Annacker, C. (1994) Part Two of the International Law Commission's Draft Articles on State Responsibility. *German Yearbook of International Law*, 37, p. 231.

[163] *Case concerning the difference between New Zealand and France concerning the interpretation or application of two agreements, concluded on 9 July 1986 between the two States and which related to the problems arising from the Rainbow Warrior Affair*, (1990) XX RIAA 215, paragraph 109 (citing Soerensen).

[164] *Ibid*, paragraph 110.

[165] *LaGrand (Germany v. United States of America)*, Memorial of the Federal Republic of Germany of 16 September 1999, paragraph 6.53. This issue was not addressed, but the ICJ did reference this *LaGrand (Germany v. United States of America)* [2001] ICJ Rep 466, paragraph 125.

[166] *LaGrand (Germany v. United States of America) (Provisional Order)* [1999] ICJ Rep 9.

[167] *M/V 'Saiga' (No 2) Case (Saint Vincent and the Grenadines v Guinea)* [1999] ITLOS Rep 10, paragraphs 176-177.

[168] *Case concerning the difference between New Zealand and France concerning the interpretation or*

have awarded satisfaction[169] to "as far as possible, wipe out the illegal act and re-establish the situation which would, in all probability, have existed" had the internationally wrongful act not been committed.[170] Often an acknowledgement of the wrongful act and an apology for the conduct of their national, or for its own conduct[171] or a judicial or arbitral finding of the failure of a State to fulfil its obligations[172] is sufficient satisfaction. Such case law may be said to demonstrate that "the existence of moral damages in international law has been taken for granted and not challenged".[173]

In addition, it should be noted that – at least under our conception of the concept – State dignity also imposes obligations on a State arguing that its sovereignty has been violated. This is because in the assessment of whether State dignity was infringed upon, we must also take account of how that State has acted. The significant implications of this were already illustrated above via the imaginary example of State C seeking to rely on sovereignty to supress information about its human rights abuses.

Finally, it may be possible to make the argument that, given that we are now all living in a world organised into different States, the human

application of two agreements, concluded on 9 July 1986 between the two States and which related to the problems arising from the Rainbow Warrior Affair, (1990) XX RIAA 215, paragraph 122.

[169] See UNGA, *Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries*, UN Doc A/CN.4/SER.A/2001/Add.1 (2001), p. 106. See particularly, e.g., *Mixed Claims Commission Netherlands-Venezuela* (1903) X RIAA 703, p. 730 (expression of regret); I*saac M. Bowers (United States) v. Great Britain (Fijian Land Claims)* (1923) VI RIAA 109, p. 112 (payment of nominal sum of one shilling); and *Affaire relative à la concession des phares de l'Empire ottoman (Grèce c France)* [1956] XII RIAA 155, p. 216.

[170] *Factory at Chorzów*, [1928], PCIJ, Ser A, No 17, p. 47.

[171] Claim of the British Ship "I'm Alone" v. United States (1935). *American Journal of International Law*, 29 (2), p. 326. See also ILC, *Second report on State responsibility, by Mr. Gaetano Arangio-Ruiz, Special Rapporteur*, UN Doc A/CN.4/425 & Corr.1 and Add.1 & Corr.1 (1989), p. 36 et seq outlining various diplomatic practice before and after the Second World War. Examples of forms of satisfaction include:

> apologies, with the implicit admission of responsibility and the disapproval of and regret for what has occurred; punishment of the responsible individuals; a statement of the unlawfulness of the act by an inter national body, either political or judicial; assurances or safeguards against repetition of the wrongful act; payment of a sum of money not in proportion to the size of the material loss.

Ibid, p. 41, paragraph 139. See also *Dispute Concerning Responsibility for the Deaths of Letelier and Moffitt (United States v Chile)* (1992) 25 RIAA 1, p. 16.

[172] *Corfu Channel (United Kingdom v Albania)* [1949] ICJ Rep 4, p. 36; *Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)* [2007] ICJ Rep 43, paragraphs 463; 465; and *Case Concerning Ahmadou Sadio Diallo (Republic of Guinea v Democratic Republic of the Congo)* [2010] ICJ Rep 639, paragraph 161.

[173] Markert, L. and Freiburg, E. (2013) Moral Damages in International Investment Disputes - On the Search for a Legal Basis and Guiding Principles. Journal of World Investment & Trade, 14 (1), p. 17.

dignity recognised in the Charter of the United Nations,[174] necessitates the recognition of State dignity; that is dignity on the individual level is only possible with dignity on the community level.

At any rate, the overview provided in this section (7.2.3) have covered a broad range of different sources relating to dignity and more specifically State dignity. Given its diversity, the conclusions that can be drawn are limited. However, it is hoped that – not least via analogies – this section has usefully brought attention to some sources that may be relied upon to develop further the idea of anchoring sovereignty in the concept of State dignity. Arguably it provides a precedent, and provides guidance, for the application of a conception of sovereignty anchored in State dignity.

8. WHAT ARE THE CONSEQUENCES OF VIOLATING SOVEREIGNTY?

As we have established, violations of sovereignty can occur through a number of means and, in turn, may result from violations of territorial integrity, the principle of non-interference/intervention, and principles relating to the prohibition on the use of force (other than in self-defence, collective self-defence, or on the authorisation of the United Nations Security Council). These violations can have both political and legal consequences. The political consequence may be many, varied, and complex, and, at this juncture, consider some of the potential legal consequences.

The starting point is that there are legal consequences when a State commits an internationally wrongful act.[175] Each internationally wrongful act entails the international responsibility of that State.[176] An international wrongful act can result from the act or omission of a State. For instance, engaging in an armed attack against another State would clearly be an act that violates the sovereignty of the victim State, and would entail the international responsibility of the attacking State. Meanwhile, the failure to prevent transboundary harm from injuring the interests of another State would also entail international responsibility.[177]

---

[174] Freeland S. and Ireland-Piper, D. (2021) Space Law, Human Rights and Corporate Accountability. *UCLA Journal of International Law and Foreign Affairs* 26(1), p. 6.

[175] Chirwa, D. M. (2004), The Doctrine of State Responsibility as a Potential Means of Holding Private Actors Accountable for Human Rights. *Melbourne Journal of International Law* 5 (1), citing Brownlie, 1983, p. 9.

[176] UNGA, *Responsibility of States for Internationally Wrongful Acts*, 53 UN GAOR Supp, UN Doc A/56/83 (2002), Annex, art 1; *Case concerning the difference between New Zealand and France concerning the interpretation or application of two agreements, concluded on 9 July 1986 between the two States and which related to the problems arising from the Rainbow Warrior Affair*, (1990) XX RIAA 215, paragraph 75; and *Phosphates in Morocco*, [1938], PCIJ, Series A/B, No. 74, p. 28.

[177] *Trail Smelter Case (United States v Canada)* (Decision of 11 March 1941), [1949] III RIAA 1905.

The *Articles on Responsibility of States for Internationally Wrongful Acts* (ARSIWA) are (generally speaking) the authoritative statement of the law of State responsibility.[178] By way of background, however, an earlier development in the law of State responsibility was the Treaty of Westphalia 1648, which embedded State-centric ideologies such as sovereignty, territorial integrity, and non-intervention in the modern international law landscape. After decades of work, the ARSIWA were finalised and adopted by the International Law Commission (ILC) in 2001.[179] In 2002, the Articles on Responsibility of States were adopted by the General Assembly, converting their status from draft articles to articles "commended to the attention of governments".[180]

Fundamentally, however, to incur State responsibility requires a State to be sovereign, and therefore, in control of its actions and the actions of those it directs or controls.[181] In this way, State responsibility is a consequence of sovereignty. From a legal perspective, there are two key elements required for State responsibility to arise at international law.[182] First, the conduct must be attributable to the State,[183] and attribution is – as noted above – notoriously difficult on the cyber arena. For example, a violation of sovereignty or a failure to prevent a violation of sovereignty by a government body, or a private entity,[184] in *theory* could be attributable to the State.

---

[178] Shaw, M. N. (2021) *International Law*. 9th ed. Cambridge: Cambridge University Press, p. 680; Koskenniemi, M. 2001, p. 341; Crawford, J. (2002) *The International Law Commission's articles on state responsibility : introduction, text, and commentaries*. Cambridge: Cambridge University Press, p. 889.

[179] Ireland-Piper, D., Fehlhaber, M., & Bonenfant, A. (2023). International State Responsibility and Commercial Space Activities. *Oxford Research Encyclopedia of Planetary Science*.

[180] See UNGA, *Responsibility of States for Internationally Wrongful Acts*, 53 UN GAOR Supp, UN Doc A/56/83 (2002), paragraph 3. The phrase "commended to the attention of governments" is expressed as a formal seal of approval by the UNGA but has no otherwise legally binding effect (like UNSC resolutions). Therefore, ARSIWA does not have the status of international treaty and while ARSIWA remain the key instrument on state responsibility, the articles leave certain areas of law underdeveloped. Further, the generality with which the articles are written leaves interpretation subject to the specific subject matter of law, or *lex specialis*, in question. This means the principles of State responsibility can be supplanted by references to specific areas of law, such as cyber law and space law, for example.

[181] Crawford, J. (2014) *State Responsibility: The General Part*. Cambridge: Cambridge University Press, p. 133.

[182] *Prosecutor v Tihomir Blaškić (Decision on the Objection of the Republic of Croatia to the Issuance of Subpoenae Duces Tecum)* IT-95-14-PT (18 July 1997), pargraph 96; *Dickson Car Wheel Company (United States of America v United Mexican States) (Award)* (1931) 4 RIAA 669, p. 678; and *United States Diplomatic and Consular Staff in Tehran*, [1980] ICJ Rep 3, paragraph 56.

[183] UNGA, *Responsibility of States for Internationally Wrongful Acts*, 53 UN GAOR Supp, UN Doc A/56/83 (2002), Annex, art 2(a). See also *Phosphates in Morocco*, [1938], PCIJ, Series A/B, No. 74, p. 28; and *United States Diplomatic and Consular Staff in Tehran*, [1980] ICJ Rep 3, paragraph 56.

[184] See e.g. *Asian Agricultural Products Ltd. v. Republic of Sri Lanka* [1990], ICSID Case No. ARB/87/3 [75].

Generally speaking, the conduct of *de jure* or *de facto* organs of the State are directly attributable to the State.[185] A *de jure* organ is one empowered to function as an executive, legislative or judicial limb of the State.[186] A *de facto* organ is a person or entity, which although not an organ of the State, is empowered to exercise elements of governmental authority, provided that the person or entity is acting in the capacity of that authority.[187] This can include both public corporations and private companies.[188]

For example, Article 5 of the ARSIWA provides that the conduct of a person (including a legal person, such as a body corporate) which is not a State but is empowered by the law of a State to exercise "elements of governmental authority" can, in some circumstances, trigger State responsibility. Notably, under Article 7, responsibility can still arise, even where that authority is technically exceeded. The overall test for responsibility, however, is generally understood to be "effective control." This is where a State directs the specific conduct and that conduct results in the alleged internationally wrongful act.[189] There has been debate as to whether to the test should more appropriately be "overall control", a lower threshold, where specific instructions are not necessary to establish State control over an entity.[190] However, in Bosnian Genocide, the ICJ appeared to affirm the effective control test.[191]

---

[185] *Difference Relating to Immunity from Legal Process of a Special Rapporteur of the Commission of Human Rights, Advisory Opinion* [1999] ICJ Rep 62, paragraph 62; and *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)*, [2007] ICJ Rep 43, paragraph 385.

[186] UNGA, *Responsibility of States for Internationally Wrongful Acts*, 53 UN GAOR Supp, UN Doc A/56/83 (2002), Annex, art 4; UNGA, *Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries*, UN Doc A/CN.4/SER.A/2001/Add.1 (2001), p. 31.

[187] UNGA, *Responsibility of States for Internationally Wrongful Acts*, 53 UN GAOR Supp, UN Doc A/56/83 (2002), Annex, art 5. UNGA, *Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries*, UN Doc A/CN.4/SER.A/2001/Add.1 (2001), p. 51.

[188] UNGA, *Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries*, UN Doc A/CN.4/SER.A/2001/Add.1 (2001), p. 51.

[189] *Case Concerning Military and Paramilitary Activities in and against Nicaragua* [1986] ICJ Rep 14, paragraph 115; *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Federal Republic of Yugoslavia) (Judgment)* [2007] ICJ Rep 43, paragraph 299–400; UNGA, *Responsibility of States for Internationally Wrongful Acts*, 53 UN GAOR Supp, UN Doc A/56/83 (2002), Annex, art 8.

[190] *In Prosecutor v Duško Tadić (Judgement)* IT-94-1-A (15 July 1997), paragraph 120, the ICTY broke with the ICJ's conceptualisation of control. It preferred the lower threshold of 'overall control', which did not require specific instructions from a State to establish control over the actions of a de facto organ. This test was purportedly developed to recognise the influence of hierarchy in quasi-military political organisations. See also the most recent MH17 judgement of the District Court of the Hague (17 November 2022). [online] The Hague: District Court of the Hague `https://www.courtmh17.com/en/news/2022/transcript-of-the-mh17-judgment-hearing.html` [Accessed 7 November 2022].

[191] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, [2007] ICJ Rep 43, paragraph 406; Ireland-Piper,

Second, the conduct in question must constitute a breach of an international legal obligation, applicable at the time the conduct occurred.[192] Those obligations may originate from treaties, customary international law, or general principles of law.[193] States must know "or ought to have known"[194] that the conduct in question constituted a breach. Notably, Article 3 of ARSIWA provides that the characterisation of an act as internationally wrongful is question of international law, not domestic law. This means that a State cannot escape responsibility for an act on the basis that the relevant conduct was lawful under its own domestic law.[195]

Once these two elements are established (in relation to a violation of sovereignty that constitutes an international wrong, for example), a State may be under an obligation to cease conduct or make reparations. Specifically, Article 30 of ARSIWA provides that a State responsible for an internationally wrongful act is under an obligation: "(a) to cease that act, if it is continuing; (b) to offer appropriate assurances and guarantees of non-repetition, if circumstances so require".[196] Under Article 31, the responsible State is under an obligation to make full reparation for the injury caused by the internationally wrongful act. Notably, injury includes "any damage, whether

D., Fehlhaber, M., & Bonenfant, A. (2023). International State Responsibility and Commercial Space Activities. *Oxford Research Encyclopedia of Planetary Science*.

[192] UNGA, *Responsibility of States for Internationally Wrongful Acts*, 53 UN GAOR Supp, UN Doc A/56/83 (2002), Annex, art 2(b). See *Phosphates in Morocco*, [1938], PCIJ, Series A/B, No. 74, p. 28; and *United States Diplomatic and Consular Staff in Tehran*, [1980] ICJ Rep 3, paragraph 56.

[193] UNGA, *Responsibility of States for Internationally Wrongful Acts*, 53 UN GAOR Supp, UN Doc A/56/83 (2002), Annex, art 12. *Case concerning the difference between New Zealand and France concerning the interpretation or application of two agreements, concluded on 9 July 1986 between the two States and which related to the problems arising from the Rainbow Warrior Affair*, (1990) XX RIAA 215, paragraph 75; and *Case concerning the Gabčíkovo-Nagymaros Project (Hungary v. Slovakia)* [1997] ICJ Rep 7, paragraph 47. For the sources of international law, see *Corfu Channel (United Kingdom v Albania) [1949] ICJ Rep 4, pp. 22–23.*, 24 October 1945, 33 UNTS 993 (entered into force 18 April 1946), art 38(1).

[194] *Corfu Channel (United Kingdom v Albania)* [1949] ICJ Rep 4, pp. 22–23.

[195] Crawford, J. (2002) *The ILC's Articles on State Responsibility: Introduction, Text and Commentary*. Cambridge: Cambridge University Press, p. 100; and Ireland-Piper, D., Fehlhaber, M., & Bonenfant, A. (2023). International State Responsibility and Commercial Space Activities. *Oxford Research Encyclopedia of Planetary Science*. See also *Reparation for Injuries suffered in the Service of the United Nations, Advisory Opinion*, [1949] ICJ Rep 174, p. 180; and *Compañía de Aguas del Aconquija SA and Vivendi Universal v Argentine Republic* (ICSID Case No. ARB/97/3), Decision on Annulment of 3 July 2002, paragraphs 101–103. See also *Vienna Convention on the Law of Treaties*, 1155 UNTS 331 (entered into force 27 January 1980), art 27.

[196] UNGA, *Responsibility of States for Internationally Wrongful Acts*, 53 UN GAOR Supp, UN Doc A/56/83 (2002), Annex, art 30. See also *Case concerning the difference between New Zealand and France concerning the interpretation or application of two agreements, concluded on 9 July 1986 between the two States and which related to the problems arising from the Rainbow Warrior Affair*, (1990) XX RIAA 215, paragraph 113-114.

material or moral, caused by the internationally wrongful act of a State".[197] Reparations can take the form of restitution,[198] compensation,[199] and/or satisfaction.[200]

Responsibility for an international wrong may also entitle the wronged State to take lawful countermeasures. However, the injured State may only direct its countermeasures against the responsible State and only to induce it to comply with its obligations to make reparations.[201] Countermeasures must be a non-forcible response to a breach of an international obligation,[202] which need to be proportionate to the initial wrongful act,[203] and do not mitigate all other obligations, including, for example, obligations relating to peremptory norms, the non-use of force, and human rights.[204]

Notably, however, the notion of "State responsibility" is distinct from "international liability". As Ireland-Piper, Fehlhaber, and Bonenfant have observed:

> It is easy to confuse the two. The term international responsibility refers to the liability of States to pay compensation for damage, without necessarily having committed an internationally wrongful act. State responsibility, on the other hand, refers to the attribution of responsibility to a State for an internationally wrongful act. To put it another way:

[197] UNGA, *Responsibility of States for Internationally Wrongful Acts*, 53 UN GAOR Supp, UN Doc A/56/83 (2002), Annex, Art 31(2).

[198] *Ibid*, art 35. See also *M/V 'Saiga' (No 2) Case (Saint Vincent and the Grenadines v Guinea)* [1999] ITLOS Rep 10, paragraph 171; and ICSID, *CMS Gas Transmission Company v. Argentine Republic*, Case No ARB/01/8 (2005), paragraph 399.

[199] UNGA, *Responsibility of States for Internationally Wrongful Acts*, 53 UN GAOR Supp, UN Doc A/56/83 (2002), Annex, art 36.

[200] *Ibid*, art 37.

[201] *Ibid*, art 49. See also *Case concerning the Gabčíkovo-Nagymaros Project (Hungary v. Slovakia)* [1997] ICJ Rep 7, paragraph 83.

[202] UNGA, *Responsibility of States for Internationally Wrongful Acts*, 53 UN GAOR Supp, UN Doc A/56/83 (2002), Annex, art 50(1); and UNGA, *Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations*, UN Doc A/RES/2625(XXV) (1970). See also *Case Concerning Military and Paramilitary Activities in and against Nicaragua* [1986] ICJ Rep 14, paragraph 202; and *Guyana v Suriname Maritime Boundary Arbitration (Guyana v Suriname)*, [2004] PCA No 2004-04, paragraph 446.

[203] UNGA, *Responsibility of States for Internationally Wrongful Acts*, 53 UN GAOR Supp, UN Doc A/56/83 (2002), Annex, art 51. See also *Case concerning the Gabčíkovo-Nagymaros Project (Hungary v. Slovakia)* [1997] ICJ Rep 7, paragraph 85; and *Case Concerning United States Diplomatic and Consular Staff in Tehran (Iran v. United States of America)* [1980] ICJ Rep 3, paragraph 86. Any countermeasure that is disproportionate to the internationally wrongful act is "considered excessive and therefore unlawful": *Naulilaa Case (Germany v Portugal)*, (1928) II RIAA 1011, p. 1028.

[204] UNGA, *Responsibility of States for Internationally Wrongful Acts*, 53 UN GAOR Supp, UN Doc A/56/83 (2002), Annex, art 50.

> "State responsibility" refers to a State's responsibility under international law in general, whereas "international liability" denotes a State's 'civil responsibility', or obligation to pay compensation or make reparations for injuries that non-nationals suffer outside its national boundaries as a result of activities within its territory or under its control.[205]

One legal consequence of violating sovereignty, for instance through a violation of a primary obligation such as the principles of non-interference, non-use of force, and those regulating the conduct of armed hostilities, is that a State can incur legal obligations. This includes legal obligations to cease certain conduct, make reparations, or it entitle another State to take lawful countermeasures. The obligation to make reparations (see above) or the right of an injured State to take countermeasures is recognised under the principles of State responsibility.

9. CONCLUDING REMARKS

As correctly noted by Osula et al, sovereignty is one of the most politically loaded terms in the discussions of state behaviour in cyberspace.[206] The concept of sovereignty is constantly in the news. At the time of writing, violations of sovereignty such as both threatened and actual invasion and use of force, including allegations of war crimes, are taking place. This tells us quite a lot about the central role that the concept plays – it is literally used as a compass to point to right and wrong in conflicts that may literally ruin the world. Unfortunately, it is questionable whether it – in its current form – is up to the task.

This article has aimed to help address some of the challenges we face by outlining the key features of sovereignty in a brief, and hopefully accessible manner. We have also sought to provide some ideas for possible law reform.

Time will tell whether we have succeeded in relation to either of these goals. But the worry is that we do not know just how much time we have. It seems to us that given its centrality in international law and international relations, we must make urgent progress with how we understand sovereignty.

---

[205] Ireland-Piper, D., Fehlhaber, M., & Bonenfant, A. (2023). International State Responsibility and Commercial Space Activities. *Oxford Research Encyclopedia of Planetary Science* (citations omitted). See also ILC, *Third report on international liability for injurious consequences arising out of acts not prohibited by international law (prevention of transboundary damage from hazardous activities)*, by Mr. Pemmaraju Sreenivasa Rao, Special Rapporteur, UN Doc Document A/CN.4/510 (2000), paragraph 27.

[206] Osula, A.-M., Kasper, A. and Kajander, A. (2022) EU Common Position on International Law and Cyberspace. *Masaryk University Journal of Law and Technology*, 16 (1), p. 95.

LIST OF REFERENCES

[1] *Barcelona Traction, Light and power Company* [1970] ICJ Rep 3, paragraphs 78-79.

[2] Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo, Advisory Opinion [2010] ICJ Rep 403.

[3] *Affaire relative à la concession des phares de l'Empire ottoman (Grèce c France)* [1956] XII RIAA 155.

[4] *Agreement among the Government of Canada, Governments of the Member States of the European Space Agency (ESA), the Government of Japan, the Government of the Russian Federation and the Government of the United States of America Concerning Cooperation on the Civil International Space Station*, 29 January 1998, 80 Stat 271, 1 USC 113 (entered into force 27 March 2001).

[5] *Agreement governing the Activities of States on the Moon and Other Celestial Bodies*, signed on 5 December 1979, 1363 UNTS 3 (entered into force 11 July 1984).

[6] Al Arabia. (2 December 2015) *Turkey won't retaliate against Russia's sanctions*. [online] Dubai: Al Arabia. Available from: `https://english.alarabiya.net/News/middle-east/2015/12/02/Erdogan-vows-no-retaliation-against-Russian-sanctions` [Accessed 7 November 2022].

[7] Al Jazeera. (16 October 2022) *Xi vows to strengthen China's military as Party Congress begins*. [online] Doha: Al Jazeera. Available from: `https://www.aljazeera.com/news/2022/10/16/xi-touts-zero-covid-policy-as-communist-party-congress-begins` [Accessed 7 November 2022].

[8] *Al-Skeini and Others v United Kingdom*, 55721/07 [2011] 1093.

[9] Annacker, C. (1994) Part Two of the International Law Commission's Draft Articles on State Responsibility. *German Yearbook of International Law*, 37.

[10] Annan, K. (2005) "In Larger Freedom": Decision Time at the UN. *Foreign Affairs* (May/June 2005).

[11] *Antarctic Treaty*, signed on 1 December 1959, 402 UNTS 7 (entered into force 23 June 1961).

[12] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)*, [2007] ICJ Rep 43.

[13] *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda)* [2005] ICJ Rep 168.

[14] Asian Agricultural Products Ltd. v. Republic of Sri Lanka

[15] Barlow, J. A. (1996) *Declaration of the Independence of Cyberspace*. [online] Electronic Frontier Foundation: San Francisco. Available from: `https://www.eff.org/cyberspace-independence` [Accessed 7 November 2022].

[16] *Basic Position of the Government of Japan on International Law Applicable to Cyber Operations* (28 May 2021). [online] Ministry of Foreign Affairs of Japan: Tokyo, p. 3. Available from: `https://www.mofa.go.jp/files/100200935.pdf` [Accessed 7 November 2022].

[17] Besson, S. (April 2011) Sovereignty. In: *Max Planck Encyclopedias of International Law*.

[18] Buchan, R. (2018) *Cyber Espionage and International Law*. Oxford: Hart.

[19] C. Ryngaert, C. and Zoetekouw, M. 'The End of territory? The e-emergence of community as a principle of jurisdictional order in the Internet era', in Kohl, U. (ed.) (2017) *The Net and the Nation State: Multidisciplinary Perspectives on Internet Governance*, Cambridge: Cambridge University Press.

[20] Canada: Claim Against the Union of Soviet Socialist Republics for Damage Caused by Soviet Cosmos 954 (1979), Annex A: Statement of Claim. International Legal Materials, 18 (4), p. 899, paragraph 21;

[21] Cançado Trindade, A. A. (2013) *International law for humankind: towards a new jus gentium*. 2nd ed. Leiden: Brill.

[22] *Case Concerning Ahmadou Sadio Diallo (Republic of Guinea v Democratic Republic of the Congo)* [2010 ICJ Rep 639.

[23] *Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)* [2007] ICJ Rep 43.

[24] *Case Concerning Application of the International Convention on the Elimination of All Forms of Racial Discrimination (Georgia v Russian Federation) (Request for the Indication of Provisional Measures)* [2008] ICJ Rep 353, paragraph 109. Note also *Bankovic v. Belgium*, 52207/99 [2001] ECHR 2001-XII.

[25] *Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda)*, [2005] ICJ Rep 168.

[26] *Case Concerning Military and Paramilitary Activities in and against Nicaragua* [1986] ICJ Rep 14.

[27] *Case concerning the difference between New Zealand and France concerning the interpretation or application of two agreements, concluded on 9 July 1986 between the two States and which related to the problems arising from the Rainbow Warrior Affair*, (1990) XX RIAA 215.

[28] *Case concerning the Gabčíkovo-Nagymaros Project (Hungary v. Slovakia)* [1997] ICJ Rep 7.

[29] *Case Concerning United States Diplomatic and Consular Staff in Tehran (Iran v. United States of America)* [1980] ICJ Rep 3.

[30] Chan, P. (2014) China's Approaches to International Law since the Opium War. *Leiden Journal of International Law*, 27 (4).

[31] *Charter of the United Nations*, 24 October 1945, 1 UNTS XVI.

[32] Cheng, B. (1965) The Extra-Territorial Application of International Law. *Current Legal Problems*, 18 (1).

[33] China, *China's Views on the Application of the Principle of Sovereignty in Cyberspace* (2022), submitted to the Open-ended Working Group on security of and in the use of information and communications technologies.

[34] Chirwa, D. M. (2004), The Doctrine of State Responsibility as a Potential Means of Holding Private Actors Accountable for Human Rights. *Melbourne Journal of International Law* 5 (1), citing Brownlie, 1983.

[35] Claim of the British Ship "I'm Alone" v. United States (1935). *American Journal of International Law*, 29 (2).

[36] Coco, A. and de Souza Dias, T. (2021) "Cyber Due Diligence": A Patchwork of Protective Obligations in International Law. *European Journal of International Law* 32 (3).

[37] *Comingersoll S.A. v. Portugal* [2000], App no 35382/97, ECHR 2000-IV.

[38] *Comments by Austria, Pre-Draft Report of the OEWG – ICT* (31 March 2020). [online] New York: United Nations Disarmament Office. Available from: `https://front.un-arm.org/wp-content/uploads/2020/04/comments-by-austria.pdf` [Accessed 7 November 2022].

[39] *Compañía de Aguas del Aconquija SA and Vivendi Universal v Argentine Republic* (ICSID Case No. ARB/97/3), Decision on Annulment of 3 July 2002.

[40] Continental Shelf (Libyan Arab Jamahiriya v. Malta) [1985] ICJ Rep 13.

[41] *Convention on Certain Questions relating to the Conflict of Nationality Laws*, 12 April 1930, 179 LNTS 89 (entered into force 1 July 1937).

[42] *Convention on International Civil Aviation, 7 December 1944, 15 UNTS 295, ICAO 7300/9 (entered into force 4 April 1947).*

[43] Convention on the Rights and Duties of States, signed 26 December 1933, 165 LNTS 19 (entered into force 26 December 1934).

[44] Cooper, D. and C. Kuner, C. 'Data Protection Law and International Dispute Resolution', 382 Recueil des Cours of the Hague Academy of International Law (2017).

[45] Corfu Channel (United Kingdom v Albania) [1949] ICJ Rep 4, p. 22.

[46] Country-Specific "Special Rapporteur" Mechanism Must Be Abolished Immediately (17 October 2022). [online] Pyongyang: Ministry of Foreign Affairs of the Democratic People's Republic of Korea. Available from: `http://www.mfa.gov.kp/view/article/15966` [Accessed 7 November 2022].

[47] Crawford, J. (2002) *The ILC's Articles on State Responsibility: Introduction, Text and Commentary*. Cambridge: Cambridge University Press.

[48] Crawford, J. (2006) *The Creation of States in International Law*. 2nd ed. Oxford: Oxford University Press.

[49] Crawford, J. (2014) *State Responsibility: The General Part*. Cambridge: Cambridge University Press.

[50] *Customs Regime between Germany and Austria (Protocol of March 19th, 1931), Advisory Opinion*, PCIJ (ser A/B) No 41, p. 57 (per Judge Anzilotti).

[51] *Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace* (July 2020) [online] Tehran: Nour News. Available from: https://nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat [Accessed 7 November 2022].

[52] Delerue, F. (2020) *Cyber Operations and International Law*. Cambridge: Cambridge University Press.

[53] *Dickson Car Wheel Company (United States of America v United Mexican States) (Award)* (1931) 4 RIAA 669.

[54] *Difference Relating to Immunity from Legal Process of a Special Rapporteur of the Commission on Human Rights, Advisory Opinion* [1999] ICJ Rep 62.

[55] Directorate of International Law, Federal Department of Foreign Affairs, Switzerland's Position Paper on the Application of International Law in Cyberspace, UN GGE 2019/2021 (2021).[online] Switzerland Federal Department of Foreign Affairs: Bern. Available from: https://www.eda.admin.ch/dam/eda/en/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_EN.pdf [Accessed 7 November 2022].

[56] *Dispute Concerning Responsibility for the Deaths of Letelier and Moffitt (United States v Chile)* (1992) 25 RIAA 1.

[57] Draft Declaration on Rights and Duties of States with Commentaries' [1949] *Yearbook of the International Law Commission* 287.

[58] *Draft Declaration on Rights and Duties of States*, UNGAOR 4th Sess, UN Doc A/RES/375 (1949).

[59] *East Timor (Portugal v. Australia)* [1995] ICJ Rep 90.

[60] Factory at Chorzów, [1928], PCIJ, Ser A, No 17.

[61] Fitzgerald, J. (2006) The Dignity of Nation. In: Chien, S. Y. S. and Fitzgerald, J. (eds.) *The dignity of nations: equality, competition, and honor in East Asian nationalism*. Hong Kong: Hong Kong University Press.

[62] *Foreign Ministry Spokesperson Zhao Lijian's Regular Press Conference on June 2, 2022* (2022). [online] Beijing: Ministry of Foreign Affairs of the People's Republic of China. Available from: https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2511_665403/202206/t20220602_10698118.html [Accessed 7 November 2022].

[63] Francisco Lobo, J. (2018) One Piece at a Time: The 'Accumulation of Events' Doctrine and the 'Bloody Nose' Debate on North Korea. [online] Lawfare Blog. Available from: https://www.lawfareblog.com/one-piece-time-accumulation-events-doctrine-and-bloody-nose-debate-north-korea [Accessed 20 April 2023].

[64] Freeland S. and Ireland-Piper, D. (2021) Space Law, Human Rights and Corporate Accountability. *UCLA Journal of International Law and Foreign Affairs*, 26(1).

[65] Ginsburg, T. (2017) Introduction to Symposium on Sovereignty, Cyberspace, and Tallinn Manual 2.0. *American Journal of International Law Unbound*, 11.

[66] Haass, R. N. (2003) *Sovereignty: Existing Rights, Evolving Responsibilitie*s. [online] Washington D.C: US Department of State. Available from: https://2001-2009.state.gov/s/p/rem/2003/16648.htm [Accessed 7 November 2022].

[67] Handl, G. et al. (eds.) (2012) *Beyond Territoriality*, The Hague: Martinus Nijhoff; Mills, A. 'Rethinking Jurisdiction in International Law', 84(1) *British Yearbook of International Law* (2014).

[68] Heller, K. J. (2021) In Defense of Pure Sovereignty in Cyberspace. *International Law Studies*, 97.

[69] Henkin, L. (1994) The Mythology of Sovereignty. In: RStJ Macdonald (ed.) *Essays in Honour of Wang Tieya*. Martinus Nijhoff: Dordrecht.

[70] Higgins, R. (2000) *Problems and Process: International Law and How We Use It*. Oxford: Clarendon.

[71] Hummel P., et al. (2021), Data sovereignty: A review. *Big Data & Society*, p. 12

[72] ICSID, *CMS Gas Transmission Company v. Argentine Republic*, Case No ARB/01/8 (2005), paragraph 399.

[73] ILC, *Second report on State responsibility, by Mr. Gaetano Arangio-Ruiz, Special Rapporteur*, UN Doc A/CN.4/425 & Corr.1 and Add.1 & Corr.1 (1989),

[74] *International Air Services Transit Agreement*, 7 December 1944, 84 UNTS 387 (entered into force 30 January 1945), art 1, Section 1(1).

[75] *International law applicable in cyberspace* (4 April 2022). [online] Ottawa: Global Affairs Canada, paragraph 15. Available from: https://www.international.gc.ca/world-monde/issues_development-

enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng [Accessed 7 November 2022].

[76] *International Law Applied to Operations in Cyberspace: Paper shared by France with the Open-ended working group established by resolution 75/240* (December 2021), p.2. [online] New York: United Nations Office of Disarmament Affairs. Available from: https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf [Accessed 7 November 2022].

[77] International Law Association (2018) I, Sydney Conference. [online] London: International Law Association. Available from: https://www.ila-hq.org/en_GB/documents/conference-report-sydney-2018-6 [Accessed 7 November 2022].

[78] International Law Commission, *Draft Articles on Diplomatic Protection*, UN Doc A/CN.4/L.684 and Corr.1-2, UN Doc A/61/10.

[79] *Isaac M. Bowers (United States) v. Great Britain (Fijian Land Claims)* (1923) VI RIAA 109.

[80] *Island of Palmas Case (the Netherlands v. United States of America)* (1928) 2 RIAA 829.

[81] Jackson, J. H. (2003) Sovereignty-Modern: A New Approach to an Outdated Concept. *American Journal of International Law*, 97 (4) 782.

[82] Jackson, J. H. (2003) Sovereignty-Modern: A New Approach to an Outdated Concept. American Journal of International Law, 97 (4).

[83] Jakhu, R. S. and Freeland, S. (2016) The Relationship between the Outer Space Treaty and Customary International Law. *Proceedings of the International Institute of Space Law*, 59.

[84] Kazakhstan, *Outer Space Activities Act (2012)*.

[85] Keyes, M. (2005) *Jurisdiction in International Litigation*, Sydney: The Federation Press.

[86] Khan, D.E. (2012) Territory and Boundaries. In: Fassbender, B. and Peters, A. (eds.) *The Oxford Handbook of The History of International Law*. Oxford: Oxford University Press.

[87] Klabbers, J. (1998) Clinching the Concept of Sovereignty: Wimbledon Redux. *Austrian Review of International and European Law*, 3 (1).

[88] Koskenniemi, M. (2005) *From Apology to Utopia: the Structure of International Legal Argument*. Cambridge: Cambridge University Press.

[89] Kremlin. (2015) *Article by Vladimir Putin "On the Historical Unity of Russians and Ukrainians"*. [online] Moscow: Kremlin. Available from: http://en.kremlin.ru/events/president/news/66181.

[90] Kudláčková, I., Wallace, D. and Harašta, J. Cyber Weapons Review in Situations Below the Threshold of Armed Conflict. In Jančárková, T. et al (Eds.) *20/20 Vision: The Next Decade*. Tallinn: NATO CCDCOE Publications. Available from: https://ccdcoe.org/uploads/2020/05/CyCon_2020_6_Kudlackova_Wallace_Harasta.pdf [Accessed 20 April 2023].

[91] *LaGrand (Germany v. United States of America)*, Memorial of the Federal Republic of Germany of 16 September 1999, paragraph 6.53. This issue was not addressed, but the ICJ did reference this *LaGrand (Germany v. United States of America)* [2001] ICJ Rep 466, paragraph 125.

[92] *Law on Activities in Outer Space* [online], L 128 (2016). Available from: https://www.ft.dk/RIpdf/samling/20151/lovforslag/L128/20151_L128_som_vedtaget.pdf (in Danish), paragraph 4(4).

[93] *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory (Advisory Opinion)*, [2004] ICJ Rep 136.

[94] *Legality of the Use by a State of Nuclear Weapons in Armed Conflict (Advisory Opinion)* [1996] ICJ Rep 66.

[95] *Letter from the Government of the Kingdom of the Netherlands, Minister of Foreign Affairs to Parliament* (July 2019), p. 2. [online] United Nations Office for Disarmament Affairs: New York. Available from: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/02/appendix-Internaional-law-in-cyberspace-kingdom-of-the-netherlands.pdf [Accessed 7 November 2022].

[96] *M/V 'Saiga' (No 2) Case (Saint Vincent and the Grenadines v Guinea)* [1999] ITLOS Rep 10.

[97] Markert, L. and Freiburg, E. (2013) Moral Damages in International Investment Disputes - On the Search for a Legal Basis and Guiding Principles. Journal of World Investment & Trade, 14 (1).

[98] *Mavrommatis Palestine Concessions* [1924] PCIJ (ser A) no 2.

[99] McLaughlin, M. (2023) Deterring the Next Invasion: Applying the Accumulation of Events Theory to Cyberspace. [online] Opinio Juris. Available from: http://opiniojuris.org/2023/03/02/deterring-the-next-invasion-applying-the-accumulation-of-events-theory-to-cyberspace/) [Accessed 20 April 2023].

[100] Menthe, D.C. (1998) Jurisdiction in Cyberspace: A Theory of International Spaces. *Michigan Telecommunications and Technology Law Review* 4.

[101] Ministry for Foreign Affairs, Finland, *Finland published its positions on public international law in cyberspace* (15 October 2020). [online] Finnish Ministry of Foreign Affairs: Helsinki. Available from: https://

valtioneuvosto.fi/en/-/finland-published-its-positions-on-public-international-law-in-cyberspace [Accessed 7 November 2022].

[102] *Mixed Claims Commission Netherlands-Venezuela* (1903) X RIAA 703.

[103] *Nationality Decrees Issued in Tunis and Morocco [French Zone], Advisory Opinion*, [1923] PCIJ Rep (Ser B) No 4, p. 24; and S.S. Lotus, (France v. Turkey), (1927) PCIJ Ser. A, No. 10.

[104] *Naulilaa Case (Germany v Portugal)*, (1928) II RIAA 1011.

[105] *North Sea Continental Shelf Cases (Germany v. Denmark; Germany v. the Netherlands)* [1969] ICJ Rep 3.

[106] *Norwegian positions on selected questions of international law relating to cyberspace* (May 2021), p. 3. [online] Oslo: Government of Norway. Available from https://www.regjeringen.no/contentassets/a8911fc020c94eb386a1ec7917bf0d03/norwegian_positions.pdf [Accessed 7 November 2022].

[107] *Nottebohm (Liechtenstein v. Guatemala)*, [1955], ICJ Rep 4, p .24

[108] O'Connor, J. M. 'International Law Framework for Employing Cyber Capabilities in Military Operations' (Memorandum, 19 January 2017).

[109] *On the Application of International Law in Cyberspace* (March 2021), p. 4. [online] Berlin: Ministry of Foreign Affairs, Germany. Available from: https://www.auswaertiges-amt.de/blob/2446304/2ae17233b62966a4b7f16d50ca3c6802/on-the-application-of-international-law-in-cyberspace-data.pdf [Accessed 7 November 2022].

[110] Open-ended working group on developments in the field of information and telecommunications in the context of international security, "Final Substantive Report" (10 March 2021), [online] New York: UN Office of Disarmament Affairs. Available from: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf [Accessed 7 November 2022].

[111] *Opinion in the Lusitania Cases (United States v Germany)* (1956) VII RIAA 32.

[112] Oppenheim, L. and Roxburgh, R. (2005) *International Law: A Treatise, Vol I: Peace*. 3rd ed. The Lawbook Exchange: Clark.

[113] Orakhelashvili, A., 'State Jurisdiction in International Law: Complexities of a Basic Concept', in Orakhelashvili, A. (ed.) (2015), *Research Handbook on Jurisdiction and Immunities in International Law*, Cheltenham: Edward Elgar Publishing.

[114] Oster, J. 'Rethinking Shevill. Conceptualising the EU private international law

of Internet torts against personality rights', 26(2-3) *International Review of Law, Computers & Technology* (2012).

[115] Østerdahl, I. (1992) *Freedom of Information in Question: Freedom of information in international law and the calls for a New World Information and Communication Order (NWICO)*. Uppsala: Iustus Förlag AB.

[116] Osula, A.-M., Kasper, A. and Kajander, A. (2022) EU Common Position on International Law and Cyberspace. *Masaryk University Journal of Law and Technology*, 16 (1).

[117] Paris Agreement, 12 December 2015, 3156 UNTS (entered into force 4 November 2016), art 13(3).

[118] *Phosphates in Morocco*, [1938], PCIJ, Series A/B, No. 74.

[119] Pirim, C. Z. (2020) Reparation by Pecuniary Means of Direct Moral Damages Suffered by States as a Result of Internationally Wrongful Acts. Journal of International Dispute Settlement 11.

[120] Polcak, R. and Svantesson, D. (2017) *Information Sovereignty – Data Privacy, Sovereign Powers and the Rule of Law*. Cheltenham: Edward Elgar Publishing.

[121] *Position Paper on the Application of International Law in Cyberspace* (2022), p. 2. [online] Stockholm: Government of Sweden. Available from: https://www.regeringen.se/4a1ce0/contentassets/2bf3882c23bb4fdfb935310b03d562a1/swedens-position-paper-on-the-application-of-international-law-in-cyberspace.pdf [Accessed 7 November 2022].

[122] *President at the inauguration ceremony of direct reduction plant: Iranian nation unsanctionable/ We'll negotiate anywhere necessary for nation's interests*, press statement (11 November 2019). [online] Tehran: Ministry of Foreign Affairs of the Islamic Republic of Iran. Available from: https://en.mfa.gov.ir/portal/NewsView/568055 [Accessed 7 November 2022].

[123] *President Xi Jinping Meets Iranian President Ebrahim Raisi* (16 September 2022). [online] Beijing: Ministry of Foreign Affairs of the People's Republic of China. Available from: https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/202209/t20220916_10766906.html [Accessed 7 November 2022].

[124] *Prosecutor v Tihomir Blaškić (Decision on the Objection of the Republic of Croatia to the Issuance of Subpoenae Duces Tecum)* IT-95-14-PT (18 July 1997).

[125] *Pulp Mills on the River Uruguay (Argentina v. Uruguay)*, [2010] ICJ Rep 14.

[126] *Recognition/Non-Recognition in International Law*, proceedings from the Sydney Conference of the International Law Association (2018), p. 5. [online] London: International Law Association. Available from: https://www.ila-

hq.org/en_GB/documents/conference-report-sydney-2018-6 [Accessed 7 November 2022].

[127] *Reparation for Injuries suffered in the Service of the United Nations, Advisory Opinion*, [1949] ICJ Rep 174.

[128] *S.S. Lotus, (France v. Turkey)* (1927) PCIJ Ser. A, No. 10, pp. 18-19.

[129] Schiff Berman, P. (2014) Global Legal Pluralism: A Jurisprudence of Law beyond Borders, Cambridge: Cambridge University Press.

[130] Schmitt, M. (ed.) (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd ed. Cambridge: Cambridge University Press.

[131] Schultz, T. 'Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface', 19(4) *European Journal of International Law* (2008) pp. 799-839.

[132] Shaw, M. N. (2021) *International Law*. 9th ed. Cambridge: Cambridge University Press.

[133] Simonovic, I. (2002) Relative Sovereignty of the Twenty First Century. *Hastings International & Comparative Law Review*, 25.

[134] Slaughter, A. 'The Future of International Law Is Domestic (or, The European Way of Law)', 47(2) *Harvard International Law Journal* (2006) pp. 327-352.

[135] *Statement by Richard Kadlčák at Open-ended Working Group on developments in the field of information and telecommunications in the context of international security of the First Committee of the General Assembly of the United Nations* (11 February 2020). [online] Prague: National Cyber and Information Security Agency, Czech Republic. Available from: https://www.nukib.cz/download/publications_en/CZ\%20Statement\%20-\%20OEWG\%20-\%20International\%20Law\%2011.02.2020.pdf [Accessed 7 November 2022].

[136] *Statement of Spokesman for DPRK Foreign Ministry* (5 November 2022). [online] Pyongyang: Ministry of Foreign Affairs of the Democratic People's Republic of Korea. Available from: http://www.mfa.gov.kp/view/article/16089 [Accessed 7 November 2022].

[137] Sung-Won Yoon (2008) Sovereign Dignity, Nationalism and the Health of a Nation: A Study of China's Response in Combat of Epidemic. *Studies in Ethnicity and Nationalism* 8 (1), p. 85

[138] Svantesson, D. (2006) Borders on, or border around – the future of the Internet. *Albany Law Journal of Science & Technology*, 16 (2).

[139] Svantesson, D. (2017) *Solving the Internet Jurisdiction Puzzle*. Oxford: Oxford University Press.

[140] Svantesson, D. (2018) 'Lagom jurisdiction' – What Viking drinking etiquette

can teach us about Internet jurisdiction and Google France. *Masaryk University Journal of Law and Technology*, 12 (1).

[141] Svantesson, D. (2020) Is International Law Ready for the (Already Ongoing) Digital Age? Perspectives from Private and Public International Law. In: Busstra, M. et al (eds.) *International Law for a Digital World*. T. M. C. Asser Press: The Hague, 147.

[142] Svantesson, D. et al (2021) *The developing concept of sovereignty: considerations for defence operations in cyberspace and outer space*, Technology and Jurisdiction Research Team, Bond University.

[143] *Switzerland's position paper on the application of international law in cyberspace* (2021), p. 3. [online] Bern: Federal Department of Foreign Affairs, Switzerland. Available from: https://www.eda.admin.ch/content/dam/eda/en/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_EN.pdf [Accessed 7 November 2022].

[144] Sydney Morning Herald (27 May 2021) *Chinese foreign minister tells Germans 'you know what genocide looks like'*. [online] Sydney: Sydney Morning Herald. Available from: https://www.smh.com.au/world/europe/chinese-foreign-minister-tells-germans-you-know-what-genocide-looks-like-20210526-p57vdy.html [Accessed 7 November 2022] .

[145] Sydney Morning Herald. (20 July 2021) *'Illicit gain': Australia accuses China of criminal cyber attacks*, [online] Sydney: Sydney Morning Herald. Available from: https://www.smh.com.au/politics/federal/illicit-gain-australia-accuses-china-of-criminal-cyber-attacks-20210720-p58b6s.html [Accessed 7 November 2022].

[146] *The Application of International Law to State Activity in Cyberspace* (1 Dec 2020). [online] New Zealand Foreign Affairs & Trade: Wellington. Available from: https://dpmc.govt.nz/sites/default/files/2020-12/The\%20Application\%20of\%20International\%20Law\%20to\%20State\%20Activity\%20in\%20Cyberspace.pdf [Accessed 12 December 2022].

[147] The Prosecutor v. Dusko Tadić, IT-94-1-AR72, Appeals Chamber, Decision, 2 October 1995.

[148] *The R.O.C. (Taiwan) government terminates diplomatic relations with Solomon Islands with immediate effect to uphold national dignity* (16 September 2019). [online] Taipei: Ministry of Foreign Affairs of the Republic of China (Taiwan). Available from: https://en.mofa.gov.tw/News_Content.aspx?n=1330&sms=274&s=34155 [Accessed 7 November 2022].

[149] The Taiwan Question and China's Reunification in the New Era (2022). [online] Beijing: Taiwan Affairs Office of the State Council and The State Council Information Office of the People's Republic of China. Available from: https://english.www.gov.cn/atts/stream/files/62f34db4c6d028997c37ca98 [Accessed 7 November 2022].

[150] *Trail Smelter Case (United States, v Canada)* (Decision of 11 March 1941), [1949] III RIAA 1905.

[151] *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*, 27 January 1967, 610 UNTS 205 (entered into force 10 October 1967).

[152] Ubertazzi, B. (2012) Exclusive Jurisdiction in Intellectual Property, Tübingen: Mohr Siebeck; Cooper, D. et al. (eds.) 'Data protection law and international dispute resolution', 382 *Recueil des Cours of the Hague Academy of International Law* (2017).

[153] Ukraine never had a tradition of genuine statehood': Reuters. (2022) *Extracts from Putin's speech on Ukraine*. [online] London: Reuters. Available from: https://www.reuters.com/world/europe/extracts-putins-speech-ukraine-2022-02-21/ [Accessed 7 November 2022].

[154] UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (24 June 2013) UN Doc A/68/98.

[155] UNCOPUOS, *Questionnaire on possible legal issues with regard to aerospace objects: replies from Member States*, UN Doc A/AC.105/635/Add.7.

[156] UNGA, *Charter of Economic Rights and Duties of States*, UN Doc A/RES/3281(XXIX) (1974).

[157] UNGA, *Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations*, UN Doc A/RES/2625 (XXV) (1970).

[158] UNGA, *Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations*, UN Doc A/RES/42/22 (1988).

[159] UNGA, *Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty*, UNGAOR 20th Sess, UN Doc A/RES/2131(XX) (1965).

[160] UNGA, *Developments in the Field of Information and Telecommunications in*

the Context of International Security: Report of the Secretary-General, UN Doc A/74/120 (24 June 2019) 22-6.

[161] UNGA, *Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries*, UN Doc A/CN.4/SER.A/2001/Add.1 (2001).

[162] UNGA, *Draft Declaration on Rights and Duties of States*, GA Res 375(IV), UN Doc A/RES/375(IV) (1949).

[163] UNGA, *Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266*, UN Doc A/76/136 (2021).

[164] UNGA, *Permanent sovereignty over natural resources*, UN Doc A/RES/3171 (1973).

[165] UNGA, *Responsibility of States for Internationally Wrongful Acts*, 53 UN GAOR Supp, UN Doc A/56/83 (2002).

[166] UNGA, *Territorial integrity of Ukraine: defending the principles of the Charter of the United Nations*, GA Res ES-11/4, UN Doc A/RES/ES-11/4 (12 October 202) (143 in favour, 5 against, 35 abstentions).

[167] United Nations Convention on the Law of the Sea, signed on 10 December 1982, 1833 UNTS 3 (entered into force 16 November 1994).

[168] *Vienna Convention on Consular Relations*, signed on 24 April 1963, 596 UNTS 261 (entered into force 19 March 1967).

[169] Waldron, J. (2011) Are Sovereigns Entitled to the Benefit of the International Rule of Law? European Journal of International Law, 22 (2).

[170] Wright, J. (2018) *Cyber and International Law in the 21st Century.* Speech, Chatham House, Royal Institute of International Affairs. [online] London: Government of the United Kingdom. Available from `https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century` [Accessed 7 November 2022].

DOI 10.5817/MUJLTXXXX-X-X

THE UNWANTED PARADOXES OF THE RIGHT TO BE FORGOTTEN *

by

LUSINE VARDANYAN † HOVSEP KOCHARYAN ‡
ONDREJ HAMUĽÁK § MATÚŠ MESARČÍK ¶
TANEL KERIKMÄE || TEA KOOKMAA **

The dynamic development of digital and informational technologies raises the issue of proper and effective protection of human privacy, which, in turn, is gradually turning from a real fundamental right into a kind of illusion. Just a piece of information about an individual distributed on the Internet may leave its negative and often indelible mark on the life and reputation of the addressee of such information, regardless of the legality and reliability of such information. And even if such information is subsequently recognized as false and/or vicious and even removed from public access, the addressee of the information will still be associated with such information in the social consciousness. In this regard, each person is at risk on the Internet, where anyone can potentially become the victim of a single publication or a post of an Internet user. In this context the emergence of the phenomenon of the right to be forgotten in European legal reality may be considered as a step forward in the question of human privacy protection in the digital age. However, this right is not without drawbacks. The most significant of these drawbacks will be analyzed in this paper, such as the practical difficulties

* The paper has been prepared on behalf of the project GAČR no. 20-27227S "The Advent, Pitfalls and Limits of Digital Sovereignty of the European Union" funded by the Czech Science Foundation.

† Lusine Vardanyan, lusine.vardanyan01@upol.cz, Ph.D. Candidate, Palacký University Olomouc, Faculty of Law, Czech Republic;

‡ Hovsep Kocharyan, hovsep.kocharyan01@upol.cz, Ph.D. Candidate, Palacký University Olomouc, Faculty of Law, Czech Republic;

§ Ondrej Hamuľák (corresponding author), ondrej.hamulak@upol.cz, Senior Researcher, Palacký University Olomouc, Faculty of Law, Czech Republic;

¶ Matúš Mesarčík, matus.mesarcik@flaw.uniba.sk, Assistant Professor, Comenius University in Bratislava, Faculty of Law, Slovakia;

|| Tanel Kerikmäe, tanel.kerikmae@taltech.ee, Professor of European Legal Policy and Law Tech, Tallinn University of Technology (TalTech), Department of Law, Estonia;

** Tea Kookmaa, tea.kookmaa@njordlaw.ee, Attorney-at-law, NJORD Law Firm, Estonia.

of thoroughly exercising this right and the difficulties posed by new technological developments.

KEY WORDS
right to be forgotten, privacy, GDPR, technology, innovation

1. INTRODUCTION
The right to be forgotten (the right to erasure) is a deeply interconnected with the judicial law-making activity of the CJEU. Its significant development in the European legal reality is connected with an unprecedented case of Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) (known as the Google Spain case or Costeja case), where the Court ruled that: "the data subject may (...) require those links (concerning him/her) to be removed from the list of (search) results", "(...) in particular where they appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes and in the light of the time that has elapsed"[1]. The CJEU's judgment naturally caused a number of questions and discussions regarding the essence and nature of this right. In particular, some experts have critically perceived the emergence of the phenomenon of the right to be forgotten, consideringit as "unforgettable fiasco, (...) morphing into a nightmare for the web giant"[2], "an emerging threat to media freedom in the digital age"[3], "that threatens to censor entire swathes of the web"[4]. However, despite the existence of critical views, other scholars, on the contrary, reacted positively to the Court's judgment, arguing that the right to be forgotten as a privacy-protective right, that can exist side-by-side with freedom of expression and information, and with a reasonable delineation of their borders and an effective balancing of their coexistence, such a right can provide the data subject with opportunity to perform his/her privacy protection on the "eternal" Internet. As L. Cook points out: "The right

[1] Judgement of 13 May 2014, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, C-131/12, EU:C:2014:317 (herein after "Google Spain"), paragraph 98, paragraph 94.

[2] Wohlsen, M. (2014) For Google, the 'Right to Be Forgotten' Is an Unforgettable Fiasco. *WIRED* Available from: https://www.wired.com/2014/07/google-right-to-be-forgotten-censorship-is-an-unforgettable-fiasco/

[3] Oghia, M. J. (2018) Information Not Found: The "Right to Be Forgotten" as an Emerging Threat to Media Freedom in the Digital Age. *CIMA Digital Report*. Available from: https://www.cima.ned.org/publication/right-to-be-forgotten-threat-press-freedom-digital-age/

[4] See Solon, O. (2014) EU 'Right To Be Forgotten' Ruling Paves Way for Censorship. *WIRED* Available from: http://www.wired.co.uk/news/archive/2014-05/13/right-to-be-forgotten-blog

to be forgotten represents a positive shift in cyberspace law and policy because it increases individuals' control over personal information, and restores the balance between free speech and privacy in the digital world"[5], in the conditions when "(...) the Internet has robbed individuals of both privacy and autonomy in a sense that we no longer have the choice to keep certain information private, nor do we have the freedom not to speak"[6].

As we can see, before the right to be forgotten was written into the law, it had already been extended via interpretation of the right to erasure as one of the rights of the data subject by the CJEU in its case-law. In the year 2016, the European Commission adopted a new regulation – the Regulation (EU) 2016/679 of the European Parliament and of the Council, also known as the General Data Protection Regulation (the GDPR). The aim of adopting a new regulation was to create unified data protection related rules in all Member States of the EU. In several aspects, the GDPR resembles its predecessor, Directive 95/46/EC of the European Parliament and of the Council. Most of the general principles related to data protection, as well as the obligations applicable to data processing entities are similar to those in the Directive. However, the GDPR also stipulates new obligations for data processing entities. In addition, the GDPR specifies certain data subjects' rights and stipulates a few new ones. In its Article 17, the GDPR stipulates that the data subject "shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies." The grounds for exercising the right to be forgotten are specified in Article 17(1).

However, the implementation of the right to be forgotten in legal practice is not without drawbacks, naturally leaving its negative mark on the effectiveness of protecting the data subjects' privacy in the digital age, which will be analysed in more detail below. Although several statistics exist concerning the effectiveness of the right to be forgotten[7], the authors aim to point out paradoxes provided by the exercise of the right in question that may significantly influence the outcome in a negative way and ultimately diminish the protection of an individual.

The goal of the article is to discuss the challenges for the right to be forgotten from three angles – the jurisprudence of the CJEU,

[5] Cook L. (2015) The Right to Be Forgotten: A Step in the Right Direction for Cyberspace Law and Policy. Journal of Law, Technology & Internet 6(1). Available from: https://scholarlycommons.law.case.edu/jolti/vol6/iss1/8

[6] Ibid.

[7] See e.g. Google Transparency Report on delisting requests.Available from: https://transparencyreport.google.com/eu-privacy/overview.

regulatory provisions and emerging new concepts in technology. In the first part of the article, the authors will provide an overview of drawbacks of the right to be forgotten considering the selected paradoxes deriving from the jurisprudence of the CJEU and regulatory provisions. In sections two and three of the article authors analyse two landmark decisions of the CJEU that create unwanted paradoxes of remembering claimants despite their efforts to be forgotten. However, shortcomings of the right to be forgotten are not inherited only through the decisions of the CJEU. The fourth part of the article discusses regulatory gaps concerning the reflection of the right in the GDPR. The fifth section provides an analysis of potential challenges raised by new technologies and related new concepts as the emergence of this virtual space represents an ideal laboratory for further discussion on remembering and forgetting in the digital world. Conclusions are provided at the end of the article.

2. COSTEJA'S UNFORGETTABLE PARADOX: HOW TO BE UNINTENTIONALLY REMEMBERED?

The growing interest in the right to be forgotten is due to the fact that nowadays ensuring the protection of the right to privacy as one of the fundamental human rights in the EU is one of the most important tasks of the EU human rights law, which still remains as a real headache for the EU lawmakers, especially in the conditions of rapid development of digital technologies. In this framework, the CJEU's ruling may be considered as a sort of response to intervention in human privacy and a step forward for finding an effective *status quo* between the right to privacy and freedom of expression and information[8], because "Once information is uploaded, the Internet stores it permanently, in what has been called 'digital eternity'. Hence, when personal information is uploaded online, our most embarrassing or painful moments may acquire lasting significance and haunt our lives. The Internet is an integral part of our lives to collect information, manage finances, socialize, and shop. Thus, it risks infringing upon individuals' right to privacy"[9].

However, being the cradle of the right to be forgotten, the CJEU nonetheless makes serious mistake in its judgments, which naturally leaves

[8] Concerning the human rights aspect of the decision, see paras 66 and 69 of the Google Spain case. The case itself is deliberated under the prism of Article 7 and Article 8 of the Charter of the fundamental rights of the European Union.

[9] Alessi, S. (2017) Eternal Sunshine: The Right to Be Forgotten in the European Union after the 2016 General Data Protection Regulation. *Emory International Law Review* 32(1). Available from: https://scholarlycommons.law.emory.edu/cgi/viewcontent.cgi?article=1186&context=eilr

its negative mark on the effectiveness of protecting of the data subjects' privacy in the digital age. In this context naturally arise the questions on how the CJEU's judgment weakens the privacy-protective potential of this right? The answer is hidden in the description of the factual circumstances by the CJEU in its judgment on Google Spain case. In particular, the paragraph 14 of the case states that: "(...) when an internet user entered Mr. Costeja González's name in the search engine of the Google group ('Google Search'), he would obtain links to two pages of La Vanguardia's newspaper, of 19 January and 9 March 1998 respectively, on which an announcement mentioning Mr. Costeja González's name appeared for a real-estate auction connected with attachment proceedings for the recovery of social security debts."[10] As it can be noticed, from the very wording of the factual circumstances of the Google Spain case, it is possible to clearly understand what personal data the applicant wanted to hide from public access to protect his privacy. This is due to the fact that the Court not only described the applicant's name, neglecting the rules for maintaining the confidentiality of data subjects taking into account the essence and nature of the case under consideration, but also did not hide from public access the personal information that the applicant sought to remove from the Internet search engine.

In such circumstances, the following questions naturally arise: first, could it be considered that the CJEU's judgment effectively protected the privacy of Mr. Costeja González, and, second, is it possible in such conditions to call the Google Spain case as victorious for the applicant, and consider it as a victory in fact? We can safely answer no, since the Court only de jure protected the privacy of Mr. Costeja González, but de facto only inadvertently aggravated his situation. As we can see, even if the applicant, who applied to the court regarding the realization of his right to be forgotten, wins the court proceeding and achieves the removal of his undesirable personal data from the Internet, such personal data will still be publicly available (for example, on the CJEU's official websites: http://curia.europa.eu or https://eur-lex.europa.eu), where any Internet user can read, as, for example, the authors of this scientific research. And this is all just a natural consequence of the fact that from the very beginning the Court did not properly take care of protecting the applicant's privacy and hiding information that was the subject of the dispute in the case under consideration. It turns out that the CJEU's judgment on the Google Spain case had the opposite effect on the data subject: it can be said that instead of the right to be forgotten, his right

[10] Google Spain case, para 14.

to be remembered was realized. Paradoxically, the CJEU itself became an 'undesirable PR manager' of the applicant, whose name is associated with the information on his insolvency and firmly entrenched in the public consciousness due to the works of various experts, scientists and journalists, turning his case into "a perfect example of the Streisand Effect in action"[11]. This fact is also emphasized by M. Xue, G. Magno and others, who tend to believe that: "Costeja himself suffers from the Streisand effect – although he won this landmark case, it is unlikely he will ever be forgotten because his name now appears on thousands of web sites".[12] The same opinion is held by A. Bunn, arguing that: "For Mr. González the decision has resulted in something of a curious irony: his bid not to be indefinitely linked through Google search to information concerning his debts was successful, but as a result of that success he is likely to be linked to the information he wished forgotten for a long time to come".[13] In his turn, P. W. Erikson points out that: "In a case of ultimate irony, Costeja González, who has been the subject of news stories around the world, will be now very difficult to ever forget. Perhaps his new celebrity status will offset any negatives".[14] In this context the Court's attitude to the presentation of the factual circumstances even allows to call the Google Spain case useless for the applicant, who, instead of getting rid of painful data, found himself in the public spotlight. According to G. Giampa: "(...) the sheer lack of respect for privacy along with the immediate gratification an individual receives through a Google search or Twitter feed. Costeja Gonzalez has inadvertently fought 'for the right[s] of others to more easily safeguard their privacy', but the principle outweighs the effects of the legal action"[15].

Of course, one can argue that this case was unprecedented for the Court's judicial practice, and the CJEU could not then foresee the effect of its judgment, which lead to the situation that "Mr. Costeja is better

[11] Holland, J.A. (2019) Contemporary Practical Alternatives to a "Right To Be Forgotten" in the United States. *Latin American Law Review* 2. Available from: https://revistas.uniandes.edu.co/doi/full/10.29263/lar02.2019.02

[12] Xue M., Magno G. et al. (2016) The Right to be Forgotten in the Media: A Data-Driven Study. *Proceedings on Privacy Enhancing Technologies 2016* (4). p. 1–14. Available from: http://www.nyu.engineering/sites/default/files/migrated/pdfs/RTBF_Data_Study.pdf

[13] Bunn, A. (2015) The curious case of the right to be forgotten. *Computer Law & Security Review* 31(3). p. 336 - 350. Available from: https://www.sciencedirect.com/science/article/abs/pii/S0267364915000606

[14] Erikson, P.W. (2014) The EU's right to be forgotten. Available from: https://www.linkedin.com/pulse/20140710033506-2822374-the-eu-s-right-to-be-forgotten/

[15] Giampa, G. (2016) Americans Have a Right to Be Forgotten. *Law School Student Scholarship* 740. Available from: https://scholarship.shu.edu/student_scholarship/740/

known than before".[16] Although the mere fact of the unprecedented nature of the case cannot be considered as a justification for the Court's approach. Being the EU's highest judicial authority, it should understand the importance of careful description of the factual circumstances in its judgments to duly protect legitimate interests of the participants in the judicial process, especially in the conditions of the digital age, where the fragile privacy and reputation of a person very often become targets of the Internet community. As an example, we can take the case of the famous actress Barbra Streisand, who demanded the removal of the photo of her Malibu house taken by photographer Kenneth Adelman from the Internet, and her lawsuit only dramatically increased the number of views of this photo on the Internet, hence the name "Streisand effect", i.e. the effect of even greater spread of information when trying to hide or remove it from the public access.[17] Another example is the case of Max Mosley, who filed a lawsuit to protect his privacy and remove from the Internet his photos, containing sexual content, and although he won the case, the search results increased the frequency of references to the episode.[18]

It should be noted that such cases are numerous in practice, especially in the world of celebrities. The public is always interested in such 'forbidden' information, starting with unsuccessful photos of the American singer Beyonce[19] and ending with the romance of the Welsh footballer Ryan Giggs[20], because as it is said the forbidden fruit is always the sweetest. As A. De Baets rightly observes: "(...) any removal of documents would arouse curiosity and direct attention towards, rather than away from (...). Although the availability of digital information quickly publishable on the internet enhances both the disclosure of embarrassing information and tighter informational self-determination strategies, (...) the application of the right to be forgotten would not substantially affect the totality

[16] Schechner, S. (2014) Google Defends 'Right to Be Forgotten' Response. *Wall Street Journal*. Available from: https://www.wsj.com/articles/google-defends-right-to-be-forgotten-response-1416414403

[17] See Barbara Streisand vs. Kenneth Adelman et. al. Superior Court of California, County of Los Angeles, Case No. SC077257

[18] See Mosley v. News Group Newspapers [2008] EWHC 1777 (QB).

[19] See Zhang, M. (2013) Beyonce Publicist's Takedown Request Causes Unflattering Photos to Go Viral. *PetaPixel*. Available from: https://petapixel.com/2013/02/08/beyonce-publicists-takedown-request-causes-unflattering-photos-to-go-viral/

[20] See Masnick, M. (2011) Forget The Streisand Effect, I Think We've Seen The Dawning Of The Giggs Effect. *techdirt*. Available from: https://www.techdirt.com/articles/20110520/16102414365/forget-streisand-effect-i-think-weve-seen-dawning-giggs-effect.shtml

of sources for historians studying absolute public figures."[21] In such situations, the CJEU should not forget that in the digital world the issue of protecting the person's privacy and reputation becomes even more serious and vulnerable than protecting privacy and reputation offline. This means that it is necessary to be extremely careful in presenting the factual circumstances of the case and, if necessary, hide from public access information that can violate the applicant's privacy and reputation. And it cannot be said that the Court does not have such powers: it is enough to pay attention to the provision of Article 31 of the Protocol (No. 3) on the Statute of the Court of Justice of the European Union, providing that: "The hearing in court shall be public, unless the Court of Justice, of its own motion or on application by the parties, decides otherwise for serious reasons."[22] At the same time, the protection of the privacy, reputation and legitimate interests of the applicant can be safely considered as 'serious reasons' for the purposes of the above provision, because it is not by chance that the EU Charter on Fundamental Rights recognizes the fundamental nature of the rights to privacy and data protection[23].

3. PIESCZEK'S EFFECT AS A NEW EXAMPLE OF COSTEJA'S UNFORGETTABLE PARADOX?

It should be noted that the Costeja case is not the only case of the CJEU's 'blunder'. In the case of Eva Glawischnig-Piesczek v Facebook Ireland Limited, another victim of the Court's short-sighted approach in ensuring the applicant's privacy became the Austrian politician Eva Glawischnig-Piesczek, who appealed to the court for protection of her rights in connection with rude and offensive expressions of an Internet user about her. Analysing this case, it is possible to notice that the CJEU as in the case of Google Spain again forgets about the importance of ensuring the confidentiality of both the applicant herself and the information that caused the consideration of the case. Thus, in the Court's judgment the following factual circumstances are mentioned: "On 3 April 2016, a Facebook Service user shared on that user's personal page an article from the Austrian online news magazine

[21] De Baets, A. (2016) A historian's view on the right to be forgotten. *International Review of Law, Computers & Technology* 30(1-2). Available from: https://www.tandfonline.com/doi/full/10.1080/13600869.2015.1125155

[22] *Consolidated version of the Treaty on the Functioning of the European Union Protocol (No 3) on the Statute of the Court of Justice of the European Union*, 7 June 2016 (C 202/210). Available from: http://data.europa.eu/eli/treaty/tfeu_2016/pro_3/oj

[23] See art. 7 and 8 of the *Charter of Fundamental Rights of the European Union* (2012/C, 326/02). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex\%3A12012P\%2FTXT

oe24.at entitled 'Greens: Minimum income for refugees should stay', which had the effect of generating on that page a 'thumbnail' of the original site, containing the title and a brief summary of the article, and a photograph of Ms Glawischnig-Piesczek. That user also published, in connection with that article, a comment which the referring court found to be harmful to the reputation of the applicant in the main proceedings, and which insulted and defamed her. This post could be accessed by any Facebook user."[24] Of course, unlike the Costeja case, the information, which is "harmful to the reputation of the applicant (…) which insulted and defamed her"[25], is not directly disclosed in the judgment, although it is still mentioned about the fact of insulting and slander against the well-known Austrian politician Ms. Glawischnig-Piesczek. However, it is impossible to blame only the Court: the Advocate General (AG), who made his opinion on this case may also be considered as a culprit. It is only necessary to pay attention to the paragraphs 12 and 14 of the Opinion of AG Szpunar, where applicant's data, as well as the subject of the case under consideration, are not kept confidential: "On 3 April 2016 a user (...) also published (...) an accompanying disparaging comment about the applicant accusing her of being a 'lousy traitor of the people', a 'corrupt oaf' and a member of a 'fascist party'. (…) namely that the applicant was a 'lousy traitor of the people' and/or a 'corrupt oaf' and/or a member of a 'fascist party'.[26] That is, if the fault of the Court was that it did not hide the applicant's identity in its judgment, then the AG is responsible for not initially hiding information, containing defamation against the Austrian politician, which, in turn, may be called as another example of manifestation of the 'Streisand effect' in the CJEU's judicial practice, because as D. Keller correctly notes: "On the claimant's side, the question is whether a filter effectively protects legitimate interests and rights — like the reputation and dignity rights at issue in Glawischnig-Piesczek. A clumsy filter, with conspicuous errors causing a 'Streisand effect' and additional negative attention to the claimant, might ultimately fail to protect her interests."[27] In his turn, M. Smith highlights that: "Facebook can be ordered to scrub those words—and any 'equivalent'

[24] Judgement of 3 October 2019, Eva Glawischnig-Piesczek v Facebook Ireland Limited, C-18/18, EU:C:2019:821, paragraph 12.

[25] Ibid.

[26] Opinion of AG Szpunar in Judgement of 3 October 2019, Eva Glawischnig-Piesczek v Facebook Ireland Limited, C-18/18, EU:C:2019:821, Recitals 12, 14.

[27] Keller, D. (2019) The CJEU's new filtering case, the terrorist content regulation, and the future of filtering mandates in the EU. *The Center for Internet and Society.* Available from: http://cyberlaw.stanford.edu/blog/2019/12/cjeu\%E2\%80\%99s-new-filtering-case-terrorist-content-regulation-and-future-filtering-mandates-eu

language—from its platform (...) worldwide. So says the European Court of Justice (ECJ). But if you perform a Google search for 'lousy traitor' and 'corrupt oaf' (even without the 'fascist party' label), your top hit will be a New York Times opinion piece identifying by name and photo (...) (of Eva Glawischnig-Piesczek)".[28]

As one can see, the case of Eva Glawischnig-Piesczek v Facebook Ireland Limited once again confirms the fact that such practice essentially weakens the effectiveness of the right to be forgotten, and this is one of the reasons why these right turn into just an illusive tool for the data subject in the context of his/her privacy protection in the court. As M. Cunningham correctly notes: "Europeans sought suppression of all these stories, which ironically boosted them further into the spotlight, creating a 'Streisand effect,' an attempt to hide information that spurs the unintended consequence of publicizing it more widely (...) and scores of others publish stories about the right to be forgotten generally and often cite to particular stories targeted for erasure".[29] Of course, this state of affairs may cause a negative impact on the CJEU's reputation and the EU citizens may have sceptical and even nihilistic views on the effectiveness of the Court's activities in the field of protecting their fundamental rights, and therefore the Court should change its approach when considering cases of this nature in order to avoid future manifestation of 'Costeja paradox' or 'Piesczek effect'. The Court should clearly understand that nowadays the contours of the formation of the right to be forgotten mostly depend on itself and it is not by chance that S. Kulk and F. Zuiderveen Borgesius note that: "The Court of Justice of the European Union gave limited guidance as to when a search result should be delisted (...) We can expect much more case law on delisting requests. More case law will hopefully lead to more guidelines for deciding delisting requests".[30] In the conditions of such an ineffective approach of the Court, the scenario of increasing case law on right to be forgotten cannot be expected, and thus this right may remain just a failed project, but not a real right that is able to protect human privacy and reputation. And if someone in such circumstances applies

[28] Smith, M. (2019) ANALYSIS: Global Censorship, but Not Erasure, Spurs Streisand Effect. *Bloomberg Law*. Available from: https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-global-censorship-but-not-erasure-spurs-streisand-effect.

[29] Cunningham, M. (2017) Privacy Law That Does Not Protect Privacy, Forgetting the Right to be Forgotten. *Buffalo Law Review* 65(3). Available from: https://digitalcommons.law.buffalo.edu/cgi/viewcontent.cgi?article=4656&context=buffalolawreview

[30] Kulk S. and Borgesius, Z. F. (2017) Privacy, Freedom of Expression, and the Right to Be Forgotten in Europe. In: Polonetsky, J., Tene, O. and Selinger E. (eds.) *Cambridge Handbook of Consumer Privacy*. Cambridge: Cambridge University Press. Available from: https://dare.uva.nl/search?identifier=f7d0f415-3404-426a-8833-12861fee7112

to the Court, most likely, the applicant's desire will not be the realization of his/her right to be forgotten, but on the contrary – his/her public exposition.

Another significant example regarding this issue is the ECtHR case of Hurbain v. Belgium.[31] Under the circumstances of this case, in 1994 in print edition of the Belgian daily newspaper Le Soir published an article about a fatal traffic accident caused by a drunk driver, as a result of which two people died and others were injured. The accident culprit stood trial and in 2006 he was rehabilitated. In 2011, he filed a lawsuit against Le Soir newspaper's publisher Patrick Hurbain, as a search on the applicant's last name immediately resulted in a link to the electronic archive of the newspaper Le Soir, where there was an article about the accident, which, according to the applicant, spoiled his reputation of a doctor, that is why he demanded to remove the text or at least hide his personal data from the article. As we can see, in this case, the same as in M.L. and W.W. v. Germany[32] and GC and Others v. CNIL[33] , only the name of the accident's culprit is concealed, but the factual circumstances capable of adequately protecting the anonymity of such a person are not concealed in any way. It should not be forgotten that the case concerned the removal of information from the electronic version of Le Soir's article, but not its print edition, and by detailing the circumstances of the accident, the Court still leaves open the possibility of identifying such a person, who, in turn, could become another victim of the 'Streisand effect'.

4. PRACTICAL DIFFICULTIES WHEN EXERCISING THE RIGHT TO BE FORGOTTEN

In addition to the jurisprudence of the CJEU discussed above, GDPR tries to take a step forward in ensuring that the data subject can effectively become forgotten. Article 17(2) stipulates the following: "Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data". Article 17(2) is of significant importance in ensuring the effectiveness of the right to be forgotten in our digital age. Pursuant to Article 17(2),

[31] *Hurbain v. Belgium.* (2021) ECtHR, No. 57292/16.
[32] *W.W. v. Germany.* (2018) ECtHR, No. 60798/10 and 65599/10.
[33] Judgement of 24 September 2019, GC and Others v. CINIL, C-136/17, EU:C:2019:773.

we can understand that the controller has two obligations. First, when receiving a valid request for the right to be forgotten, erase all personal data itself. In addition, when the controller has made this personal data public, the controller must take reasonable steps to inform other controllers of this request as well. The aim of Article 17(2) is to ensure that even if the initial controller has shared the personal data to third parties (other controllers), then the personal data at their disposal will be deleted as well.

The obligation stipulated in Article 17(2) definitely contributes to effective execution of the right to be forgotten in the digital age. It can be said with certainty that in most cases, at least when personal data is being processed as part of digital services, the data controller at some point discloses the data subject's personal data to other controllers as well. For example, when the data controller shares the personal data of its client, for marketing purposes, with another company belonging to the same group of companies as the controller itself.

While the obligation stipulated in Article 17(2) constitutes as a positive step towards ensuring the effective implementation of the right to be forgotten, the obligation to notify other controllers also raises several practical issues. The wording of Article 17(2) stipulates that the controller must take reasonable steps to inform other controllers. In addition, two other conditions apply: the controller must take into account available technology and the cost of implementation. It is important to note that the obligation to notify other controllers can, in many circumstances, be difficult for the controller. The controller may not be able to track down all the other controllers to whom it has shared personal data. In addition, even if the controller is able to track down the other controllers to whom it has shared the personal data, it is important to note that these controllers may have disclosed the same personal data to other controllers again. Article 17(2) stipulates that the controller must take reasonable steps to inform other controllers about the data subject's request to erase the personal data. The GDPR does not give any guidance as to what constitutes a reasonable step to inform other controllers. It is understandable that a strict obligation to inform all the other controllers would be too impractical. Considering how often data controllers share personal data with their co-operation partners, clients or entities in other roles, it is understandable that we cannot expect a controller to be able to inform all the other controllers. In that sense, the wording take reasonable steps seems a good balance. This means that the controller must make sufficient effort to notify the other controllers or the right to be forgotten. However, the controller is not obliged to make an unreasonable effort. What shall be sufficient to qualify as reasonable

steps shall depend on who is the controller and what is the context of the personal data processing overall. In addition, the controller must take into account available technology and the cost of implementation. In practice, the latter means that if the controller needs to implement new technological solutions to carry out the informing, then in that case the controller should assess the cost of implementation. It can be understood from the wording of Article 17(2) that the controller that is the technological solution for performing the notification obligation is too expensive for the controller, then this may, depending on the context, constitute as a legitimate ground for not going forward with informing the other controllers. However, the authors of the article have seen in their professional legal practice that many controllers struggle with understanding what the notion of reasonable steps mean in a particular situation where they are considering whether to take additional actions to notify other controllers or not. In many cases, informing other controllers about the right to be forgotten request can be time-consuming as well as expensive. Since the term reasonable steps has not been clarified further in the GDPR, it remains very abstract for the controller and is subject to interpretation. It is very likely that due to a lack of specific guidelines for interpreting reasonable steps, many controllers would interpret this in favor of themselves. Also, based on the authors' experience as legal professionals, it is likely that many controllers would rather avoid making efforts to inform other controllers about the data subject's request. This means that it is questionable how effectively Article 17(2) contributes to the effective implementation of the right to be forgotten on the top of unwanted paradoxes discussed in previous sections.

5. TECHNOLOGICAL ADVANCEMENTS AS A NEW BATTLEFIELD

In the future, new technological developments can pose even greater risks for the right to be forgotten. In recent years, new technological concepts such as the metaverse, NFTs[34] and blockchain technology[35] have been widely talked about and the use of these technologies is getting closer and closer to the services and products which people engage in daily.

One of the most intriguing topics in the field of technology at the moment is the emergence of metaverse. As a concept, the metaverse means an independent world of virtual reality. In 2020, Facebook announced the new name of its brand – Meta.[36] The change in the name of the brand

[34] Non-fungible token.

[35] An advanced database mechanism that allows transparent information sharing within a business network.

[36] Meta. (2021) *Introducing Meta: A Social Technology Company.* [press release] 28 October.

reflects the social media giant's future plans to develop Facebook from a social media company to a metaverse company. Facebook's aim is to use the metaverse to help people connect better. Facebook's vision of metaverse is a mixture of both virtual and augmented reality which enables people – with the use of VR headsets and other tools – to connect with each other in a more efficient and real-life simulating way. In addition, metaverse would allow people to engage in various types of immersive experiences.

It is important to note that the metaverse is a very new concept. Although it is discussed widely among both technology and legal experts, the actual meaning of the concept still remains vague.[37] Different legal experts, scholars, as well as experts in the field of technology have defined metaverse in their own ways. For example, some authors have said that "the idea of a metaverse involves a computer-generated universe; a fully immersive online world where people gather to play games, socialize and work."[38] In contrast, other authors have described the metaverse as "a shared virtual world that users can access from any platform via the internet, and where they can interact with their virtual avatars."[39] The fact that metaverse is still a vague concept is partly also due to the fact that some technological advancements are still needed to launch the metaverse. The idea of the metaverse rather reflects the coming of a new era.

However, if the metaverse would turn out at least to a large extent in the way as it has been described, it would bring along various opportunities in almost all fields – social media, entertainment, e-commerce, education and many others.[40] For example, metaverse would allow customers of e-shops to try on clothes in the virtual world. Similarly, elementary school students could learn about forest trees by immersing themselves into a forest in the metaverse.

Available from: https://about.fb.com/news/2021/10/facebook-company-is-now-meta/

[37] It is important to note that different opinion leaders in technology have different views on what the "metaverse" would actually look like in reality. For example, see Hoffman, CH. (2021) What Is the Metaverse? Is It Just Virtual Reality, or Something More? *How-to Geek*. Available from: https://www.howtogeek.com/745807/what-is-the-metaverse-is-it-just-virtual-reality-or-something-more/

[38] (2022) *The British Journal of Criminology*, 62(6), 2022, Vol. 62, No. 6.

[39] EU. (2022) Legal issues in the metaverse / Part 1 - Introduction to the metaverse. *CMS Legal*. Available from: https://cms-lawnow.com/en/ealerts/2022/07/legal-issues-in-the-metaverse-part-1-introduction-to-the-metaverse\#:\~:text=What\%20is\%20the\%20metaverse\%3F,both\%2C\%20e.g.\%20through\%20VR\%20glasses.

[40] For example, see Balis, J. (2022) How Brands Can Enter the Metaverse. *Harvard Business Review*. Available from: https://hbr.org/2022/01/how-brands-can-enter-the-metaverse

While the metaverse would bring along unseen opportunities, several privacy experts have already expressed serious concerns about the privacy rights in the metaverse.[41] One author has pointed out: "We can expect companies in metaverse to collect personal information for individual identification, advertisement, and tracking through multiple channels, like wearable devices, microphones, heart and respiratory monitors, and user interactions to the extent that we have never seen before."[42] It is easy to understand that in the metaverse, the extent of personal data processing would be even greater than it is on the social media platform which we are using today. Therefore, data protection and data subject's rights in the metaverse would be more difficult to achieve. The question of how to protect data subjects' rights in the metaverse needs great attention.

As we have discussed previously, the metaverse can mean that there will be a need for new and fundamentally different privacy related legal acts. What about the right to be forgotten? Will it be difficult or even impossible to enforce the right to be forgotten in the metaverse? Here, there are different opinions. First, most privacy experts agree that it could be much more difficult to enforce the right to be forgotten due to the even more rapid pace of sharing personal data between different data processors. This means that upon receiving a request to have personal data erased, it can prove impossible for the controller to delete the data, as it is already being processed by so many other service providers in the metaverse despite the obligation in the Article 17 (2) GDPR as discussed above. It is also important to remember that it could be difficult for supervisory authorities to carry out supervisory proceedings in the metaverse. It can be difficult for the supervisory authority to understand and track how the personal data processing activities have been carried out. Therefore, the enforcement of the right to be forgotten can prove to be a difficult task in the metaverse.

It is important to understand that NFTs, the metaverse and blockchain technology are all concepts related to each other. It has been predicted that NFTs would be used as a currency in the metaverse. It is important to note that in the metaverse, the right to be forgotten cannot always be fully respected, especially in relation to NFTs. This is related to the technical

[41] For example, see the article by Weingarden, G. and Artzt, M. (2022) Metaverse and Privacy. *IAPP*. Available from: https://iapp.org/news/a/metaverse-and-privacy-2/; also Vittorio, A. (2022) Metaverse Technology Opens Up a Wider World of Privacy Concerns. *Bloomberg Law*. Available from: https://news.bloomberglaw.com/privacy-and-data-security/metaverse-technology-opens-up-a-wider-world-of-privacy-concerns

[42] Unknown. (2021) What is the future of your Privacy in METAverse. *Data Privacy Manager*. Available from: https://dataprivacymanager.net/what-is-the-future-of-your-privacy-in-facebook-metaverse/

functioning of NFTs and blockchain technology. Blockchain's distributed ledgers contain data that can't be deleted or changed. This means that when a data subject submits a request to have personal data deleted, this may be impossible.

If the metaverse will be a virtual universe existing in parallel to the real world, companies will not be able to exercise the same control over data processing as they can do it in the real world. If the right to be forgotten cannot be implemented in the metaverse, yet the technological development towards the metaverse is still happening at an ever-greater pace, then perhaps a political decision may be necessary here to review the current concept of the right to be forgotten and its effective exercise.

Some experts have also expressed the opinion that the metaverse can help companies to achieve greater compliance with data protection related legal acts. For example, some authors have expressed the opinion that the metaverse presents an opportunity to be a breakthrough in privacy-compliant digital marketing.[43] Indeed, it is worthwhile to note that companies have been criticized for not being able to adequately apply GDPR rules in the digital age, especially in the context of digital marketing. Companies struggle to meet all the requirements in the GDPR when carrying out digital marketing activities. Complying with all the rules in the GDPR means that digital marketing will be made less visually attractive and user-friendly. For example, users of digital platforms are overburdened with cookie consent notices and privacy policy pop-ups. Privacy notices

[43] Hiken, A. (2021) Why the metaverse could be a breakthrough in privacy-compliant digital marketing. *MarketingDive*. Available from: https://www.marketingdive.com/news/why-metaverse-could-be-breakthrough-privacy-compliant-digital-marketing/610661/. Similarly Garon, J. M. (2022) Legal Implications of a Ubiquitous Metaverse and a Web3 Future. Available from: https://ssrn.com/abstract=4002551; Di Pietro, R. and Cresci, S. (2021) Metaverse: Security and Privacy Issues. In: *Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, Atlanta, 13 - 15 December, Georgia: IEEE, pp. 281-288. Available from: https://ieeexplore.ieee.org/document/9750221; Wang, Y. et al. (2023) A Survey on Metaverse: Fundamentals, Security, and Privacy. *IEEE Communications Surveys & Tutorials* 25(1). Available from: https://ieeexplore.ieee.org/document/9880528; See also overview of privacy concerns in Metaverse Glorin, S. (2023) A Descriptive Study on Metaverse: Cybersecurity Risks, Controls, and Regulatory Framework. *International Journal of Security and Privacy in Pervasive Computing* 15(1). Available from: https://ssrn.com/abstract=4316659; Leenes emphasizing local governance Leenes, R. (2008). Privacy in the Metaverse. In: Fischer-Hübner, S., Duquenoy, P., Zuccato, A., Martucci, L. (eds) *The Future of Identity in the Information Society. Privacy and Identity 2007. IFIP — The International Federation for Information Processing* 262. Available from: https://doi.org/10.1007/978-0-387-79026-8_7; or discussion on privacy measures in Metaverse in Canbay, Y., Utku, A. and Canbay, P. (2022) Privacy Concerns and Measures in Metaverse: A Review. In: Ozbudakh, F. et al. (eds.) *15th International Conference on Information Security and Cryptography (ISCTURKEY)*, Ankara, 19 - 20 October. Turkey: ISC, pp. 80-85, Available from: https://ieeexplore.ieee.org/document/9880528

tend to be long and burdensome for data subjects to read, being full of legal terms. This has led to a situation in which data controllers are producing long privacy notices while data subjects do not bother to read them. This means that many data subjects are not even aware of their rights as data subjects, including the right to be forgotten.

The problem with long and burdensome privacy notices has already been extensively discussed by legal experts.[44] It is important to note that privacy notices have an important meaning for the right to be forgotten. A privacy notice is usually the main source of information for the data subject about its rights. According to Article 13(2)(b) and 14(2)(c) in the GDPR, it is the controller's obligation to notify the data subject about its right to request the deletion of personal data. Therefore, it is important that privacy notices are presented to a data subject in an understandable and clear way, as a privacy notice is, among its other functions, a source of information about one's right to be forgotten. Long and burdensome privacy notices are an obstacle for the effective implementation of the right to be forgotten.

Regarding the problem of long and burdensome privacy notices, some scholars have suggested that the next step is the adoption of very short 'just-in-time' contextual notices. 'Just-in-time' notices – like road signs – are there to help and can be developed in a way that blend into the right context, irrespective of whether they appear on a web page, a smartphone screen or a person's toaster display. Using "just-in-time" notices means that critical information about data processing is communicated to the data subject just before the data processing is about to take place.[45] Although such data-subject-friendly ideas have been expressed long before the idea of the metaverse came into existence, the adoption of such measures has not been very successful. Companies still publish traditional privacy notices on their webpages.

The development of the metaverse can mean that just-in-time privacy notices and other more virtual and data-subject-friendly measures may become more prevalent. This is because the metaverse means that augmented reality shall be an important part of our everyday lives. When augmented reality becomes an everyday part of our lives, controllers will be able to use augmented reality to communicate with data subjects as well. Augmented

[44] For example, see Stokel-Walker, Ch. (2022) Privacy policies are four times as long as they were 25 years ago. *New Scientist*. Available from: https://www.newscientist.com/article/2307117-privacy-policies-are-four-times-as-long-as-they-were-25-years-ago/; Delinger, A. (2019) Most privacy policies are too long and complicated to read. That needs to change. *MIC*. Available from: https://www.mic.com/impact/privacy-policies-are-too-complicated-to-understand-new-analysis-confirms-18002848.

[45] Ustaran, E. (2013) *The Future of Privacy*. London: Cecile Park Publishing, pp. 94-95.

reality enables data controllers to use images, signs and other visual aspects, instead of text, to draw data subjects' attention to changes in the processing of their personal data. These tools can be used to draw data subjects' attention to their rights, including the right to be forgotten. Therefore, there is a chance that with the help of new technology and the tools it provides, data subjects' awareness of their rights will be enhanced and subsequently offer more viable opportunities for the exercise of data subject´s rights including the right to be forgotten.

6. CONCLUSION

The expectations of forgetting in the digital age and advent of right to be forgotten were high, it is far from general regulatory success. The right to be forgotten (or its predecessor in the form of right of erasure), now stipulated in Article 17 of the GDPR, has brought with it several paradoxes. As we have seen from the case-law described in this article, in many cases, the applicants who have applied for the removal of "painful" information about themselves have become even more associated with such information. In such conditions, the right to be forgotten turns not so much into a privacy-protective instrument, but a mean of black PR on the part of both European and national courts, acting in such cases not so much as the guarantors of European justice, but as undesirable 'PR managers' for such applicants.

Aside from the Streisand effect and the Costeja paradox discussed in sections 2 and 3, the right to be forgotten also faces difficulties arising from written law itself. GDPR obliges data controllers to notify other data controllers (such as other companies) about the data erasure request as well. This can turn out to be an impossible task, especially in the digital age and unprecedent pace and speed of information flow. In the future, the right to be forgotten will face even greater challenges. The rapid development of new technologies, such as the metaverse, NFTs, blockchain technology and others will make it even more difficult for data subjects to enforce this right. On the other hand, technological advancements can also help develop innovative tools which lead to greater data protection compliance. For example, augmented reality could enable data controllers to replace long privacy notices with different visual tools which would catch the data subject's interest more efficiently.

In conclusion, the right to be forgotten plays an important role in securing data subject's rights in a world where massive amounts of information and data are being produced and processed all the time. It remains to be seen how national courts, the CJEU, data protection supervisory authorities, data

controllers as well as other key players will be able to implement this right more successfully.[46] Recent developments created some unwanted paradoxes. However, their mitigation is closely tied with important political decisions and adopting regulations in the advent of new technological development.

LIST OF REFERENCES

[1] Alessi, S. (2017) Eternal Sunshine: The Right to Be Forgotten in the European Union after the 2016 General Data Protection Regulation. *Emory International Law Review* 32(1). Available from: https://scholarlycommons.law.emory.edu/cgi/viewcontent.cgi?article=1186&context=eilr

[2] Balis, J. (2022) How Brands Can Enter the Metaverse. *Harvard Business Review*. Available from: https://hbr.org/2022/01/how-brands-can-enter-the-metaverse

[3] Barbara Streisand vs. Kenneth Adelman et. al. Superior Court of California, County of Los Angeles, Case No. SC077257

[4] Bunn, A. (2015) The curious case of the right to be forgotten. *Computer Law & Security Review* 31(3). p. 336 - 350. Available from: https://www.sciencedirect.com/science/article/abs/pii/S0267364915000606

[5] Canbay, Y., Utku, A. and Canbay, P. (2022) Privacy Concerns and Measures in Metaverse: A Review. In: Ozbudakh, F. et al. (eds.) *15th International Conference on Information Security and Cryptography (ISCTURKEY)*, Ankara, 19 - 20 October. Turkey: ISC, pp. 80-85, Available from: https://ieeexplore.ieee.org/document/9880528

[6] Charter of Fundamental Rights of the European Union (2012/C, 326/02). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex\%3A12012P\%2FTXT

[7] Consolidated version of the Treaty on the Functioning of the European Union Protocol (No 3) on the Statute of the Court of Justice of the European Union, 7 June 2016 (C 202/210). Available from: http://data.europa.eu/eli/treaty/tfeu_2016/pro_3/oj

[8] Cook L. (2015) The Right to Be Forgotten: A Step in the Right Direction for Cyberspace Law and Policy. Journal of Law, Technology & Internet 6(1). Available from: https://scholarlycommons.law.case.edu/jolti/vol6/iss1/8

[46] Kocharyan, H., Hamuľák, O. and Vardanyan, L. (2022) "The Right to be Remembered?": The Contemporary Challenges of the "Streisand Effect" in the European Judicial Reality. *International and Comparative Law Review* 22(2). p. 105-120. https://doi.org/10.2478/iclr-2022-0017

[9] Cunningham, M. (2017) Privacy Law That Does Not Protect Privacy, Forgetting the Right to be Forgotten. *Buffalo Law Review* 65(3). Available from: https://digitalcommons.law.buffalo.edu/cgi/viewcontent.cgi?article=4656\&context=buffalolawreview

[10] De Baets, A. (2016) A historian's view on the right to be forgotten. *International Review of Law, Computers & Technology* 30(1-2). Available from: https://www.tandfonline.com/doi/full/10.1080/13600869.2015.1125155

[11] Delinger, A. (2019) Most privacy policies are too long and complicated to read. That needs to change. *MIC*. Available from: https://www.mic.com/impact/privacy-policies-are-too-complicated-to-understand-new-analysis-confirms-18002848

[12] Di Pietro, R. and Cresci, S. (2021) Metaverse: Security and Privacy Issues. In: *Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, Atlanta, 13 - 15 December, Georgia: IEEE, pp. 281-288. Available from: https://ieeexplore.ieee.org/document/9750221

[13] Erikson, P.W. (2014) The EU's right to be forgotten. Available from: https://www.linkedin.com/pulse/20140710033506-2822374-the-eu-s-right-to-be-forgotten/

[14] EU. (2022) Legal issues in the metaverse / Part 1 - Introduction to the metaverse. *CMS Legal.* Available from: https://cms-lawnow.com/en/ealerts/2022/07/legal-issues-in-the-metaverse-part-1-introduction-to-the-metaverse\#:\~:text=What\%20is\%20the\%20metaverse\%3F,both\%2C\%20e.g.\%20through\%20VR\%20glasses.

[15] Farrall, S. et al. (eds.) (2022) *The British Journal of Criminology*, 62(6), 2022, Vol. 62, No. 6.

[16] Garon, J. M. (2022) Legal Implications of a Ubiquitous Metaverse and a Web3 Future. Available from: https://ssrn.com/abstract=4002551

[17] Giampa, G. (2016) Americans Have a Right to Be Forgotten. *Law School Student Scholarship* 740. Available from: https://scholarship.shu.edu/student_scholarship/740/

[18] Glorin, S. (2023) A Descriptive Study on Metaverse: Cybersecurity Risks, Controls, and Regulatory Framework. *International Journal of Security and Privacy in Pervasive Computing* 15(1). Available from: https://ssrn.com/abstract=4316659

[19] Google Transparency Report on delisting requests.Available from: https://transparencyreport.google.com/eu-privacy/overview.

[20] Hiken, A. (2021) Why the metaverse could be a breakthrough in privacy-compliant digital marketing. *MarketingDive*. Available from: https://www.marketingdive.com/news/why-metaverse-could-be-breakthrough-privacy-compliant-digital-marketing/610661/

[21] Hoffman, CH. (2021) What Is the Metaverse? Is It Just Virtual Reality, or Something More? *How-to Geek*. Available from: https://www.howtogeek.com/745807/what-is-the-metaverse-is-it-just-virtual-reality-or-something-more/

[22] Holland, J.A. (2019) Contemporary Practical Alternatives to a "Right To Be Forgotten" in the United States. *Latin American Law Review* 2. Available from: https://revistas.uniandes.edu.co/doi/full/10.29263/lar02.2019.02.

[23] Hurbain v. Belgium. (2021) ECtHR, No. 57292/16.

[24] Judgement of 13 May 2014, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, C-131/12, EU:C:2014:317,

[25] Judgement of 24 September 2019, GC and Others v. CINIL, C-136/17, EU:C:2019:773.

[26] Judgement of 3 October 2019, Eva Glawischnig-Piesczek v Facebook Ireland Limited, C-18/18, EU:C:2019:821.

[27] Keller, D. (2019) The CJEU's new filtering case, the terrorist content regulation, and the future of filtering mandates in the EU. *The Center for Internet and Society.* Available from: http://cyberlaw.stanford.edu/blog/2019/12/cjeu\%E2\%80\%99\\s-new-filtering-case-terrorist-content-regulation-and-future-filtering-mandates-eu

[28] Kocharyan, H., Hamuľák, O. and Vardanyan, L. (2022) "The Right to be Remembered?": The Contemporary Challenges of the "Streisand Effect" in the European Judicial Reality. *International and Comparative Law Review* 22(2). p. 105-120. https://doi.org/10.2478/iclr-2022-0017

[29] Kulk S. and Borgesius, Z. F. (2017) Privacy, Freedom of Expression, and the Right to Be Forgotten in Europe. In: Polonetsky, J., Tene, O. and Selinger E. (eds.) *Cambridge Handbook of Consumer Privacy*. Cambridge: Cambridge University Press. Available from: https://dare.uva.nl/search?identifier=f7d0f415-3404-426a-8833-12861fee7112

[30] Leenes, R. (2008). Privacy in the Metaverse. In: Fischer-Hübner, S., Duquenoy, P., Zuccato, A., Martucci, L. (eds) *The Future of Identity in the Information Society. Privacy and Identity 2007. IFIP — The International Federation for Information*

Processing 262. Available from: https://doi.org/10.1007/978-0-387-79026-8_7.

[31] Masnick, M. (2011) Forget The Streisand Effect, I Think We've Seen The Dawning Of The Giggs Effect. *techdirt*. Available from: https://www.techdirt.com/articles/20110520/16102414365/forget-streisand-effect-i-think-weve-seen-dawning-giggs-effect.shtml.

[32] Meta. (2021) *Introducing Meta: A Social Technology Company.* [press release] 28 October. Available from: https://about.fb.com/news/2021/10/facebook-company-is-now-meta/.

[33] Mosley v. News Group Newspapers [2008] EWHC 1777 (QB).

[34] Oghia, M. J. (2018) Information Not Found: The "Right to Be Forgotten" as an Emerging Threat to Media Freedom in the Digital Age. *CIMA Digital Report*. Available from: https://www.cima.ned.org/publication/right-to-be-forgotten-threat-press-freedom-digital-age/.

[35] Opinion of AG Szpunar in Judgement of 3 October 2019, Eva Glawischnig-Piesczek v Facebook Ireland Limited, C-18/18, EU:C:2019:821.

[36] Schechner, S. (2014) Google Defends 'Right to Be Forgotten' Response. *Wall Street Journal*. Available from: https://www.wsj.com/articles/google-defends-\\right-to-be-forgotten-response-1416414403.

[37] Smith, M. (2019) ANALYSIS: Global Censorship, but Not Erasure, Spurs Streisand Effect. *Bloomberg Law*. Available from: https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-global-censorship-but-not-erasure-spurs-streisand-effect.

[38] Solon, O. (2014) EU 'Right To Be Forgotten' Ruling Paves Way for Censorship. *WIRED* Available at: http://www.wired.co.uk/news/archive/2014-05/13/right-to-be-forgotten-blog.

[39] Stokel-Walker, Ch. (2022) Privacy policies are four times as long as they were 25 years ago. *New Scientist*. Available from: https://www.newscientist.com/article/2307117-privacy-policies-are-four-times-as-long-as-they-were-25-years-ago/.

[40] Unknown. (2021) What is the future of your Privacy in METAverse. *Data Privacy Manager*. Available from: https://dataprivacymanager.net/what-is-the-future-of-your-privacy-in-facebook-metaverse/.

[41] Ustaran, E. (2013) *The Future of Privacy*. London: Cecile Park Publishing.

[42] Vittorio, A. (2022) Metaverse Technology Opens Up a Wider World of Privacy Concerns. *Bloomberg Law.* Available from: https://news.bloomberglaw.

com/privacy-and-data-security/metaverse-technology-opens-up-a-wider-world-of-privacy-concerns

[43] W.W. v. Germany. (2018) ECtHR, No. 60798/10 and 65599/10.

[44] Wang, Y. et al. (2023) A Survey on Metaverse: Fundamentals, Security, and Privacy. *IEEE Communications Surveys & Tutorials* 25(1). Available from: https://ieeexplore.ieee.org/document/9880528.

[45] Weingarden, G. and Artzt, M. (2022) Metaverse and Privacy. *IAPP*. Available from: https://iapp.org/news/a/metaverse-and-privacy-2/.

[46] Wohlsen, M. (2014) For Google, the 'Right to Be Forgotten' Is an Unforgettable Fiasco. *WIRED* Available from: https://www.wired.com/2014/07/google-right\\-to-be-forgotten-censorship-is-an-unforgettable-fiasco/.

[47] Xue M., Magno G. et al. (2016) The Right to be Forgotten in the Media: A Data-Driven Study. *Proceedings on Privacy Enhancing Technologies 2016* (4). p. 1–14. Available from: http://www.nyu.engineering/sites/default/files/migrated/pdfs/RTBF_Data_Study.pdf

[48] Zhang, M. (2013) Beyonce Publicist's Takedown Request Causes Unflattering Photos to Go Viral. *PetaPixel*. Available from: https://petapixel.com/2013/02/08/beyonce-publicists-takedown-request-causes-unflattering-photos-to-go-viral/

DOI 10.5817/MUJLT2023-1-4

STRENGTHENING OF EU REGULATORY INTERVENTION AGAINST DATA EXPLOITATIONS BY ONLINE PLATFORMS WITH A ZERO-PRICE BUSINESS MODEL

by

ANDRÁS TÓTH *

The article aims to analyse the relationship between data protection and online platforms' zero-price business model. This business model functions in a way that online platforms provide their services "free of charge", but in exchange for personal data. This business model may not only come with competition problems, but also is detrimental to data protection principles, such as the principle of data minimisation. Users are unaware of the value of the personal data they provide, partly due to the false illusion of the service being free of charge. This market failure could be remedied by regulations that would ensure that users are able to use online services that are currently zero-price without providing personal data.

KEY WORDS

Attention Market, Data Exploitation, Zero-Price Business Model, Online Platforms

1. INTRODUCTION

The zero-price business model is a feature of online attention market platforms (e.g., Facebook, Google). These platforms collect data and aim to gain human attention[1] in order to provide an interface for advertisers in the online space, regardless of what service – that is offered free of charge (e.g., social media, email, free video streaming, online search engine service) – is used to gather the attention of these people. The platforms also sell data that can help third parties understand the habits of users. Platforms that operate using this business model provide their services for users in exchange for their personal data.

* toth.andras@kre.hu, Associate Professor, Faculty of Law, Károli Gáspár University of the Reformed Church, Hungary

1 Newman, J. M. (2019) Regulating Attention Markets. *University of Miami Legal Studies Research Paper*. Available from: `https://ssrn.com/abstract=3423487` [Accessed 15 June 2021].

According to UN data, this market is highly concentrated globally, with US and Chinese undertakings accounting for 90% of the market share of the largest online platforms, of which the market share of American undertakings is 70%, while the ratio of European undertakings does not even reach 4%.[2]

The article aims to present and analyse how online zero-price business models violate data protection principles, in particular the principle of data minimisation, and seeks to provide a possible remedy that could enhance users' choice. In the article, after the introductory remarks in which I present the general features of online attention markets, I delve into the characteristics of the zero-price business model in Section 2. The first two sections are necessary to frame my analysis in order that I could find, on one hand, the connecting points between data protection and the zero-price business model, and, on the other hand, the possible violation of data protection rules by this model. After that, in Section 4, I propose the solution that could remedy the situation. In the end, I conclude. Although the main analysis concentrates on EU law, certain developments and events related to the issue are also mentioned from outside the European Union, such as the United States.

2. THE ZERO-PRICE BUSINESS MODEL

Online attention markets are platform-based. Platforms provide services to different directions and function as intermediaries between supply and demand. This creates an opportunity for them to collect remuneration from several directions. Platforms can be two- or multi-sided, depending on the number of groups between which they create interaction. What they always have in common is that they are built on exploiting network effects and economies of scale.[3] Demand from all sides of the platform is connected by a network effect, higher demand also attracts additional demand and supply. A network effect can create market power, as the more people that use the platform, the more attractive it will be to others as well. This encourages further investment and thus users to join, as a result of which a so-called spill over effect can emerge, which after reaching a given tipping point can make the platform dominant.[4] When the entire market tips in favour of a single undertaking due to a combination of economies of scale and network effect the competition no longer exists on the market

[2] United Nations (2019) Digital Economy Report 2019, p. 23

[3] Capobianco, A. and Nyeso, A. (2018) Challenges for Competition Law Enforcement and Policy in the Digital Economy. *Journal of European Competition Law & Practice*, 9 (1), p. 20.

[4] Capobianco, A. and Nyeso, A. (2018) Challenges for Competition Law Enforcement and Policy in the Digital Economy. *Journal of European Competition Law & Practice*, 9 (1), p. 22.

but for the market.[5] In this case, the market power can persist for a long time, as shown by the example of tech giants. This is remarkable because these undertakings acquired market power thanks to their innovations that constitute intellectual property.[6] In this regard, we should mention the Schumpeterian competition theory, which states that an investment that creates intellectual property will be rewarded by the creation of a monopoly. The monopoly then ensures that there is a return on the investment into the creation of the intellectual property.[7] According to the Schumpeterian dynamic competition theory, the new entrants to these innovative markets quickly dethrone the former winners. However, it is exactly these tech giants that serve as proof that the Schumpeterian competition theory seems to be truncated on markets characterised by innovation, as the market power of these tech giants has been unchallenged for decades.[8] Therefore, it is important that the regulation of such markets allows for conditions that enable the entry of innovative market players. This is why the IMF emphasises that ensuring interoperability and data portability are important tools for fostering competition in digital markets,[9] and it is no accident that these principles are also important building blocks that have been included in the DMA.[10]

Two-sided transaction platforms and non-transaction platforms can be differentiated.[11] For example, a media service provider is a two-sided non-transaction platform where there is interaction between the two sides, but no detectable transaction occurs; therefore, the two sides of the platform are not paying for the same service. For example, on the media market, a television channel competes against printed media products for advertisers but does not compete for the same subscribers. In this case, the users pay the

---

5 Stigler Center for the Study of the Economy and the State, 'Stigler Committee on Digital Platforms Final Report' (2019) www.chicagobooth.edu/research/stigler/news-and-media/committee-on-digital-platforms-final-report (accessed 15 June 2021).

6 Waked, D.I. (2020) Antitrust as Public Interest Law: Redistribution, Equity and Social Justice. *The Antitrust Bulletin*, 65 (1), p. 98.

7 Shelanski, H.A. and Sidak, J.G. (2001) Antitrust Divestiture in Network Industries. *The University of Chicago Law Review*, 68 (1), p. 5.

8 Gal, M. and Petit, N. (2021) Radical Restorative Remedies for Digital Markets. *Berkeley Technology Law Journal*, 37 (1), pp. 617-674.

9 Georgieva, K., Díez, F.J., Duval, R. and Schwarz, D. (2021) Rising Market Power, A Threat to the Recovery? *IMF Blog* (15 March 2021) blogs.imf.org/2021/03/15/rising-market-power-a-threat-to-the-recovery accessed 15 June 2021.

10 Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) OJ L 265, 12.10.2022, pp. 1–66.

11 Capobianco, A. and Nyeso, A. (2018) Challenges for Competition Law Enforcement and Policy in the Digital Economy. *Journal of European Competition Law & Practice*, 9 (1), p. 23.

platform for the valuable content, while advertisers pay for the opportunity to attract the attention of the users. In the case of two-sided transaction markets (such as card payments, online marketplaces, or the platforms of the sharing-based economy, e.g., Airbnb, Uber), there is a detectable transaction between the two sides since it is the same product/service that is present on both markets. Here, only one transaction is carried out through the platform; therefore, in theory a fee can be charged for the transaction performed via the platform on a single occasion and from only one side of the platform (except if the platform explicitly provides a service to the other side as well, such as home delivery).

The online platforms of data-driven or attention markets (e.g. Google, Facebook) are non-transaction two-sided markets, where the platform provides users with content and experiences and advertisers with a space where they can advertise to the users gathered by the zero-price service. Since both sides are using a different service, the platform is able to demand remunerations from both sides. On the online attention markets, the user pays for the service used, which can be social media, video sharing, voice /video calls, or internet searches, with their data.[12] This is how personal data becomes the new raw material of the digital economy,[13] the new oil.[14] It is an asset in the same way as copyrights, business secrets, and patents – this is often reflected by the books of undertakings as well.[15] Therefore, one cannot say that users pay with their personal data for the personalised advertisements.[16] With the data, the users pay for the online services (e.g. social media, email, free video streaming, online search engine); the advertisers are the ones who pay for the personalised advertisements. This paper seeks to draw attention to the fact that there are groups of users who value the protection of their personal data more than personalised advertisements, but they do not have a choice when it comes to expressing this preference.

On attention markets, data are required in order to grab more attention through more targeted advertisements, as individuals pay the most attention

[12] Joint Report by Autorité de la Concurrence and Bundeskartellamt, *Competition Law and Data* (accessed 10 May 2016), p. 3.

[13] DPS: Opinion on coherent enforcement of fundamental right sin the age of big data, Opinion 8/2016 (23 September 2016), p. 6.

[14] See: `https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data` (10 July 2021).

[15] European Data Protection Supervisor (2014) *Preliminary Opinion of the European Data Protection Supervision: Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy* (8 March 2014).

[16] We disagree with the opinion of the OECD, see: OECD, 'Quality considerations in digital zero-price markets Background note by the Secretariat' (28 November 2018) DAF/COMP(2018), p. 14.

to information that is highly customised.[17] According to a British study, the income of those offering advertising space to untargeted advertisements is 70% lower than those implementing targeted advertising.[18] The more attention is attracted, the more data are collected and the higher the personalisation of advertisements will be, which increases the advertising revenue that can be invested into even more effective attention-grabbing techniques and content (e.g. entertainment). This starts a cycle at the end of which the market can tip in favour of such a platform, which can thus become dominant.[19]

Getting attention is the key to being able to direct it to other people, products, or topics.[20] On attention markets, advertisers pay the providers of advertising space to ensure that the attention of buyers, which qualifies as a limited resource (since a day only consists of 24 hours),[21] is directed at them. Since attention is a limited resource, there is fierce competition for attracting this attention, sometimes even using unfair practices (so-called attention theft[22]).

Therefore, it is in the interest of online platforms within an attention market to grab as much of the users' attention as possible. This enables the platform to acquire more personal data, based on which it can provide advertisers and users with more numerous and more valuable services. Nevertheless, the personal data acquired and later used by platforms to gain more attention from individuals can also be (mis)used to influence the thinking of users, as was clearly shown by the 2016 US presidential elections and the Cambridge Analytica scandal.[23] These events show precisely the costs of data transfers that users are not aware of due to the breach of the data protection principle described in Section 3.

---

17 Newman, J. M. (2019) Regulating Attention Markets. *University of Miami Legal Studies Research Paper*. Available from: `https://ssrn.com/abstract=3423487` [Accessed 15 June 2021].

18 Competition and Markets Authority (2020) Online Platforms and Digital Advertising, p. 42.

19 OECD (2017) Algorithms and Collusion – Note from the European Union, DAF/COMP/WD(2017), p. 12.

20 Hendricks, V.F. and Vestergaard, M. (2019) *Reality Lost*. Cham: Springer, p. 6.

21 Hendricks, V.F. and Vestergaard, M. (2019) *Reality Lost*. Cham: Springer, p. 5.

22 Wu, T. (2019) Blind Spot: The Attention Economy and the Law. *Antitrust Law Journal*, 82 (3), p. 771.

23 Hendricks, V.F. and Vestergaard, M. (2019) *Reality Lost*. Cham: Springer, p. 15.

3. DETRIMENTAL EFFECTS OF ZERO-PRICE BUSINESS MODEL ON PRINCIPLE OF DATA MINIMISATION

The zero-price business model is used on a non-transaction two-sided market, where the advertisers pay for access to users, while users pay for the services (or entertainment) of the platform. Although the users of the two sides of the platform pay for different services, there is still a correlation between the pricing of the two sides. The success of the platform depends on how many users it has, which is determined by the quality of the content it offers and the price of accessing this content. The advertising income can be used to increase the quality of the service or reduce the access fees, which in this case means the extent and intensity of personal data transfer. The quality of the service also necessitates that the ratio between content and advertisements is balanced or proportional, as excessive advertising spoils the user experience. However, from the point of view of the study, it is not attention exploitation, but data exploitation that is relevant. Data exploitation is contrary to the principle of data minimisation pursuant to Article 5 (1) c) of the GDPR. Together, these two (attention and data exploitation) ultimately increase the vulnerability of users. While the exploitation of attention can be fought with media law tools, in this study, however, I would like to present a possible regulatory solution against data exploitation that is explained by the following three reasons.

First, information asymmetry exists between the user and the platform. Information asymmetry can be traced back to two additional reasons. On the one hand, the information asymmetry created by the false illusion of a free-of-charge service (the so-called bounded rationality)[24] and the confidentiality of the data exchange transactions, due to which the users are not aware of the true value of the personal data they provide. While opinion polls show[25] that users are concerned about their personal data, they do not really care about protecting their data (the privacy paradox).[26] In part, this can be traced back to them not being able to see the weight of their data in

[24] Vásquez Duque, O. and Hoffmann, J. (2021) Can data exploitation be properly addressed by competition law? A note of caution. Concurrences, February 2021 https://www.concurrences.com/en/review/issues/no-1-2021/law-economics/can-data-exploitation-be-properly-addressed-by-competition-law-a-note-of-en (Accessed: 10 July 2021).

[25] Directorate-General for Communication: Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union https://data.europa.eu/data/datasets/s864_74_3_ebs359?locale=en (Accessed: 5 August 2021).

[26] Vásquez Duque, O. and Hoffmann, J. (2021) Can data exploitation be properly addressed by competition law? A note of caution. Concurrences, February 2021 https://www.concurrences.com/en/review/issues/no-1-2021/law-economics/can-data-exploitation-be-properly-addressed-by-competition-law-a-note-of-en (Accessed: 10 July 2021).

the transaction. It is no coincidence that online attention merchants protect the data exchange agreements even with confidentiality clauses.[27] In many cases, the undertakings share the data with third parties without the explicit knowledge of the users.[28] The decision of the German competition authority against Facebook also highlights that consumers are unaware that they are being exploited by Facebook and that their data are being acquired by the undertaking even when they are using the internet for purposes other than browsing Facebook.[29] As a result of the illusion of the service being free and being presented as free, consumers do not fully understand the fact that they are actually paying for the service they consider free. The service being free gives consumers the impression that the undertakings providing such services do not need to generate any income to cover the costs of their 'free' services.[30] Anderson claims that consumers absolutely believe that the online space has changed the fundamental principles of how undertakings operate.[31] However, the truth is that behind online undertakings, there are people, facilities and servers, all of which require the expenditure of significant funds.[32] On the other hand, the cause of information asymmetry is due to privacy policies that are often worded in such a lengthy and complicated manner that most consumers have difficulty to understand them or simply do not wish to spend time reading them.[33] Certain studies have shown that it would take the average user more than 200 hours annually to carefully read these documents in the case of every single online transaction

[27] Hoofnagle, C.J. and Whittington, J. (2014) Free: Accounting for the Costs of the Internet's Most Popular Price. *UCLA Law Review*, 61 (3), p. 634.

[28] Tene, O. and Polonetsky, J. (2013) Big Data for All: Privacy and User Control in the Age of Analytics. *Northwestern Journal of Technology and Intellectual Property*, 11 (5), p. 261; Elvy, S-A. (2017) Paying for privacy and the personal data economy. *Columbia Law Review*, 117 (6), pp. 1369–1460.

[29] See: Bundeskartellamt prohibits Facebook from combining user data from different sources (7 February 2019) `www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html` (Accessed: 9 August 2021).

[30] Hoofnagle, C.J. and Whittington, J. (2014) Free: Accounting for the Costs of the Internet's Most Popular Price. *UCLA Law Review*, 61 (3), p. 620.

[31] Hoofnagle, C.J. and Whittington, J. (2014) Free: Accounting for the Costs of the Internet's Most Popular Price. *UCLA Law Review*, 61 (3), p. 620.

[32] Hoofnagle, C.J. and Whittington, J. (2014) Free: Accounting for the Costs of the Internet's Most Popular Price. *UCLA Law Review*, 61 (3), p. 621.

[33] OECD (2016) Big Data: Bringing Competition Policy to the Digital Era, DAF/COMP/M(2016)14, Section 88; Botta, M. and Wiedemann, K. (2019) Exploitative Conducts in Digital Markets: Time for a Discussion after the Facebook Decision. *Journal of European Competition Law & Practice*, 10 (8), pp. 465–478.

they enter.[34] Only 18% of European users reported that they actually read privacy policies.[35]

Second, to gain data, attention merchants often reach for unfair tools. Examples include the so-called 'dark pattern', an example of which is when consumers are tricked into consenting to the provision of their personal data through the use of a graphical solution that makes it appear as if this is their only available option; for example, they can only choose between OK and Learn More and the OK option is even graphically highlighted. This solution was used, for example, by Facebook to obtain the telephone numbers of users, which further assisted the undertaking in mapping out the social connections of users.[36] In the EU, the DSA creates opportunities to act against such dishonest tools.[37] There are situations when creating the illusion that the service is free can be caught in the act as an unfair commercial practice, as shown by the Hungarian decision adopted against Facebook, where Facebook was fined for explicitly advertising its social media as free.[38]

Thirdly, on online attention markets, data exploitation already exists independently of competition distortion; however, it is further intensified by the platform becoming unavoidable due to network effects and economies of scale. As a result of the 'take it or leave it' effect[39] arising from this, even users that are more conscious of data protection do not have a choice but to participate in the data exploitation or opt out of the service. Probably the already mentioned privacy paradox could also be traced back to this since

---

[34] OECD (2016) Big Data: Bringing Competition Policy to the Digital Era, DAF/COMP/M(2016)14.

[35] In the opinion of two-thirds (67%) of respondents, they are too long, while nearly four out of ten respondents (38%) found them to be unclear or hard to understand. It would take on average 244 hours a year for each internet user to read through the privacy policies of all the websites they view, which is more than 50% of the time that the average user spends on the internet. See: European Data Protection Supervisor (2014) *Preliminary Opinion of the European Data Protection Supervision: Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy* (8 March 2014), p. 34.

[36] Warner, M.R. (2018) Potential Policy Proposals for Regulation of Social Media and Technology Firms, White Paper Draft, 20 August 2018, p. 17.

[37] Adopted text of Regulation on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC; PE-CONS No/YY - 2020/0361(COD), Art. 25. para. (1) Available at: `https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/IMCO/DV/2022/06-15/DSA_2020_0361COD_EN.pdf`.

[38] See: Hungarian Competition Authority (2019) GVH imposed a fine of EUR 3.6 M on Facebook. Available at: `https://www.gvh.hu/en/press_room/press_releases/press_releases_2019/gvh-imposed-a-fine-of-eur-3.6-m-on-facebook` (Accessed: 26 July 2021).

[39] van Lieshout, M. (2015) The Value of Personal Data. In: Jan Camenisch, Simone Fischer-Hübner and Marit Hanses (eds.) *Privacy and Identity Management for the Future Internet in the Age of Globalisation*. Cham: Springer, p. 34; Lypalo, D. (2021) Can Competition Protect Privacy? An Analysis Based on the German Facebook Case. *World Competition*, 44 (2), p. 169.

even though most users are not at all satisfied with this business model that allows them to use 'free' services in the online space, they have no choice but to accept the situation. The majority (it is important that not everyone) of European users object to the fact that they are only able to access 'free' services in exchange for personal data.[40] The 'take it or leave it' effect means that users who are concerned about the fate of their personal data have no choice but to accept the terms of the attention merchants if they want to benefit from the services they offer, otherwise they will be left out.

To sum, users may 'pay' with their data much more on online attention markets than what they receive. This is due to information asymmetries, deceptive unfair practices, and because there are no market barriers to the disproportionate exploitation of data by online platforms as a result of a lack of competition. It is also true that even if competition existed, due to the illusion of the service being free and the confidentiality of the data trade, the platform would still be able to engage in data exploitation without consumers being aware of it. In the EU, the already-mentioned Directive on the prohibition of unfair commercial practices creates opportunities to act against these unfair tools. However, information asymmetry is a market failure that must be remedied by special regulations. A solution to this would be if users could decide if they wanted to pay for the services of online attention merchants with personal data or with cash.

Hoofnagle and Whittington also believe that if undertakings began asking for money in exchange for the services currently offered for free, those worried about privacy could enjoy these services without advertisements or tracking.[41] Botta and Wiedemann also arrived at the conclusion that users should be able to decide whether they wish to use the services of online attention merchants in exchange for personalised advertisements or a monthly fee.[42] The study of the British Competition Authority[43] also suggests that online platforms should operate using a more diverse business model depending on the data protection settings of users. Creating this option seems necessary in light of the right to informational self-determination.

---

[40] Directorate-General for Communication: Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union `https://data.europa.eu/data/datasets/s864_74_3_ebs359?locale=en` (Accessed: 5 August 2021).

[41] Hoofnagle, C.J. and Whittington, J. (2014) Free: Accounting for the Costs of the Internet's Most Popular Price. *UCLA Law Review,* 61 (3), p. 662.

[42] Botta, M. and Wiedemann, K. (2019) Exploitative Conducts in Digital Markets: Time for a Discussion after the Facebook Decision. *Journal of European Competition Law & Practice*, 10 (8), p. 466.

[43] Competition and Markets Authority (2020) Online Platforms and Digital Advertising, pp. 386–387.

4. STRENGTHENING OF REGULATORY INTERVENTION AGAINST DATA EXPLOITATION

Since data exploitation happens independently of the distortion of competition, the enforcement of competition law would not ensure an overall solution, as it would only allow action against undertakings with dominant market positions. Of course, the German Facebook decision[44] highlighted that competition law can be applicable to data exploitation; however, these proceedings are initiated against single undertakings and took a lot of time. Therefore, competition law cannot provide a quick and comprehensive industry-wide solution, as it is stated by the DMA.[45] The DMA further strengthens the implementation of the GDPR in two ways. First, the DMA narrows the data processing rights of gatekeepers, because it excludes the application of two legal bases stipulated in Article 6 b)[46] and f)[47] of the GDPR in a certain scope, and limits it to the consent-based processing. This scope of data processing is delineated by Article 5(2) of the DMA.[48] Second, the DMA delegates the enforcement of this narrowed data processing legal basis to the European Commission instead of the data protection authority of the place of establishment. The DMA raises the costs of end user profiling but does not prohibit the core of zero price business models and the reason of the data exploitation.[49] The DSA prohibits online platforms to present advertisements based on profiling using personal data of the recipient of the service when they are aware with reasonable certainty that the recipient of the service is a minor.[50] Interestingly, the Data Act goes further in case of non-personal data. This means that the designated gatekeepers under the DMA cannot

[44] See: Bundeskartellamt prohibits Facebook from combining user data from different sources (7 February 2019) www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html (Accessed: 9 August 2021).

[45] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) OJ L 265, 12.10.2022, p. 1–66, Rec. 5.

[46] Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

[47] Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party.

[48] E.g. combining end user personal data collected from a core platform service with data collected from other services; cross-using personal data from a core platform service in other services provided separately by the gatekeeper.

[49] Belloso, N.M. and Petit, N. (2023) The EU Digital Markets Act (DMA): A Competition Hand in a Regulatory Glove https://ssrn.com/abstract=4411743, p. 19.

[50] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) OJ L 277, 27.10.2022, p. 1–102., Art. 28(2).

request or be granted access to users' data generated by the use of a product or related service or by a virtual assistant.[51]

Hoofnagle and Whittington also believe that the current regulatory framework essentially turns a blind eye to the commercial business model based on personal data and nothing prevents these undertakings from acquiring valuable data from users while disregarding the right to data protection.[52] Therefore, Hoofnagle and Whittington argue for the transformation of the entire business model built on this.[53] Friedman arrives at the same conclusion due to the false illusion of free services and he would thus ban the entire zero price business model.[54] Evans believes that consumers know that in the data-driven economy they have to provide personal data in exchange for experiences, and this works the same way as a subscription in the case of an offline newspaper.[55] Therefore, Evans considers the provision of personal data a type of consideration for accessing the experiences. In my opinion, the problem is that data protection principles (i.e. data minimisation) are not fully prevailed in relation to the provision of personal data. Therefore, it is reasonable to create regulations that require zero price online platforms to provide an option to users to use the service they currently use in exchange for personal data for monetary payments instead. In such cases, the online platform would not be allowed to request any personal data, analogous to the case of Article 6 (2) of the Directive on privacy and electronic communications,[56] beyond what is required for the management of the subscription and the billing of the service.

The question arises as to whether the service offered to users who refuse to provide personal data can remain free and be delivered without monetary payment obligations. There are strong indicators that this is true since the services of online attention merchants were originally provided for free[57]

---

[51] Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), COM/2022/68 final, Rec. 36.

[52] Hoofnagle, C.J. and Whittington, J. (2014) Free: Accounting for the Costs of the Internet's Most Popular Price. *UCLA Law Review*, 61 (3), p. 609.

[53] Hoofnagle, C.J. and Whittington, J. (2014) Free: Accounting for the Costs of the Internet's Most Popular Price. *UCLA Law Review*, 61 (3), p. 610.

[54] Friedman, D.A. (2008) Free Offers: A New Look. *New Mexico Law Review*, 38 (1), pp. 68-69.

[55] Evans, D.S. (2020) The Economics of Attention Markets. Available at: `https://ssrn.com/abstract=3044858` (Accessed: 26 July 2021).

[56] European Parliament and Council Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L 201 [2002] 37–47.

[57] Furthermore, Facebook displayed fewer advertisements at launch than MySpace, which was the market leader at the time, and only increased the amount of advertisements to the current level, which is considered by some to be an exploitation of the undertaking's monopoly, after the latter player disappeared from the market. See: Wu, T. (2019) Blind Spot: The Attention Economy and the Law. *Antitrust Law Journal*, 82 (3), pp. 790–791.

and gathered a huge mass of users. They only increased the proportion of advertisements after they had become dominant.[58] Taking this into consideration, the exercise of data protection rights should be free in the sense that users should be able to continue accessing the services without fee payments even if they refuse to share their data. This solution is favourable from the point of view that the EU Data Protection Commissioner believes that the exercise of data protection rights cannot be an alternative to monetary payments.[59]

However, if general advertising would not be enough to provide the service without fee payments, the question is whether it is possible to introduce monetary payments in addition to paying with data. In this case, payment with data would become an alternative to monetary payments, which is contrary to the spirit of data protection according to the EU Data Protection Commissioner since the protection of personal data is a fundamental right and therefore cannot be considered a commodity.[60] However, payment with data is a practice that is already present but concealed and therefore acts as a 'hotbed' for data exploitation. Furthermore, Directive (EU) 2019/770 recognises the business model of paying with data on a regulatory level with respect to certain aspects of contracts concerning digital content and digital services.[61] This Directive provides guarantees for contracts within the framework of which a merchant provides digital content or digital services to consumers or assumes an obligation to do so, while the consumer provides personal data or assumes an obligation to do so.[62] Although Directive (EU) 2019/770 does not apply to situations where consumers are forced to watch advertisements without having concluded a contract with the merchant just so they can access the digital content or digital service, the Member States can still freely decide to extend the scope of this Directive to such situations which do not originally fall within its scope or introduce other regulations for such cases.[63] Pursuant to Article 8 (1) b) of the Directive, the digital services have to comply with the expectations of the

[58] Wu, T. (2019) Blind Spot: The Attention Economy and the Law. *Antitrust Law Journal*, 82 (3), pp. 790–791.

[59] European Data Protection Supervisor (2017) Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content of the European (14 March 2017).

[60] European Data Protection Supervisor (2017) Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content of the European (14 March 2017).

[61] European Parliament and Council Directive 2019/770 of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, OJ L 136/1.

[62] European Parliament and Council Directive 2019/770 of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, OJ L 136/5.

[63] Ibid.

consumers based on the public claims of the merchant. Therefore, claims about a free service mean that not even personal data can be collected in exchange for that service.[64]

Of course, there are users who consider personalised advertisements to be a positive feature.[65] Privacy is heterogenous which means that there are a range of privacy preferences.[66] However, the scope and intensity of the provision of data should be regulated in the case of those paying with data as well. On the one hand, since the market power of the attention merchants means that there are no competition-based barriers to the data exploitation (consumers cannot switch to other service providers because of this: the 'take it or leave it' effect), on the other hand, this exploitation is facilitated by consumers not being aware of the true value of the personal data they provide (information asymmetry). The latter situation would certainly be improved if consumers who pay with data were made aware of the monetary value of the data they provide. The scope and intensity of the provision of personal data could perhaps be regulated with transparency rules, such as the proposal concerning two-step consent by Botta and Wiedemann, which would mean that users would receive an email with the data protection settings they have selected and they would have to accept them again or the selected settings would only be in effect for a fixed period of time and the consent should be renewed after the expiry of this period.[67] It is important that users who use online services in return for personal data transfer also have a clear idea of the scope and extent of the data transfer they are required to provide in order to make an informed consent decision.

The above proposal (the creation of the option to pay with data) would resolve the privacy paradox as well. As discussed above, the privacy paradox can partially be traced back to the fact that although users are concerned about their data, they do not take steps to protect them. This may be improved if monetary payments appearing as alternatives to paying with

---

[64] In this context, see the decision of the Hungarian Competition Authority against Facebook due to misleading claims about a free service (6 December 2019). Available at: www.gvh.hu/sajtoszoba/sajtokozlemenyek/2019_es_sajtokozlemenyek/12-milliard-ft-birsagot-szabott-ki-a-gazdasagi-versenyhivatal-a-facebook-ra (Acccessed: 15 August 2021).

[65] See: Evans, D.S. (2020) The Economics of Attention Markets. Available at: https://ssrn.com/abstract=3044858 (Accessed: 26 July 2021), pp. 26-27; Botta, M. and Wiedemann, K. (2019) Exploitative Conducts in Digital Markets: Time for a Discussion after the Facebook Decision. *Journal of European Competition Law & Practice*, 10 (8), p. 475.

[66] Pinheiro, F. (2021) Revisiting the 'Code': Building privacy competition into the architecture of the Internet. *European Competition Law Review*, 42 (8), p. 453.

[67] Botta, M. and Wiedemann, K. (2019) Exploitative Conducts in Digital Markets: Time for a Discussion after the Facebook Decision. *Journal of European Competition Law & Practice*, 10 (8), p. 476.

data would draw attention to the significance of providing data. On the other hand, the alternative option of paying in cash would create an opportunity for better data protection, and it could ensure that users consider the terms and conditions of data processing more thoroughly.

5. CONCLUSION

In the zero price business model, online platforms provide services in exchange for personal data.. However, this business model is detrimental to data protection principles, such as the principle of data minimisation, and fundamental rights, such as the right to self-determination. One of the reasons for this is information asymmetry, as a result of which users are unaware of the value of the personal data they provide, due to the false illusion of the service being free of charge. Another reason is the 'take it or leave it' effect caused by the dominance of the services offered by online platforms. Since data exploitation takes place not only due to the distortion of competition, the enforcement of competition law would not ensure a breakthrough on this front, as it would only allow action against undertakings with dominant market positions. Consequently, the elimination of the information asymmetry and the reinforcement of the right to self-determination require additional regulations that would ensure that users are able to use online services that are currently zero price without providing personal data. The question arises as to whether these online services would be able to remain free in this case. If free online services cannot be provided through general advertising, it must be ensured that users can decide to use the services in exchange for monetary payments. In addition, through the proper enforcement of the GDPR, in particular the principle of privacy by design, it must be ensured that the extent to which data are provided is not excessive, as there is currently no limit on this in the absence of competition.

LIST OF REFERENCES

[1] Autorité de la Concurrence and Bundeskartellamt: Competition Law and Data (10 May 2016).

[2] Belloso, N.M. and Petit, N. (2023) The EU Digital Markets Act (DMA): A Competition Hand in a Regulatory Glove, https://ssrn.com/abstract=4411743.

[3] Botta, M. and Wiedemann, K. (2019) Exploitative Conducts in Digital Markets: Time for a Discussion after the Facebook Decision. *Journal of European Competition Law & Practice*, 10 (8), pp. 465–478.

[4] Bundeskartellamt prohibits Facebook from combining user data from different

sources (7 February 2019) www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html (Accessed: 9 August 2021).

[5] Capobianco, A. and Nyeso, A. (2018) Challenges for Competition Law Enforcement and Policy in the Digital Economy. *Journal of European Competition Law & Practice*, 9 (1), pp. 19–27.

[6] Competition and Markets Authority (2020) Online Platforms and Digital Advertising.

[7] Directorate-General for Communication: Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union https://data.europa.eu/data/datasets/s864_74_3_ebs359?locale=en (Accessed: 5 August 2021).

[8] EDPS: Opinion on coherent enforcement of fundamental right sin the age of big data, Opinion 8/2016 (23 September 2016).

[9] Elvy, S-A. (2017) Paying for privacy and the personal data economy. *Columbia Law Review*, 117 (6), pp. 1369–1460.

[10] European Data Protection Supervisor (2014) Preliminary Opinion of the European Data Protection Supervision: Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy (8 March 2014).

[11] European Data Protection Supervisor (2017) Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content of the European (14 March 2017).

[12] Evans, D.S. (2020) The Economics of Attention Markets. Available at: https://ssrn.com/abstract=3044858 (Accessed: 26 July 2021), pp. 26–27.

[13] Friedman, D.A. (2008) Free Offers: A New Look. *New Mexico Law Review*, 38 (1), pp. 49–94.

[14] Gal, M. and Petit, N. (2021) Radical Restorative Remedies for Digital Markets. *Berkeley Technology Law Journal*, 37 (1), pp. 617–674.

[15] Georgieva, K., Díez, F.J., Duval, R. and Schwarz, D. (2021) Rising Market Power, A Threat to the Recovery? IMF Blog (15 March 2021) blogs.imf.org/2021/03/15/rising-market-power-a-threat-to-the-recovery accessed 15 June 2021.

[16] Hendricks, V.F. and Vestergaard, M. (2019) *Reality Lost*. Cham: Springer.

[17] Hoofnagle, C.J. and Whittington, J. (2014) Free: Accounting for the Costs of the Internet's Most Popular Price. *UCLA Law Review*, 61 (3), pp. 606–670.

[18] Hungarian Competition Authority (2019) GVH imposed a fine of EUR 3.6 M on Facebook. Available at: https://www.gvh.hu/en/press_room/

press_releases/press_releases_2019/gvh-imposed-a-fine-of-eur-3.6-m-on-facebook (Accessed: 26 July 2021).

[19] Lypalo, D. (2021) Can Competition Protect Privacy? An Analysis Based on the German Facebook Case. *World Competition*, 44 (2), pp. 169-198.

[20] Madrigal, A.C. (2013) The Machine Zone: This Is Where You Go When You Just Can't Stop Looking at Pictures on Facebook. *The Atlantic*, 31 July 2013. Available at: https://www.theatlantic.com/technology/archive/2013/07/the-machine-zone-this-is-where-you-go-when-you-just-cant-stop-looking-at-pictures-on-facebook/278185 (Accessed: 26 June 2021).

[21] Newman, J.M. (2019) Regulating Attention Markets. *University of Miami Legal Studies Research Paper*. Available at: https://ssrn.com/abstract=3423487 (Accessed: 12 June 2021).

[22] OECD (2016) Big Data: Bringing Competition Policy to the Digital Era, DAF/COMP/M(2016)14.

[23] OECD (2017) Algorithms and Collusion – Note from the European Union, DAF/COMP/WD(2017).

[24] OECD (2018) Quality considerations in digital zero-price markets Background note by the Secretariat, DAF/COMP(2018).

[25] Pinheiro, F. (2021) Revisiting the 'Code': Building privacy competition into the architecture of the Internet. *European Competition Law Review*, 42 (8), pp. 453–467.

[26] Shelanski, H.A. and Sidak, J.G. (2001) Antitrust Divestiture in Network Industries. *The University of Chicago Law Review*, 68 (1), pp. 1–99.

[27] Stigler Center for the Study of the Economy and the State, 'Stigler Committee on Digital Platforms Final Report' (2019) www.chicagobooth.edu/research/stigler/news-and-media/committee-on-digital-platforms-final-report accessed 15 June 2021.

[28] Tene, O. and Polonetsky, J. (2013) Big Data for All: Privacy and User Control in the Age of Analytics. *Northwestern Journal of Technology and Intellectual Property*, 11 (5), pp. 239-275.

[29] United Nations (2019) Digital Economy Report 2019.

[30] van Lieshout, M. (2015) The Value of Personal Data. In: Jan Camenisch, Simone Fischer-Hübner and Marit Hanses (eds.) *Privacy and Identity Management for the Future Internet in the Age of Globalisation*. Cham: Springer, pp. 26–38.

[31] Vásquez Duque, O. and Hoffmann, J. (2021) Can data exploitation be properly addressed by competition law? A note of caution. Concurrences, February 2021 https://www.concurrences.com/en/review/issues/no-1-

2021/law-economics/can-data-exploitation-be-properly-addressed-by-competition-law-a-note-of-en (Accessed: 10 July 2021).

[32] Waked, D.I. (2020) Antitrust as Public Interest Law: Redistribution, Equity and Social Justice. *The Antitrust Bulletin*, 65 (1), pp. 87–101.

[33] Warner, M.R. (2018) Potential Policy Proposals for Regulation of Social Media and Technology Firms, White Paper Draft, 20 August 2018.

[34] Wu, T. (2019) Blind Spot: The Attention Economy and the Law. *Antitrust Law Journal*, 82 (3), pp. 771–806.

DOI 10.5817/MUJLT2023-1-5

PLAYING THE SYSTEM: CONTENT RECOGNITION TECHNOLOGIES AND CREATIVE PROCESS OF SAMPLING MUSICIANS *

by

IVAN DAVID † RUDOLF LEŠKA ‡

In the first part of the study, we summarize the existing types of copyright bots. In the second part, we present the current state of legal research on the implementation of copyright bots and our own analysis which focuses on the Czech Supreme Court's decision concerning copyright bots. The core of this paper concerns the impact of copyright bots on the work of sampling musicians and how the creativity of musicians is shaped by their struggle to avoid detection of sampled music by bots in the online environment.

KEY WORDS

Copyright, Bots, Technology, Sampling, Content Recognition

1. INTRODUCTION

It is no secret that the improvement of copying technologies has always been a catalyst for conflict in creative industries as far as copyright law is concerned. It is also clear that legal concerns can shape an artist's creativity and work, mainly in copyright-intensive industries like the film and music industry, which depend on the online distribution of their products. It occurred to us that the introduction of automated content recognition technologies has

* This work was supported by the Improving schematics of Doctoral student grant competition and their pilot implementation at the Palacký University Olomouc under grant no. CZ.02.2.69/0.0/0.0/19_073/0016713. Specifically, the research was conducted within the "Law and Remix Culture: Aesthetics and Ethics of Musical Remix" project (project no. DSGC-2021-0015). Our thanks go to anonymous reviewers who substantially helped us to precise our paper and its findings. The data that support the findings of this study are available on request from the corresponding author, Ivan David. The data are not publicly available due to their containing information that could compromise the privacy of research participants.

† ivan.david@kmvs.cz, PhD Candidate, Department of Media Studies, Palacký University Olomouc, Czechia, and Counsel, KMVS Law Office, Czechia

‡ leska@staidl-leska.com, Senior Assistant Professor, University of Finance and Administration, Czechia, and Counsel, Štaidl Leška advokáti, Czechia

had a palpable impact on the creativity of artists, mainly in the field of music production. As we will demonstrate, our research and this study have proven this hypothesis to be correct. Based on our 38 semi-structured interviews, 36 with professional musicians who routinely use sampled materials in their own work as well as one with a representative from an international record label and one from a global company that develops content recognition technologies, we present the attitudes of artists towards automated content recognition technologies (copyright bots)[1] and how they deal with them in their creative practice. Like the character Josef Švejk in the famous novel by Czech writer Hašek,[2] these artists tend to employ various strategies to play the system rather than submit themselves to it.

Our approach is interdisciplinary, as we believe it could be a meaningful contribution to the often abstractly technical legal research. We therefore conducted a qualitative sociological analysis and applied it to our findings based on desktop legal research. In the first part of our study, we summarize the existing types of copyright bots; in the second part, we present the current state of legal research on the implementation of copyright bots and our own analysis which focuses on the Czech Supreme Court's decision concerning copyright bots; the core of this paper then concerns the impact of copyright bots on the work of sampling musicians.

We do not address the issue of liability (including the well-researched sampling case law, such as the *Pelham*[3] case), management and mechanisms of automated takedown notices, nor the precision of copyright bots, as this has already been done by others – examples of anecdotal[4] as well as serious[5]

---

1 Bot, "a computer program that works automatically, especially one that searches for and finds information on the internet" *(Cambridge Advanced Learner's Dictionary & Thesaurus*. Available from: `https://dictionary.cambridge.org/dictionary/english/bot` [Accessed 20 November 2022]).

2 Hašek, J. (2005) *The Good Soldier Švejk and His Fortunes in the World War*. Translated from Czech by Cecil Parrott. London: Penguin Books.

3 Judgment of 29 July 2019, Pelham GmbH and others, C-476/17, EU:C:2019:624.

4 A 10-hour long video of white noise (available from `https://www.youtube.com/watch?v=VcQZAzDVTlA`) received five wrongful copyright claims. Cf. Tune, C. and Iverson, S. (2020) The Rise of the Copyright Bots. *Internet and Technology Law*. Available from `https://www.internetandtechnologylaw.com/copyright-bots/` [Accessed 16 November 2022].

5 The Washington Post's story describes the difficulties classical musicians faced during the COVID-19 pandemic when automated bots misidentified their recorded content with other recordings. Cf. Brodeur, M. (2020) Copyright bots and classical musicians are fighting online. The bots are winning. The Washington Post. Available from: `https://www.washingtonpost.com/entertainment/music/copyright-bots-and-classical-musicians-are-fighting-online-the-bots-are-winning/2020/05/20/a11e349c-98ae-11ea-89fd-28fb313d1886_story.html` [Accessed 16 November 2022]. For an overview of similar cases cf. Berkowitz, A. (2022) Classical Musicians v. Copyright Bots. *Information Technology and Libraries*, 41(2). Available

flaws in the technology can be found in numerous sources; instead, we focus on how legal regulations, which are facing automated enforcement, are communicated, with the hope that this information may prove useful for policy makers, online content sharing platforms and copyright owners alike. Sociological findings serve for discussion of optimal or right legal regulation which should be based on the informed understanding of social expectations by the addressees of the regulation. Otherwise, the law becomes in tension with actual behavior of individuals which undermines the legal awareness and the rule of law as such.

Last but not least, data from our research have furthermore relevancy also for research in the field of musicology and aesthetics.

For the purpose of this study, we use the English term copyright as an umbrella term for author's rights and related rights (including phonograms) and the term copyright owner for any holder of copyright, whether it is the author and performing artist or entities so authorized, such as employers, assignees and licensees.

2. TYPES OF AUTOMATED TECHNOLOGIES USED TO DETECT ILLEGAL CONTENT

In today's online landscape, there is a large number of technologies used for the automated detection of illegal content. Such technologies are used for many purposes – from combatting child pornography to preventing the spread of terrorist content. Nonetheless, the primary focus of this chapter is on the technologies used by automated programs for recognizing copyright-infringing materials ("copyright bots"), which typically target films and music, photographs or pieces of literature[6] distributed without the appropriate licensing.

Many such technologies are of a hybrid nature. However, for the sake of simplicity, we can schematically divide the technologies into the following categories.[7]

---

from https://ejournals.bc.edu/index.php/ital/article/view/14027 [Accessed 16 November 2022].

[6] Most often, this concerns e-books. See for instance: Rosenblatt, B. (2017) A Bounty Hunting Service for E-Book Piracy. Copyright and Technology. Available from https://copyrightandtechnology.com/2017/01/30/a-bounty-hunting-service-for-e-book-piracy/ [Accessed 16 November 2022]

[7] In this chapter, we use the typology and terminology developed in the two recent EUIPO expert studies: European Union Intellectual Property Office (2020) *Automated Content Recognition: Discussion Paper – Phase 1, Existing Technologies and Their Impact on IP*. ISBN 978-92-9156-280-0. Available from: https://data.europa.eu/doi/10.2814/52085 [Accessed 16 November 2022], and European Union Intellectual Property Office (2022) *Automated Content Recognition: Discussion Paper – Phase 2, IP Enforcement and Management*

2.1. HASHING

The method of hashing is based on the principle that simple identifiers consisting of a relatively short number of unique characters of a fixed-length value ("hashes") are automatically generated for the identification of digital files. The new hash files – usually of a significantly smaller size than the original digital files – are then stored in reference databases. When determining whether a certain unknown digital file is identical to a file for which a hash has been generated, a hash is also generated for this unknown digital file using the same technology; the new hash and the original hash are then compared and a match is sought.

The clear advantage of this technology is that it is simple, easy to implement, fast and undemanding in terms of storage space and hardware performance. Furthermore, this technology can be used for a wide range of digital files regardless of their content (i.e., whether they contain pictures, music, texts or another type of content).

The obvious disadvantage is that the technology is primarily designed to match identical files. If the original file – in our case a file with copyrighted material – is altered in any way (for instance, by compression or change in format), a different hash will be generated (two distinct data will always deliver different hash) and no match will be found. What is more, hashes are only used to recognize specific digital files; they thus have no descriptive capacity and as such do not recognize the actual content of these files.

As far as copyright-infringing materials are concerned, hashing technology (as such) is most often successfully used by providers of platforms designed for sharing public and openly accessible content.[8] In such cases, it helps to ensure that if a digital file is flagged by any user or content owner as copyright infringing, other identical files on the platform are also disabled and the (identical) content is not reuploaded.

2.2. WATERMARKING

In the case of watermarking, the data used to identify digital files are not stored in separate reference databases, like in hashing, but such identifying data are incorporated directly into the digital files.

Therefore, it is not necessary to compare the hash of the original digital file with the automatically generated hash of the unknown file to find a potential match; instead, the information needed to identify the file can be found directly in the file itself.

Use Cases . ISBN 978-92-9156-326-5. Available from: `https://data.europa.eu/doi/10.2814/952694` [Accessed 16 November 2022]

[8] YouTube uses hashing technology in its Content ID tool to prevent identical files from being uploaded repeatedly.

Watermarks can either be generic, i.e., applied to large number of digital files and usually identifying their source,[9] or specific, thus identifying each unique digital file. We can also distinguish between watermarks that are clearly visible and thus generally readable by anyone using the file[10] and those that are invisible (typically found in the metadata of the marked file) and which generally require special software to be read. In terms of the "source" of the digital file that a watermark identifies, it can be either the original source in the sense of information on the rights holder, or the "illegal" source, i.e., the source from which the pirated (i.e., copyright-infringing) materials are spread.

While the advantage of watermarks is that there is no need for the creation of separate hashes and reference databases containing these hashes, the main disadvantage of this method is that only digital files that have been previously watermarked can be successfully recognized. Marking each digital file with a watermark can also be very demanding and resource-intensive, especially if watermarks are to be generated for every unique file. Finally, watermarking technologies are generally less standardized than hashing technologies, meaning that in the case of more sophisticated, i.e., invisible (embedded) watermarks, special software equipment is needed for these watermarks to be successfully read and recognized. One the other hand, the current state of art in watermarking technology – unlike hashing technology – is generally reliable even for marked files that are somehow altered.

2.3. FINGERPRINTING

Fingerprinting can simply be described as a more sophisticated form of hashing. Just like in hashing, identifying files (called "fingerprints") are automatically generated resulting in digital files that are smaller in storage size than the originals. These newly created files are then stored in separate reference databases. When a match is sought, the pre-existing fingerprints are compared with the newly generated fingerprints for the unknown digital files.

The major difference between hashing and fingerprinting is that

[9] For instance, generic watermarks are used to mark audiovisual files for films intended for viewing by members of the Academy of Motion Pictures Arts and Sciences when voting for the "Oscar" winner in different categories. The same applies to audiovisual files used by members of Czech Film and Television Academy for choosing the winners of the "Czech Lion Awards". In these and similar cases, the watermark informs the viewer that the digital file in question is intended solely for this purpose and cannot be used elsewhere – thus also identifying the source of the file.

[10] Most likely the best-known example of visible watermarks are the graphic logos of TV networks used to mark all programs broadcasted by them.

while hashing is only used for identifying identical digital files as such, fingerprinting can even identify identical or similar file content. Practically speaking, this means that fingerprinting technology is more resistant to the alternation of digital files, as it can still identify the major traits of the content contained in the files in question. In practice, fingerprinting software analyzes the content (music, films, texts etc.) and extracts statistical samples of the content (for instance, several samples for each second of a particular song); the more samples that are extracted, the more precise the fingerprinting recognition will be. On the other hand, the more precise the fingerprinting method is, the more demanding it is in terms of hardware (storage space, computational capacity) – mainly when compared to less demanding methods such as hashing and watermarking.

At the moment, fingerprinting appears to be the most popular and sophisticated method for the automated detection of illegal content as far as copyright infringement is concerned. Fingerprinting is, for instance, the main component of such software devices as YouTube Content ID[11] and Facebook Rights Manager.[12] The same principle is also the basis of the popular music recognition application Shazam.[13] When fingerprinting is used to find copyright-infringing materials (music, images and videos) on content sharing platforms like the above-mentioned YouTube or Facebook, content owners are typically given several options for dealing with copyright-infringing content, most often in the form of blocking,[14] tracking[15] or monetizing[16] the flagged content. In some cases, the automated technology also contains mechanisms for resolving conflicts concerning IP ownership (amongst IP owners or between an IP owner and a user) over specific pieces of content.[17]

In any case, it largely depends on the operator of the search technology as to where the accuracy threshold should lie. As is stands, the search tool can be set up in such a way that it can detect even very short extracts

[11] See `https://support.google.com/youtube/answer/2797370?hl=en` [Accessed 15 November 2022]. For Content ID analysis cf. Shinn, L. (2015) YouTube's Content ID as a Case Study of Private Copyright Enforcement Systems, *AIPLA Q. J., 43 (2/3)*. Perel, M and Elkin-Koren, N. (2016) Accountability in Algorithmic Copyright Enforcement. *STAN . TECH . L. REV .*, 19, 473, p. 510 et seq.

[12] See `https://rightsmanager.fb.com/` [Accessed 15 November 2022]

[13] See `https://www.shazam.com/` [Accessed 15 November 2022]

[14] Blocking means that the content is blocked from further access.

[15] Tracking means that content owner only receives statistics on how frequently the content is accessed.

[16] Monetizing usually means that advertisements are added to the content and the content owner receives (full or partial) revenue from the advertisers.

[17] This is the case of YouTube, for example. See "Resolve Asset Ownership Conflicts" at `https://support.google.com/youtube/answer/3013321?hl=en` [Accessed 15 November 2022]

of copyright-protected material (e.g., just a few seconds of sampled music) used in other works. Nevertheless, the operator of this technology can (and very often does) deliberately configure the search engine so that the targeted copyrighted extracts are not too short. Firstly, this reduces the demands placed on the hardware equipment needed to run the search engine; secondly, it undoubtedly helps in preventing too many false positives or too severe content restrictions, as they can be controversial when considering the existence of copyright exceptions.

2.4. AI-BASED (ENHANCED) CONTENT RECOGNITION

The latest trend in the field of automatic content recognition is technological solutions based on artificial intelligence. Unlike all the aforementioned automatic recognition technologies, in this case the software solution actually "understands" what it sees or hears. In other words, AI-based technology can perform a much deeper analysis of potentially copyright-breaching content than hashing, watermarking or fingerprinting technologies ever could.

The development of these technologies is likely most pronounced in the automatic analysis of static and moving images – where artificial intelligence can (based on existing databases), for example, recognize the faces of specific people in an image and perform a predetermined action accordingly. Thanks to this technology, digital files can be sorted and categorized and keywords and other descriptors can be automatically generated.

Despite the obvious advantages posed by this advanced technology, as it can significantly improve accuracy in the detection of illegal content, its main disadvantage is the substantial demand on hardware performance and storage capacity. For these reasons, such advanced solutions are often combined or supplemented in practice with one or more of the above-mentioned "traditional" methods of automatic content recognition.

In summary, each of the above-specified technologies is suitable for a different purpose, mainly because they possess a different level of accuracy when searching for illegal content (even when the searched content has been in some way altered); furthermore, they require different demands in terms of the required storage space and performance of the hardware on which they run. These technologies are often combined to multiply their advantages and achieve higher precision.

3. COPYRIGHT AND AUTOMATED CONTENT RECOGNITION TECHNOLOGY: THE DILIA CASE

Copyright, as any other right, deteriorates if unenforced. Rampant infringement in the online environment facilitated by the operation of non-liable platforms, which reap exorbitant profits on content they have neither produced nor paid for, is impossible to fight by human oversight. The legal rules that limit the liability of intermediaries – originally designed for traditional web hosting providers and by no means for social networks and similar services[18] – have allowed for such a broad interpretation that they provide a safe harbor (if not safe heaven) for platform operators, revolutionarily shifting the burden of copyright policing from those who monetize the content to those who create it. This has prompted these platforms to store hundreds of millions of protected authorial works.[19] Human policing of such vast amounts of content is clearly impossible and this situation has naturally given rise to automated solutions. While originally it was only copyright owners who were active in policing and enforcing copyright, newer case law in the US, EU and elsewhere has balanced the situation by forcing platform operators to adopt a more proactive approach to monitoring content on their websites.[20] YouTube – which is facing possibly ruinous effects of copyright infringement litigation – has become one of the most proactive services in assisting copyright owners with content policing through their proprietary Content ID system.

Although copyright bots are not appealing to the tech industry and some parts of academia,[21] they work substantially better than anything else

[18] For the origins of the rules that limit the liability of intermediaries and a critical assessment of how these rules have been misinterpreted to cover much broader types of services cf. the study by Leška, R. and Půr, M. (2022) Technologické společnosti a jejich odpovědnost za obsah na internetových platformách. *New Direction*. Available from: `https://newdirection.online/publication/technologicke_spolechnosti_a_jejich_odpovdnost_za_obsah_na_internetovch_pla` [Accessed 20 November2022]. For critical insight into US platform liability (or lack thereof), cf. Gabison, G. and Buiten, M. (2020) Platform Liability in Copyright Enforcement. *Columbia Science and Technology Law Review*, 21, pp. 237–280. For advocacy against amendments to the current US law, cf. Samuelson, P. (2021) Pushing Back on Stricter Copyright ISP Liability Rules. *Michigan Technology Law Review*, 27, pp. 299–344.

[19] Reportedly, YouTube alone stores approx. 800 mil. videos as of May 2022 (containing many authorial works and other protected content, often without a license). Cf. Hayes, A. (2022) YouTube Stats: Everything You Need to Know In 2022! Wyzowl. Available from: `https://www.wyzowl.com/youtube-stats/` [Accessed 16 November 2022].

[20] The evolution of this case law and industry agreements exceeds the scope of our study. Developments in EU law are summarized in the YouTube/Cyando judgment. Frank Peterson v Google LLC and Others and Elsevier Inc.v Cyando AG, Court of Justice of the European Union, joined cases C-682/18 and C-683/18.

[21] Pamela Samuelson, for instance, believes that the use of copyright bots by platform operators is inconsistent with copyright exceptions (user freedoms, as she calls it), incompatible with

currently available to us – unless we opt for some sort of blanket licensing, perhaps managed by collection societies. Of course, the content-matching technology used by these bots might often not recognize the context (although research in this direction is fast) resulting in mistakes (not unlike human error),[22] particularly when it comes to recognizing exceptions and limitations to copyright; nevertheless the system should be designed in such a way that allows the person asserting the exception to prove their claim (after the content has been disabled) and let the content be human-verified by the copyright owner with escalation to the platform operator. This is the only way this can work. Admittedly, the system makes mistakes when it comes to classical music, though technology is improving rapidly in this field, as confirmed by our interviewee (see below). To require human oversight for every single copyright claim for the tens of millions filed by copyright owners is unfeasible,[23] though this seems to be precisely the agreement that Lawrence Lessig came to with Liberation Music in a widely publicized lawsuit settlement.[24]

We do not share in condemnations of copyright bots as evil. In a situation where copyright infringement is rampant and personal policing impossible, it is hard to imagine that copyright owners alone would report infringing content while platforms would be free to erroneously keep millions of files with infringing content online – the approach should be fair and should not place stricter burdens on copyright owners than platform operators.

We are unaware of any case law which would specifically address the tolerated limit of erroneous takedown notices when assessing the rights of copyright owners. One exception is a landmark dispute in Czechia concerning the local collective management organization DILIA[25] and the

the no general monitoring obligation, in violation of rights to personal data and perhaps even the (EU) Charter of Fundamental Rights. Cf. Samuelson, P. (2021) Pushing Back on Stricter Copyright ISP Liability Rules. *Michigan Technology Law Review*, 27, pp. 299–344. We disagree with such a categorical stance.

[22] Even courts struggle to interpret exceptions and limitations and are often in disagreement with one another on the very same issues. It is therefore naive to believe that an assessment performed by a distant and under-educated employee would be a substantial improvement.

[23] DiCarlo, I. (2022) Copyright Bots Need a Tune-up. JTIP Blog. Available from: `https://jtip.law.northwestern.edu/2022/03/05/copyright-bots-need-a-tune-up/` [Accessed 10 November 2022]. Various studies examine the practice of prohibiting or at least making it very complicated for copyright owners to report infringing conduct, cf. Depoorter, B. and Walker, R. (2014) Copyright False Positives. *Notre Dame Law Review*, 89(1), p. 319. We believe this to be ill-advised for legislators as it would immensely benefit the technology companies without taking into account content creators.

[24] For details and an analysis of the case cf. Tan, C. (2014) Lawrence Lessig v Liberation Music Pty Ltd: YouTube's Hand (or Bots) in the Over-Zealous Enforcement of Copyright. *European Intellectual Property Review*, 36(6), pp. 347–351.

[25] Full legal name: DILIA, divadelní, literární, audiovizuální agentura, z. s. (Theatre, literary, audiovisual agency)

operator of the most popular Czech cyber-locker service "Ulož.to".[26] DILIA filed a complaint in which it asked the court to order the cyber-locker operator to ensure the permanent stay-down of certain Czech motion pictures (including Jiří Menzel's *Closely Watched Trains*, which received the Academy Award for Best Foreign Language Film in 1968).[27] What is important, DILIA also asked the court to order the defendant to remove their limit on the total number of requests made by DILIA from its IP address to the defendant's servers. The case went to trial at the Municipal Court in Prague[28] and a judgment was issued by the High Court in Prague[29] and finally confirmed by the Supreme Court.[30] What is interesting about DILIA's second claim is that the court investigated the correctness of DILIA's takedown notices. DILIA originally made these notices manually and Ulož.to even concluded a special agreement with DILIA, under which DILIA was entitled to directly remove infringing content uploaded by users to the website. Once DILIA switched to automated data processing, the bots started to find – and remove – large amounts of (illegal) user data and Ulož.to withdrew from the agreement with immediate effect due to contract breach. Under the contract, DILIA agreed to only remove content to which they held the rights.

The number of false positives was under 1 %.[31] According to private information from DILIA and the letter of withdrawal from Ulož.to, which was read in a public hearing at court, in the period from June to October 2012, DILIA removed 2264 files of which Ulož.to identified 11 false positives.[32] This drives the number of false positives down further below 0.5 %. Formally,

[26] The operator's legal name at the time the Supreme Court's judgment was made was Ulož.to cloud a. s., later it was petacloud a. s. At the time of publication, the operator of the website has changed. Today, it is another entity named Cloud Platforms a. s. while the domain name itself was sold to yet different entity Meta Web Services a. s.

[27] Procedurally, the claim was combined. The plaintiff requested a a) permanent injunction (in case it was proven that the defendant was actively involved in illicit conduct), b) permanent stay-down based on certain word filters (in case the request for a permanent injunction was denied). This part of the proceeding is beyond the scope of our study but it can be noted that the plaintiff was only successful with claim b) since the court did not find (or was unwilling to find) enough evidence of structural infringement on the website.

[28] Unpublished judgment of the Municipal Court in Prague of 22 February 22 2019, 34 C 5/2017. Available from: `https://www.dreport.cz/wp-content/uploads/TechLaw_judik\%C3\%A1t_Ulozto_Dillia_34-C-5-2017.pdf` [Accessed 1 November 2022].

[29] Unpublished judgment of the High Court in Prague of 20 January 2021, 3 Co 58/2019.

[30] Judgment of the Supreme Court of 8 June 2022, 23 Cdo 1840/2021. Available from the website of the court and numerous online sources, including `http://kraken.slv.cz/23Cdo1840/2021` [Accessed 1 November 2022].

[31] Srstka, J. (2014) Žaloba DILIA proti úložišti www.ulozto.cz. Věstník DILIA, , p. 41. Available from `https://www.dilia.cz/ke-stazeni?cat=ostatni` [Accessed 1 November 2022]. The court mentions "a minimal percentage" (paragraph 31 of the judgment of the municipal court).

[32] It should be noted that some of those files were manifestly illegal too, they just did not contain content by DILIA authors; some were suspicious Wikipedia articles which appeared

Ulož.to's withdrawal from the agreement under which DILIA was entitled to directly remove files on the Ulož.to service was legally valid and this fact was undisputed. On the other hand, even if DILIA had to later rely on standardized procedures under Ulož.to's policy and the framework of the E-Commerce Directive[33] and its Czech transposition,[34] the argument explaining DILIA's false positives did not convince the court when deciding about the "free pass" DILIA was given to be able to crawl, search and report infringing content. Unfortunately, the trial court was not specific in the legal justification stipulating that all of DILIA's requests are not to be blocked, including a defense against "denial-of-service" (DOS) attacks (flooding the target with information/traffic); nevertheless, judging by the context, it appears that the trial court found this obligation in the general tort law and in the general provision against causing unjustifiable harm to others (Art 2900 of the Czech Civil Code).[35] The appellate court also did not make reference to any specific statute, though it suggested that such an obligation is a sort of special claim made by the copyright owner in the spirit of recital 17 of the Enforcement Directive.[36] Finally, the Supreme Court upheld this position and further specified it in reference to Art 98c(1) of the Czech Copyright Act,[37] which provides collective management organizations with the right to ask users for information concerning uploaded content while per analogiam extending this claim to the platform operator (cyber-locker service), even if the platform operator is not a user in itself (the case was decided under pre-DSM Directive law).

The lesson learned from this interesting Czech case regarding the operation of copyright bots is that the use of copyright bots is fully legal, the intermediary is legally obliged to allow copyright bots unobstructed access to search through its service,[38] and that even if errors occur, they are not grounds enough to forbid copyright owners from performing searches in the service (provided that it does not constitute abusive conduct). That being said, copyright owners remain liable for actual damages caused by any such

as protected content, although it is unclear why someone would upload a Wikipedia article to a cyber-locker.

33 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

34 Act No. 480/2004 Coll., on certain information society services.

35 Act No. 89/2012 Coll., the Civil Code.

36 Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights.

37 Act No. 121/2000 Coll., on copyright, on rights related to copyright and on the amendment of certain laws (Copyright Act).

38 It must be noted that the operator of the service is also protected against possible abuses of such rights by the general provisions of the civil code prohibiting abusive conduct.

errors under applicable tort law. We believe this basic principle to remain valid even with the transposition of the new DSM Directive[39] in the laws of EU member states.

4. IMPACT OF COPYRIGHT BOTS ON THE WORK OF SAMPLING MUSICIANS

In our research completed in 2022,[40] we conducted 36 semi-structured interviews with professional musicians who use music samples in their work. We spoke with 21 electronic dance musicians, 10 hip-hop and rap musicians and 5 alternative pop musicians. We also conducted an interview with a representative of a major Czech music label that uses YouTube Content ID technology, and one interview with a representative of a major international software company that develops globally successful automated software recognition technology.

In our interviews with the musicians, we focused on several topics concerning the impact of copyright on their creative practice, both from an aesthetic and ethical point of view. Importantly, all of the interviewed musicians – at least occasionally-release their records themselves on various platforms without interference from a record label, which would otherwise take care of the standard release protocol and rights clearance (if samples are concerned).

One of the main conclusions here was that even though all of the interviewed musicians were at least aware of the basic principles of copyright (though many were unsure of the specifics, for instance the conditions for copyright exceptions), the total majority admitted that they generally make no attempt to clear the rights to samples used in their projects; if they do seek permission, one of the main reported motivations was precisely the existence of copyright bots.

It appears from the interviews that copyright bots were often the only confrontation these artists had with actual copyright enforcement, and as such they represented the whole copyright system "in a nutshell".

According to our findings, the existence of copyright bots has a profound impact on the work of sampling artists from a creative point of view, as these

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

[40] The research was realized within the OP VVV project "Improving the schemes of the Doctoral student grant competition and their pilot implementation", reg. No. CZ.02.2.69/0.0/0.0/19_073/0016713. Specifically, the research was conducted within the "Law and Remix Culture: Aesthetics and Ethics of Musical Remix" research project (project no. DSGC-2021-0015). The results of these interviews are reported in this submission for the first time.

bots force them to either (less often) clear all third party rights, or (more often) radically shorten, transform or modify music samples so that they cannot be recognized by the ubiquitous copyright bots.[41] Some of these artists even admitted to using apps for automated content recognition (like Shazam) to ensure that copyright bots do not recognize the shortened and altered samples after they are uploaded to YouTube or a similar content sharing platform. Other artists, for instance, "test" the copyright bots on YouTube by uploading a music video containing uncleared samples, though without making the video public – they then simply wait to see if they will be notified of copyright infringement by the YouTube administrator.[42]

Only a small minority of artists who do not use popular content sharing platforms or online distribution tools, but instead only release their records on vinyl or MC, seemed to be "immune" to the influence of copyright bots on their work; such artists thus tend not to limit themselves in their use of uncleared samples, exhibiting no need to significantly shorten or modify these samples just for the sake of going unrecognized by copyright bots.[43]

Similarly, artists who do not want their music to be overly screened by copyright bots but still want to publish it online, choose online platforms which (to their knowledge) have lenient policies regarding the automatic detection of illegal content.[44]

Another strategy that some sampling artists have developed in response to copyright bots is to only use samples of music they consider to be "old", "underground", "forgotten", "unknown" etc. – and which they (usually correctly) anticipate will not be screened by automated technologies.[45]

---

[41] One of the artists – a member of a successful alternative pop band – told us: *"We try to make the result unrecognizable. We release it on every possible media platform there is. Either we release some things ourselves, some through independent labels.* [...] *There was never a problem with the algorithm finding something that was taken from somewhere else* [...]." Another artist – working mostly as a DJ – told us: "[...] *some years ago I was looking for other music myself and I never had a problem with that because there was always some creative input* [from my side] *into it and it's not like a copier. It's* [...] *at least usually edited in such a way that the algorithm can't recognize it. The listener recognizes it there, the excerpt, and says to himself: 'Yeah, I know this', only it's slower and transposed a few degrees elsewhere, but the algorithm doesn't bother with it, because it's only interested in copy-paste."*

[42] One of the hip-hop artists told us: *"It is possible, I advised the same to* [anonymized name of another artist] *when he asked me how I do it. And I know* [anonymized name of another artist] *will also upload it to YouTube and find out that way. So it's probably a good idea to lock it so it's not public and upload it to YouTube. And they'll let you know if there's a problem."*

[43] Another hip-hop artist told us: *"I can put absolutely anything I want on vinyl and I'm good, because we're in the Czech Republic and we're completely off the radar. No digital robots check it, and* [...] *no one will notice, you can put whatever you want there."*

[44] One of the interviewed creators of electro dance music told us: *"I put it, for example, on Bandcamp, because on Bandcamp I feel that they don't care much about copyright unless someone reports it to that person, but I was afraid to put it on Spotify, for example, because I know that their algorithms are probably much more trained to capture those copyright breaches."*

[45] For example, one of the interviewed hip-hop artists expressed it thusly: *"I think that about 80*

Almost all of the interviewed artists that publish their music online had some real-life experience with copyright bots flagging their work for containing samples with uncleared rights; what usually happened was that the IP owner requested monetization, i.e., the partial or complete redirection of advertising revenue generated by the content to the IP owner's account.[46] Most of the artists we talked to found this practice to be correct and fair.[47] At the same time, most of the artists seemed to be "at peace" with the current state of affairs and some even found copyright bots to serve as an instigator of creativity, a sort of a game.[48]

Our interview with a representative of a major Czech record label essentially confirmed our findings from our interviews with the musicians as well as our general knowledge of how copyright bots operate (as described above). YouTube's 2022 policy for Content ID allows copyright owners to choose the length of the sample with potentially uncleared rights that YouTube's automated recognition software should search for – ranging from 1 second to the entire song. Our respondent confirmed that the record label he represents chooses to monetize the content in 90 % of infringing cases and very rarely decides to block the content in question. We can assume that similar economic behavior is also characteristic of other major labels.[49] The interviewee also explained that ContentID allows copyright owners to choose whether the content will be automatically blocked or whether it

% or 90 % of the samples [that I use in my work] *are absolutely unrecognizable because I distort them and use them in such a way that it's impossible* [for copyright bots to recognize them]. *And the samples that are, let's say, more sloppy, or that are more readable, are basically from underground metal bands. I talked about it recently with a couple of people, and basically the feedback was that they* [the copyright bots] *are not searching for this."* The same artist also told us: *"When I use a sample that is, let's say, a bit more readable, I think about where the line is and how to use it, so that I can use it and not consider it some form of theft. But of course, I realize that what I'm doing is stealing in a way."* Another hip-hop artist we interviewed told us: "[...] *all I can think of is that the only thing that cannot be sampled is something that is paid out, monetized on YouTube. So if we use a sound from an old blues thing on YouTube that nobody profits from, then it's cool."*

[46] One of the rappers told us: *"Well, it happened to us with an album [that copyright bots detected that we used an uncleared sample], and I think it's easily solvable* [...] *and that it was resolved in such a way that we didn't pay any money, of course, but that they* [i.e., the IP owners] *revoked our monetization and it all went to the other party."*

[47] The same interviewed rapper commented on the same situation: *"Meaning the sample was just stupidly overused and so on. So it was just a tax on stupidity."*

[48] One of the hip-hop artists told us: *"So, in a way, it annoys me that it's a little bit more complicated, how the robots watch it more closely, how everything is online and digital, but on the other hand, it's still the same and it's actually an interesting game, like it was before.* [...] *So it just depends on your creativity, how you can hide it so that no robot finds it, so that no one knows where you got it from, so you have a good unique source that no one knows and therefore no one can track it, that's the best approach and the magic of it."*

[49] 90 % of matched content being monetized is also mentioned by Perel, M. and Elkin-Koren, N. (2016) Accountability in Algorithmic Copyright Enforcement. *Stanford Technology Law Review*, 19, p. 512 (quoting Lev-Aretz,Y. (2012) Second Level Agreements. *Akron Law Review*, 45, p. 152.

will first be reported to the copyright owner, who then decides how to proceed with such content based on the circumstances. This record label representative corroborated our finding that YouTube's automated content detection technology cannot detect samples that have been materially altered. Finally, he also confirmed that the vast majority of musicians who use uncleared samples in their work, which are then detected by copyright bots, usually do not protest against advertising revenue being redirected to the owner of the sampled recording, or even against the blocking of such content.

Rightsowners' policies cannot be confirmed by YouTube Copyright Transparency Report,[50] since it only provides general information on the number of content matched and taken down, not the ration of monetized and taken down content.

In our interview with a representative of a company that develops globally successful automated software recognition technology, we learned that major global copyright owners prefer to intentionally configure YouTube copyright bots or their own bots so that very short samples go undetected. This prevents erroneous content recognition (false positives) – generally, the longer the detected segment of content, the lesser the chance of an error made by the copyright bot – and also avoids the recognition of content subject to copyright exemption, as users tend to exploit exceptions for short sampled fragments; furthermore, the reporting of potentially legitimate content is generally reputationally undesirable. Our respondent also confirmed that copyright bots still have difficulty identifying materially altered samples – especially if the song's tempo has been changed. This appears to be in line with reports of our interviewees experiencing issues with longer samples rather than very short or substantially modified samples and it is confirmed by YouTube Copyright Transparency Report.[51]

---

[50] In its last version, Google published this report in June 2022 for the previous year. Cf. Google Inc. (2022) YouTube Copyright Transparency Report H2 2021. Available from https://storage.googleapis.com/transparencyreport/report-downloads/pdf-report-22_2021-7-1_2021-12-31_en_v1.pdf [Accessed 6 June 2023]. Certain dynamic data (though with little relevance for this paper) can be found online at https://transparencyreport.google.com/youtube-policy/removals [Accessed 6 June 2023].

[51] *"Despite the power of technology, there are some cases where Content ID fails to identify a match with a user video. This can be due to uploaders' efforts to evade Content ID, or due to the fleeting use of the copyrighted work. For videos missed by automated identification, many Content ID partners have the ability to issue claims manually. While this tool covers an important gap, it accounted for fewer than 0.5% of Content ID claims made in the second half of 2021. For music rightsholders in particular, the automation rate is even higher. Finally, all channels on YouTube also have access to our copyright removal webform to request removal of any content not captured by another tool to which they have access."* In: Google Inc. (2022) YouTube Copyright Transparency Report H2 2021. Available from https://storage.googleapis.com/transparencyreport/report-

5. CONCLUSION

In this study, we did not advocate for specific statutory solutions and did not judge the existence of automated content recognition technologies as generally good or bad – our aim was to summarize their current legal framework using the example of the DILIA vs. Ulož.to case and to portray how these technologies have changed the creative attitudes of artists and what kind of playing field it creates, as these technologies will surely be with us for long.

In today's world, it is technology (and how it is configured by humans) which dictates what is legal and what is not on a daily basis. While in the past, the legitimacy of certain practices – for example when it comes to copyright exceptions – was derived from the conduct of individuals using the copyrighted content (publishers), it is now largely derived from the conduct of platform operators. "Automated processes designed to protect copyright-protected material"[52] thus clearly impose limits on the content available online,[53] though as demonstrated by our practical research, human creativity proves very resourceful and although one would think you cannot outsmart technology,[54] you actually can. In another words: "Do something inventive with it!"[55] One of the interviewed artists called this process "an interesting game" and it is indeed a "metagame"[56] when sampling artists try – not without success – to play the system in their creative work, whether it is copyright compliant or not.

LIST OF REFERENCES

[1] "Resolve Asset Ownership Conflicts" at https://support.google.com/youtube/answer/3013321?hl=en [Accessed 15 November 2022].

[2] Act No. 121/2000 Coll., on copyright, on rights related to copyright and on the amendment of certain laws (Copyright Act).

[3] Act No. 480/2004 Coll., on certain information society services.

[4] Act No. 89/2012 Coll., the Civil Code.

---

downloads/pdf-report-22_2021-7-1_2021-12-31_en_v1.pdf [Accessed 6 June 2023], p. 12.

[52] Eakman, A. (2015) The Future of the Digital Millennium Copyright Act: How Automation and Crowdsourcing Can Protect Fair Use. *Indiana Law Review*, 48 (2) p. 631, 634.

[53] *Ibid.*

[54] Douglas,N. (2018) You Can't Fool YouTube's Copyright Bots. LifeHacker. Available from https://lifehacker.com/you-cant-fool-youtubes-copyright-bots-1822174263 [Accessed 20 November2022].

[55] Starsky, C. How to Avoid YouTube Copyright Claims. Available from https://www.youtube.com/watch?v=w-7TMj_7UYU [Accessed 20 November 2022]

[56] Bailey, J. (2021) Copyright in the Age of Bots. Available from https://www.plagiarismtoday.com/2021/09/23/copyright-in-the-age-of-bots/ [Accessed 20 November 2022]

[5] Bailey, J. (2021) Copyright in the Age of Bots. Available from https://www.plagiarismtoday.com/2021/09/23/copyright-in-the-age-of-bots/ [Accessed 20 November 2022].

[6] Berkowitz, A. (2022) Classical Musicians v. Copyright Bots. *Information Technology and Libraries*, 41(2). Available from https://ejournals.bc.edu/index.php/ital/article/view/14027 [Accessed 16 November 2022].

[7] Brodeur, M. (2020) Copyright bots and classical musicians are fighting online. The bots are winning. The Washington Post. Available from: https://www.washingtonpost.com/entertainment/music/copyright-bots-and-classical-musicians-are-fighting-online-the-bots-are-winning/2020/05/20/a11e349c-98ae-11ea-89fd-28fb313d1886_story.html [Accessed 16 November 2022].

[8] Cambridge Advanced Learner's Dictionary & Thesaurus. Available from: https://dictionary.cambridge.org/dictionary/english/bot [Accessed 20 November 2022

[9] Depoorter, B. and Walker, R. (2014) Copyright False Positives. *Notre Dame Law Review*, 89(1).

[10] DiCarlo, I. (2022) Copyright Bots Need a Tune-up. JTIP Blog. Available from: https://jtip.law.northwestern.edu/2022/03/05/copyright-bots-need-a-tune-up/ [Accessed 10 November 2022].

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

[12] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

[13] Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights.

[14] Douglas,N. (2018) You Can't Fool YouTube's Copyright Bots. LifeHacker. Available from https://lifehacker.com/you-cant-fool-youtubes-copyright-bots-1822174263 [Accessed 20 November2022].

[15] Eakman, A. (2015) The Future of the Digital Millennium Copyright Act: How Automation and Crowdsourcing Can Protect Fair Use. *Indiana Law Review*, 48 (2).

[16] EUIPO expert studies: European Union Intellectual Property Office (2020) *Automated Content Recognition: Discussion Paper – Phase 1, Existing Technologies and Their Impact on IP*. ISBN 978-92-9156-280-0. Available from: https://data.europa.eu/doi/10.2814/52085 [Accessed 16 November 2022].

[17] European Union Intellectual Property Office (2022) *Automated Content Recognition: Discussion Paper – Phase 2, IP Enforcement and Management Use Cases* . ISBN 978-92-9156-326-5. Available from: https://data.europa.eu/doi/10.2814/952694 [Accessed 16 November 2022].

[18] Frank Peterson v Google LLC and Others and Elsevier Inc.v Cyando AG, Court of Justice of the European Union, joined cases C-682/18 and C-683/18.

[19] Gabison, G. and Buiten, M. (2020) Platform Liability in Copyright Enforcement. *Columbia Science and Technology Law Review*, 21.

[20] Google Inc. (2022) YouTube Copyright Transparency Report H2 2021. Available from https://storage.googleapis.com/transparencyreport/report-downloads/pdf-report-22_2021-7-1_2021-12-31_en_v1.pdf [Accessed 6 June 2023].

[21] Hašek, J. (2005) *The Good Soldier Švejk and His Fortunes in the World War*. Translated from Czech by Cecil Parrott. London: Penguin Books.

[22] Hayes, A. (2022) YouTube Stats: Everything You Need to Know In 2022! Wyzowl. Available from: https://www.wyzowl.com/youtube-stats/ [Accessed 16 November 2022].

[23] https://rightsmanager.fb.com/ [Accessed 15 November 2022].

[24] https://support.google.com/youtube/answer/2797370?hl=en [Accessed 15 November 2022].

[25] https://transparencyreport.google.com/youtube-policy/removals [Accessed 6 June 2023].

[26] https://www.shazam.com/ [Accessed 15 November 2022].

[27] Judgment of 29 July 2019, Pelham GmbH and others, C-476/17, EU:C:2019:624.

[28] Judgment of the Supreme Court of 8 June 2022, 23 Cdo 1840/2021. Available from the website of the court and numerous online sources, including http://kraken.slv.cz/23Cdo1840/2021 [Accessed 1 November 2022].

[29] Leška, R. and Půr, M. (2022) Technologické společnosti a jejich odpovědnost za obsah na internetových platformách. *New Direction*. Available from: https://newdirection.online/publication/technologicke_spolechnosti_a_jejich_odpovdnost_za_obsah_na_internetovch_pla [Accessed 20 November2022].

[30] Perel, M and Elkin-Koren, N. (2016) Accountability in Algorithmic Copyright Enforcement. *STAN . TECH . L. REV .*, 19, 473.

[31] Rosenblatt, B. (2017) A Bounty Hunting Service for E-Book Piracy. Copyright and Technology. Available from https://copyrightandtechnology.com/2017/01/30/a-bounty-hunting-service-for-e-book-piracy/ [Accessed 16 November 2022].

[32] Samuelson, P. (2021) Pushing Back on Stricter Copyright ISP Liability Rules. *Michigan Technology Law Review*, 27.

[33] Shinn, L. (2015) YouTube's Content ID as a Case Study of Private Copyright Enforcement Systems, *AIPLA Q. J., 43 (2/3)*.

[34] Srstka, J. (2014) Žaloba DILIA proti úložišti www.ulozto.cz. Věstník DILIA, , p. 41. Available from https://www.dilia.cz/ke-stazeni?cat=ostatni [Accessed 1 November 2022].

[35] Starsky, C. How to Avoid YouTube Copyright Claims. Available from https://www.youtube.com/watch?v=w-7TMj_7UYU [Accessed 20 November 2022].

[36] Tan, C. (2014) Lawrence Lessig v Liberation Music Pty Ltd: YouTube's Hand (or Bots) in the Over-Zealous Enforcement of Copyright. *European Intellectual Property Review*, 36(6).

[37] Tune, C. and Iverson, S. (2020) The Rise of the Copyright Bots. *Internet and Technology Law*. Available from https://www.internetandtechnologylaw.com/copyright-bots/ [Accessed 16 November 2022].

[38] Unpublished judgment of the High Court in Prague of 20 January 2021, 3 Co 58/2019.

[39] Unpublished judgment of the Municipal Court in Prague of 22 February 22 2019, 34 C 5/2017. Available from: https://www.dreport.cz/wp-content/uploads/TechLaw_judik\%C3\%A1t_Ulozto_Dillia_34-C-5-2017.pdf [Accessed 1 November 2022].

MUJLT Official Partner (Czech Republic)

ROWAN LEGAL, advokátní kancelář s.r.o
https://rowan.legal

Cyberspace 2022 Partners

Zákony pro lidi - AION CS
https://www.zakonyprolidi.cz

CODEXIS - ATLAS consulting
https://www.codexis.cz

Právní prostor
https://www.pravniprostor.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