

MASARYK UNIVERSITY JOURNAL OF LAW AND TECHNOLOGY

VOLUME 19 | NUMBER 2 | FALL 2025 | ISSN 1802-5943

PEER REVIEWED



CONTENTS:

MALIK | HEMMAT | MEHRAEEN | FATTAHI | SHIRANI | PONGÓ |
KÁLMÁN | SZANISZLÓ | TRIBL | PRINCE TRITTO | TORRES ORTEGA |
BUJALSKI | SZENTGÁLI-TÓTH | BERKES | SVANTESSON | HOSPES

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

Editor-in-Chief

Jakub Harašta, Masaryk University, Brno

Deputy Editor-in-Chief

Ondřej Böhm, Masaryk University, Brno

Founding Editor

Radim Polčák, Masaryk University, Brno

Editorial Board

Tomáš Abelovský, Swiss Re, Zurich

Zsolt Balogh, Corvinus University, Budapest

Michael Bogdan, University of Lund

Joseph A. Cannataci, University of Malta | University of Groningen

Josef Donát, ROWAN LEGAL, Prague

Julia Hörnle, Queen Mary University of London

Josef Kotásek, Masaryk University, Brno

Leonhard Reis, University of Vienna

Naděžda Rozehnalová, Masaryk University, Brno

Vladimír Smejkal, Brno University of Technology

Martin Škop, Masaryk University, Brno

Dan Jerker B. Svantesson, Bond University, Gold Coast

Markéta Trimble, UNLV William S. Boyd School of Law

Andreas Wiebe, Georg-August-Universität Göttingen

Aleš Završnik, University of Ljubljana

Editors

Tina Mizerová, Andrej Krištofík

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 19 | NUMBER 2 | FALL 2025

LIST OF ARTICLES

- Taniya Malik:** Freedom of Internet and State Control: A Case Study on Internet Shutdowns in India.....97
- Zahra Hemmat, Mohammad Mehraeen, Rahmatolloah Fattahi, Farhad Shirani:**
Aligning Iran's Legislation with Sustainable Development Goals: A Topic Modeling Approach.....127
- Tamás Pongó, Renáta Kálmán, Réka Brigitta Szaniszló, Norbert Tribl:**
Oversight Board – An Effective Tool to Protect Free Speech?.....151
- Philippe Prince Tritto, Ilse Carolina Torres Ortega:** Jurists of the Gaps: Large Language Models and the Quiet Erosion of Legal Authority.....179
- Maciej Bujalski:** On the Possible Use of Databases to Secure Receivable Debts...205
- Boldizsár Szentgáli-Tóth, Rudolf Berkes:** Artificial Intelligence in the Service of Parliaments: Some Arguments for the Necessity of a Normative Legal Framework at the European Level.....237
- Dan Jerker B. Svantesson:** Give Realistic Cyber Peace a Chance.....273

LIST OF BOOK REVIEWS

- Jan Hospes:** Bridging the Gap: A Review of Cybersecurity für Manager.....305

DOI 10.5817/MUJLT2025-2-1

FREEDOM OF INTERNET AND STATE CONTROL: A CASE STUDY ON INTERNET SHUTDOWNS IN INDIA

by

TANIYA MALIK *

This study is necessitated by India's abysmal record with internet shutdowns, raising human rights concerns. In the past decade, India has witnessed a surge in internet shutdowns, ostensibly justified on grounds of national security, counterterrorism efforts, maintenance of law and order, and suppression of misinformation. These actions have sparked concerns regarding the violation of constitutionally guaranteed freedoms of speech, expression, and profession. Recognizing the pivotal role of the internet in contemporary society, this study scrutinizes the legal framework surrounding such shutdowns and the permissible grounds of governmental intervention. Through an exhaustive examination of shutdown grounds, frequency, and duration across Indian states and Union Territories (UTs) during 2021-24, this study evaluates their alignment with statutory and judicial directives. Employing both doctrinal and non-doctrinal methodologies, the study interrogates the hypothesis that internet shutdowns in India often transgress mandated guidelines. Findings underscore repeated violation of the established norms at the hands of governmental authorities and stress upon strict adherence to guidelines to curb potential abuses of state authority in implementing internet shutdowns. The study concludes that while India's approach to internet shutdowns provides valuable insights for the global community, it highlights the need for stronger enforcement of legal safeguards to prevent misuse. These lessons can help other nations balance state control with the protection of digital rights.

KEY WORDS

Internet Shutdowns, Freedom of Internet, Freedoms of Speech and Expression, Anuradha Bhasin v. Union of India, Suspension Rules 2017

* Assistant Professor, Indian Law Institute, New Delhi, India. E-mail: maliktaniya@yahoo.co.in

1. INTRODUCTION

The third industrial revolution, also known as the technological or digital revolution, is swiftly revolutionizing the modes of communication employed by contemporary societies.¹ The internet, the massification of personal computers, and the universalization of smartphones are some of its defining characteristics. Before the advent of the internet, only some people could afford to participate in public debates due to the inherently restricting infrastructure of the existing communication channels, such as television, radio, and print media. The Internet platforms broke down this barrier by creating open online communities for user-generated content, published without editorial control and at no cost.² This has significantly boosted engagement in public discussions and the volume of information available.

As the internet is an enabler of free communication, it has become a site of significant conflict, with many countries seeking means to restrict the unrestricted exchange of ideas. Such restrictions are often justified under the premise of upholding law and order or curbing the dissemination of misinformation. However, at times, driven by apprehensions of unfavorable public sentiment or potential protests, governments unjustifiably impose such restrictions on citizens. In this manner, the internet has also become a source of tension, especially when it comes to using state authority to regulate cyberspace and protect digital freedoms. The phenomena of internet shutdowns, which are becoming more commonplace worldwide as governments try to handle internal security concerns and restrict the flow of information, is a clear example of this tension.³

Acknowledging the central role played by the internet in our everyday lives and the unprecedented opportunities it offers for the realisation of human rights, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, in May 2011, had recommended that disconnecting users from Internet access is disproportionate and violative of Article 19 of the UDHR and the ICCPR related to the protection of freedom of speech and expression.⁴ The

¹ Roberto Barroso, L. & van Brussel Barroso, L. (2023) Democracy, Social Media, and Freedom of Expression: Hate, Lies, and the Search for the Possible Truth. *Chicago Journal of International Law*, 24(51). Available from: <https://cjlil.uchicago.edu/print-archive/democracy-social-media-and-freedom-expression-hate-lies-and-search-possible-truth> [Accessed 25 Mar. 2024].

² *Ibid.*

³ Thumfart, J. (2024) Digital Rights and the State of Exception. Internet Shutdowns from the Perspective of Just Securitization Theory, *Journal of Global Security Studies*, 9(1). Available from: <https://academic.oup.com/jogss/article/doi/10.1093/jogss/ogad024/7515068> [Accessed 16 Mar. 2024].

⁴ La Rue, F. (2011) *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, A/HRC/59/50 UN. Available from: <https://primarys>

Rapporteur also called upon all States to ensure that Internet access is maintained at all times, including during times of political unrest.⁵

Internet shutdowns, defined as the intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable for a specific population or within a location.⁶ These shutdowns can vary in scope and intensity. They may involve a complete blackout where no internet services are available (both mobile and broadband), or they may be partial, such as restrictions on mobile data services while broadband remains operational in limited areas. Such Internet blackouts have been reported in various countries, ranging from authoritarian regimes to democratic nations, frequently under the guise of maintaining public order or national security.⁷ These actions raise questions on achieving the proper balance between the right of an individual to information and freedom of speech guaranteed by international human rights law and state sovereignty in preserving security.

India, with its vibrant democracy and status as the world's largest democracy, presents a particularly compelling case study of this global phenomenon. The country has witnessed a significant number of internet shutdowns, particularly in regions experiencing social or political unrest. The duration and scope of these shutdowns can significantly differ, ranging from short-term suspensions lasting a few hours to long-term disruptions extending over several months to years, as was the case in Jammu and Kashmir in 2019-2021. The government often defend these shutdowns on the grounds of national security, combating terrorism, curtailment of spread of misinformation, and preserving law and order. Nonetheless, these shutdowns have a significant impact on citizens' rights, impacting everything from access to information and the fundamental freedoms of speech and expression to emergency services and economic activity.

According to data kept up to date by the Software Freedom Law Center, New Delhi, an impartial group of experts dedicated to protecting the freedom of cyberspace, there have been 788 internet shutdowns⁸ since 2012, with

ources.brillonline.com/browse/human-rights-documents-online/promotion-and-protection-of-all-human-rights-civil-political-economic-social-and-cultural-rights-including-the-right-to-development;hrdhrd99702016149 [Accessed 17 Mar. 2024].

⁵ *Ibid.*

⁶ Ryng, J. et al. (2022) Internet Shutdowns: A Human Rights Issue. *The RUSI Journal*, 167(50). Available from: <https://www.tandfonline.com/doi/full/10.1080/03071847.2022.2156234> [Accessed 17 Mar. 2024].

⁷ De Gregorio, G. & Stremlau, N. (2020) Internet Shutdowns and the Limits of Law. *International Journal of Communication*, 14(1). Available from: <https://papers.ssrn.com/abstract=3622928> [Accessed 17 Mar. 2024].

⁸ SFLC. (2025) *Internet Shutdowns Tracker*. [online] Available from: <https://internetshutdowns.in/> [Accessed 16 Sep. 2023].

the maximum number of shutdowns being ordered in the State of Jammu and Kashmir (433), followed by Rajasthan (100), Manipur (47), & Haryana (38).⁹ According to Access Now, another international non-governmental organization that promotes internet rights, India had the greatest number of internet shutdowns worldwide in 2020.¹⁰ Not only in 2020, but also in previous years, India has demonstrated a dismal record of frequently experiencing internet outages, drawing condemnation and attention from around the globe. In fact, India is frequently referred to as the "internet shutdown capital of the world."¹¹ The figure 1 given below highlights the number of internet shutdowns imposed in India since 2012.¹²

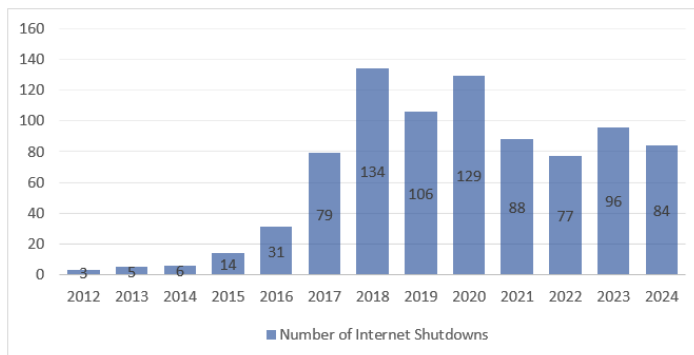


Figure 1: Number of Internet Shutdowns in India 2012 - 2024

The longest internet outage in the nation's history occurred in the State of Jammu and Kashmir in 2019—just before the State's special status was revoked—and lasted for 522 days. The internet shutdown in Jammu and Kashmir primarily affected mobile data services, with some limited restoration of low-speed 2G services after several months. Broadband services were restored gradually in certain areas. Hence, during these extended shutdowns, some internet access may have been available in restricted forms or to specific categories of users (such as government officials or essential services), but the general population experienced severe

⁹ SFLC. (2025) *op. cit.*

¹⁰ Chakravarty, A. (2021) *India Saw Highest Number of Internet Shutdowns in the World in 2020*. [online] India Today. Available from: <https://www.indiatoday.in/technology/news/story/india-saw-highest-number-of-internet-shutdowns-in-the-world-in-2020-1775608-2021-03-04> [Accessed 16 Sep. 2023].

¹¹ Alam, T. (2018) *India Ranks First in Internet Shutdown, UNESCO Shows Concerns*. [online] Entrackr. Available from: <https://entrackr.com/2018/05/internet-shutdown-india-ranks-first/> [Accessed 16 Sep. 2023].

¹² SFLC. (2025) *op. cit.*

limitations. In the case of *Anuradha Bhasin Vs. Union of India*¹³ the Supreme Court considered a challenge to the this excessively long internet shutdown period imposed in the State of Jammu and Kashmir. The court ruled that indefinite internet shutdowns are in violation of constitutional principles and established specific guidelines and principles that the authorities must adhere to when enforcing internet shutdowns.¹⁴

The Internet is the most potent communication tool available in the modern world. Our societies rely heavily on the internet for a variety of purposes, from using social media to conducting banking and corporate operations to getting access to administrative and medical services. From this perspective, any government restriction on internet access amounts to a direct infringement on the fundamental rights as guaranteed by the Indian Constitution, including freedom of speech and expression (Article 19(1)(a)), freedom to practice any profession or to engage in any trade, business, or occupation (Article 19(1)(g)), and right to life (Article 21) and its various positive interpretations, including right to livelihood and right to education (Article 21A). Although it is undeniable that none of the fundamental rights guaranteed by the Indian Constitution are absolute and that the state may impose reasonable restrictions on the exercise of these rights, any action taken by the state that infringes upon a fundamental right must be in agreement with constitutional principles that have been defined and developed with the assistance of Indian judiciary.

1.1. RESEARCH OBJECTIVES

In view of the foregoing, the primary objective of this study is to describe the frequency, reasons, and duration of internet shutdowns that are implemented nationwide in India. After identifying them, the study examines whether these internet shutdowns follow the statutory and judicial principles laid down by the Supreme Court in *Anuradha Bhasin's* case. This landmark judgment by the Supreme Court of India has clarified the constitutional limits on the government's power to suspend internet services. The Supreme Court of India, in particular, is the highest authority for upholding fundamental rights in the country, and its decisions have a significant impact on both individual freedoms and the actions of the government. *Anuradha Bhasin's* case established key legal standards for ensuring the proportionality of government actions, transparency, and the necessity of judicial review when fundamental rights such as freedom of speech and access to the internet are

¹³ *Anuradha Bhasin Vs. Union of India* (2020), 3 SCC 637. Available from: https://main.sci.gov.in/supremecourt/2019/28817/28817_2019_2_1501_19350_Judgement_10-Jan-2020.pdf [Accessed 16 Sep. 2023].

¹⁴ *Ibid.*

restricted. By analyzing this case, the study aims to demonstrate how these judicial principles serve as a safeguard against arbitrary government actions and how they apply to the increasing instances of internet shutdowns in India. The study additionally aims to propose specific measures that could be implemented to stop authorities from abusing their power to impose internet shutdowns. These suggestions will be predicated on the knowledge obtained from the examination of the number, justification, and length of internet shutdowns, as well as the assessment of how well they adhere to the current legal system and judicial norms. By fulfilling these objectives, this study hopes to further the current debate about how to strike an equilibrium in the context of internet shutdowns between protecting individuals' fundamental rights while safeguarding national security.

1.2. RESEARCH METHODOLOGY

This research uses both doctrinal and non-doctrinal research methods in accordance with the study's objectives. The doctrinal methodology has been used to study the legal framework related to imposition of internet shutdowns in India. Primarily, this has been accomplished by carefully examining and evaluating the relevant statutes, procedural rules, and judicial pronouncements. The non-doctrinal method (empirical approach) has been used to examine whether the central or state governments are adhering to the relevant regulations and procedures while issuing directions for internet shutdowns. The purposive sampling technique has been used to identify the most recent internet shutdowns imposed in the various Indian states during 2021, 2022, 2023, and 2024. The issuing authority, reasons, and duration of these internet shutdowns are also recorded. Secondary resources, such as departmental websites, newspaper reports, and official notifications, have been relied upon to collect data.

There are six sections to this study. After introducing the research topic and design in the introductory section, the second section explores internet shutdowns as a global phenomenon, analyzing the key motivations behind their imposition by governments. The third section provides an overview of the statutory, procedural, and judicial guidelines for enforcing internet shutdowns in India. The fourth section of the paper compiles the data related to the nation's most recent and significant internet shutdowns from the years 2021, 2022, 2023, and 2024. The fifth section thoroughly examines the guidelines with the data gathered on internet shutdowns and identifies anomalies committed by authorities while issuing these orders. The sixth section concludes the findings of the study and makes recommendations for improvements.

2. INTERNET SHUTDOWNS: UNDERSTANDING THE GLOBAL CRISIS AND ITS UNDERLYING CAUSES

According to the most recent report from Access Now, a non-profit organization working on digital civil rights, internet shutdowns in 2024 reached an unprecedented scale in terms of frequency and geographic spread, making it the worst year ever for digital blackouts.¹⁵ The scope of these disruptions expanded significantly, with shutdowns affecting more countries, communities, and individuals than in any previous year. Governments increasingly turned to internet shutdowns as a tool for control during critical moments such as protests, elections, and conflicts, resulting in widespread communication disruptions that endangered lives and silenced dissent. The year 2024 witnessed a staggering 296 internet shutdowns across 54 countries—a 9.5% increase from the previous year.¹⁶ Not only did the number of shutdowns rise, but their impact was also more severe, with broader geographic regions and entire nations being plunged into digital darkness. From Myanmar and Bangladesh to India, Pakistan, Iran, and Russia, shutdowns were deployed with alarming regularity, affecting millions and cutting off essential access to information, economic activity, and social services. Figure 2 below gives an overview of the total number of shutdowns imposed globally during the years 2016 to 2024.

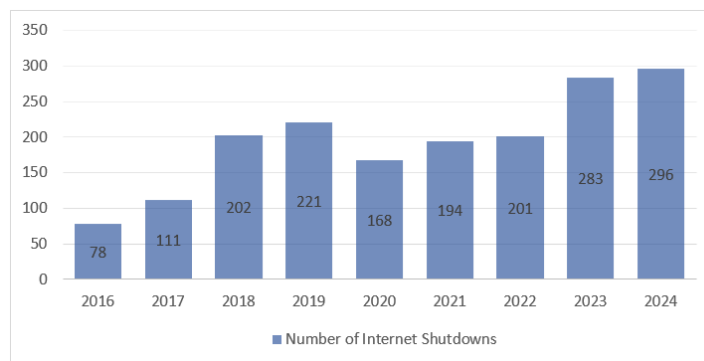


Figure 2: Number of Internet Shutdowns imposed globally during 2016 - 2024

¹⁵ Access Now. (2024) *Emboldened offenders, endangered communities: Internet shutdowns in 2024*. [online] Available from: <https://www.accessnow.org/wp-content/uploads/2025/02/KeepItOn-2024-Internet-Shutdowns-Annual-Report.pdf> [Accessed 12 Jun. 2025].

¹⁶ Access Now. (2024) *op. cit.* p. 5.

In particular, conflicts and protests emerged as significant drivers of shutdowns, with many countries seeing widespread, multi-regional blackouts.¹⁷ What was once a tool reserved for isolated incidents has now evolved into a widespread tactic, used by both democratic and authoritarian regimes. Shutdowns are now also increasingly imposed by foreign actors, such as in the cases of Israel and Russia using digital blackouts as part of military strategies in Gaza and Ukraine, respectively. Some countries, particularly in the Middle East and Africa, are imposing shutdowns during national exams to prevent cheating. In 2024, countries like India, Iraq, Syria, and Algeria continued this practice.¹⁸

This global expansion in the scope of shutdowns also highlights the growing impunity with which governments wield this tool. Despite international frameworks protecting the right to information and communication, authorities cited vague reasons like national security or public safety to justify the shutdowns, while their true motivations often involved silencing opposition, curbing protests, or controlling narratives during electoral cycles. The devastating scope and spread of internet shutdowns in 2024 demonstrated a clear shift in how digital communication is weaponized, with more lives being affected by these disruptions than ever before. The global rise of shutdowns underscores the urgent need for coordinated international action to protect access to the internet as a fundamental human right.

As the global leader in internet shutdowns—though briefly and only marginally overtaken by Myanmar in 2024—India continues to use such measures frequently in response to protests, civil unrest, and national security concerns. This makes India a key jurisdiction for analyzing the reasons behind these shutdowns and the legal and judicial responses aimed at preventing excessive infringement on fundamental rights. Studying India's approach provides important insights into how shutdowns are justified and regulated while balancing public safety with the protection of individual freedoms.

¹⁷ Access Now. (2024) *op. cit.* p. 7.

¹⁸ Access Now. (2024) *op. cit.* p. 9.

3. STATUTORY, PROCEDURAL, AND JUDICIAL GUIDELINES RELATED TO INTERNET SHUTDOWNS IN INDIA

Under the constitutional scheme, India is a federal state comprising twenty-eight (28) states and nine (9) union territories. While states have their own elected governments, Union Territories are either governed directly by the central government or have a limited local government structure, with greater central oversight. The power to impose internet shutdowns in India primarily lies with state governments for their respective regions and with the central government for Union Territories. Further, in the Indian states, the elected state governments are tasked with maintaining law and order (including ordering shutdown of internet services). Meanwhile, in union territories, the central government of India is discharging this obligation. Under both these scenarios, this responsibility of maintaining law and order is passed down orders to key district-level officials in charge of law enforcement, i.e., the district magistrate and the superintendent of the police.¹⁹

The law related to internet shutdowns has undergone transformation in India in the year 2017. Consequently, the current regulatory framework can be divided into two distinct periods: the period preceding 2017 and the period following 2017.

3.1. PRE-2017 INTERNET SHUTDOWN REGULATIONS

Until 2017, internet shutdowns were primarily imposed by the district magistrates under Section 144 of the Code of Criminal Procedure (hereinafter “Cr.P.C”). It is pertinent to note at this juncture that the legislators did not intend to implement internet shutdowns (internet being non-existent!) at the time when Cr.P.C. 1973 was enacted. In essence, section 144 Cr.P.C. lays down a general provision granting broad powers to the district and executive magistrates to pass emergent orders in cases of nuisance or apprehended danger to issue directions to prevent any obstruction, annoyance, or injury to any person lawfully employed, or danger to human life, health or safety, or a disturbance of the public tranquility, or a riot, of an affray.²⁰ Over time, in

¹⁹ Ruijgrok, K. (2022) The Authoritarian Practice of Issuing Internet Shutdowns in India: The Bharatiya Janata Party's Direct and Indirect Responsibility. *Democratization*, 29. Available from: <https://www.tandfonline.com/doi/full/10.1080/13510347.2021.1993826> [Accessed 25 Mar. 2024]. p. 611.

²⁰ *The Code of Criminal Procedure 1973, India*. In: English. S. 144. “Power to issue order in urgent cases of nuisance or apprehended danger. (1) In cases where, in the opinion of a District Magistrate, a Sub-divisional Magistrate or any other Executive Magistrate specially empowered by the State Government in this behalf, there is sufficient ground for proceeding under this section and immediate prevention or speedy remedy is desirable, such Magistrate may, by a written order stating the material facts of the case and served in the manner provided by section 134, direct any person to abstain from

the absence of an alternative appropriate provision, administrators began to utilize Section 144 Cr.P.C. to impose internet shutdowns when they deemed it necessary to safeguard public safety and tranquility.

3.2. POST-2017 INTERNET SHUTDOWN REGULATIONS

As internet shutdowns became increasingly frequent, the central government notified the Temporary Suspension of Telecom Services (Public Emergency and Public Safety) Rules, 2017 (hereinafter "Suspension Rules, 2017") by using the powers conferred by section 7 of the Indian Telegraph Act, 1885. The Indian Telegraph Act of 1885 establishes a broad regulatory framework governing telecommunications in India. Provisions of this colonial-era statute have been modified and adapted to meet the requirements of modern telecommunications.

In contrast to the general provision of Section 144 Cr.P.C., the Suspension Rules, 2017, establish a novel procedure that state agencies must adhere to when implementing internet shutdowns. The "competent authority" may issue a directive to suspend telecommunications services through these newly established regulations. In the case of a Union Territory administered by the Central Government, the Secretary to the Government of India in the Ministry of Home Affairs may issue such a directive; for State Governments, the Secretary to the State Government in charge of the Home Department may do so.²¹ Should the necessary authorization not be obtained from the appropriate competent authority, an officer holding a rank not lower than that of a Joint Secretary to the Central/State Government may issue the directive. However, in such situations, the joint Secretary is obligated to obtain the competent authority's approval within twenty-four hours of issuing the shutdown order.²²

Temporary suspensions of telecommunications services may be mandated under the Suspension Rules, 2017, specifically in cases of "public emergency" or "public safety".²³ However, the rules do not define these two grounds; therefore, the competent authority authorized to impose the shutdowns exercises its subjective judgment regarding the applicability of these grounds.

a certain act or to take certain order with respect to certain property in his possession or under his management, if such Magistrate considers that such direction is likely to prevent, or tends to prevent, obstruction, annoyance or injury to any person lawfully employed, or danger to human life, health or safety, or a disturbance of the public tranquility, or a riot, or an affray...."

²¹ The Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules 2017, SI, TSTSR 2017, India, In: English, r. 2(1).

²² *Ibid.*

²³ The Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules 2017. *op. cit.* r. 2(2), r. 2(5).

However, the competent authority should keep in mind that the of imposing internet shutdowns cannot be exercised lightly as in the case of *Hukam Chand Shyam Lal v. Union of India*,²⁴ the Supreme Court has clarified that the two phrases "public emergency" and "in the interest of the public safety" occurring in Section 5(2) of the Telegraph Act and also the Suspension Rules, 2017, appear to take colour from each other. In this context the court observed that,

*"[I]n the first part of Sub-section (2) of Section 5 of the Telegraph Act, those two phrases occur in association with each other, and the context further clarifies with amplification that a "public emergency" within the contemplation of this Section is one which raises problems concerning the interest of the public safety, the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or the prevention of incitement to the commission of an offence."*²⁵

Therefore, *Hukam Chand Shyam Lal's* case has clarified that the scope of "public emergency" and "public safety" relates to the situations pertaining to "sovereignty and integrity of India, the security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of an offence."

While providing for additional safeguards, the Suspension Rules, 2017, also provide that any order related to the suspension of telecom services, issued by the authorized body, must delineate the rationale behind such action.²⁶ Additionally, to forestall the potential misuse of such powers, the regulations specify that both the Central and State Governments are obligated to establish a review committee.²⁷ This committee is tasked with convening within a timeframe of five working days subsequent to the issuance of directives for the suspension of services and record its finding, as required under Rule 2(6), whether the suspension orders are in accordance with the provisions of the main statute, viz., Section 5(2) of the Telegraph Act, 1885.²⁸

The most recent legal development concerning the suspension of internet services in India is the enactment of the Telecommunications Act, 2023 and subsequent adoption of the Telecommunication (Temporary Suspension of Services) Rules, 2024 (hereinafter "Suspension Rules, 2024"). The legal basis for imposing internet shutdowns in India is now provided under Section 20(2) of the Telecommunications Act, 2023. It authorizes the Central or State

²⁴ *Hukam Chand Shyam Lal v. Union of India* (1976), 2 SCC 128.

²⁵ *Hukam Chand Shyam Lal v. Union of India* (1976), *op. cit.* (n 24) para. 90.

²⁶ The Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules 2017. *op. cit.* r. 2(2).

²⁷ The Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules 2017. *op. cit.* r. 2(2), r. 2(5).

²⁸ The Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules 2017. *op. cit.* r. 2(6)

Government, or their designated officers, to suspend telecommunication services during a *public emergency* or in the interest of *public safety*. Such action must be deemed necessary or expedient to protect the sovereignty and integrity of India, national security, public order, friendly relations with foreign states, or to prevent incitement to offences. Thus, the grounds for imposing internet shutdowns under the Telecommunications Act, 2023, remain substantially the same as those provided under the earlier Indian Telegraph Act, 1885.

The Suspension Rules, 2024 prescribe the procedures and safeguards to be followed while ordering suspension of internet services. These rules formally replace the earlier Suspension Rules, 2017, and were introduced in response to growing legal challenges and public criticism surrounding the opacity and arbitrariness of internet shutdowns.²⁹ Conceptually, the Suspension Rules, 2024 mark a transition from the colonial framework of the Indian Telegraph Act, 1885, to a more contemporary regulatory structure.

Under the new regime, any suspension of telecom services' orders are now required to be published, must clearly articulate the reasons for the suspension, and must be narrowly tailored in scope.³⁰ Specifically, they must address only the stated reasons, apply to a clearly demarcated geographical area, and be time-bound, not exceeding fifteen calendar days at a time.³¹ The rules also mandate that a suspension order may be issued only if the issuing authority is satisfied that the objectives outlined in Section 20(2) of the Telecommunications Act, 2023, cannot be achieved through any other reasonable means. This effectively introduces a test of *necessity*, requiring the authority to consider the availability of less restrictive alternatives before imposing a suspension.³² Additionally, each order must be forwarded to the designated review committee within twenty-four hours of its issuance.³³ Despite these procedural refinements, the substantive framework governing authorized issuing authorities³⁴ and the composition of the review committee³⁵ remains unchanged from the 2017 Rules.

²⁹ These rules came into effect on Nov. 22, 2024.

³⁰ *The Temporary Suspension of Telecommunication Services Rules 2024*, SI, India. In: English, TSTSR 2024, r. 3(2).

³¹ *Ibid.*

³² *The Temporary Suspension of Telecommunication Services Rules 2024. op. cit.* r. 3(5).

³³ *The Temporary Suspension of Telecommunication Services Rules 2024. op. cit.* r. 3(3).

³⁴ *The Temporary Suspension of Telecommunication Services Rules 2024. op. cit.* r. 3(1).

³⁵ *The Temporary Suspension of Telecommunication Services Rules 2024. op. cit.* r. 5.

3.3. JUDICIAL STANCE AND GUIDELINES RELATED TO INTERNET SHUTDOWN

The Indian judiciary's stand and principles with regard to internet shutdowns have been shaped number of landmark cases wherein it has showcased a pragmatic approach when confronted with situations where internet access of the citizens was curtailed without adequate justification. In the case of *Faheema Shirin R. K. v. State of Kerala*,³⁶ the High Court of Kerala held that right to access the internet is considered as a part of freedom of speech and expression under Article 19(1)(a) and cannot be taken away arbitrarily.³⁷ The restriction on the use of mobile phones in a women's dormitory, as was imposed in this case, was deemed by the court to be an unjustifiable violation of the freedom to access the internet, the right to privacy, and the right to an education, all relatable to Arts. 19 and 21 of the Indian Constitution. Similarly in the case of *Banashree Gogoi v. Union of India*,³⁸ the Guwahati High Court criticized the state government for prolonged internet shutdowns and for not restoring the mobile internet services when the normalcy had returned in the state and ordered immediate restoration of the mobile internet services in the state. The court underscored that while internet suspension may be permissible under specific circumstances, it should not persist when conditions no longer warrant it, as internet plays a vital role in modern life.³⁹

Most importantly, the issue of imposition of telecom shutdowns by government authorities has been discussed at length by the three-judge bench of Supreme Court in the case of *Anuradha Bhasin Vs. Union of India*,⁴⁰ while hearing the matter related to the imposition of restrictions on telecommunication services in the backdrop of revocation of the special status of the State of Jammu & Kashmir in 2019. The District Magistrates across the State of J&K, by invoking Section 144 of the Cr.P.C., ordered the suspension of internet, landline, and mobile phone services on August 4, 2019 and thereafter on August 5, 2019, also imposed restrictions on movement and public gatherings of citizens citing concerns about peace and tranquility. Anuradha Bhasin, a journalist, challenged these restrictions on internet access and movement in the Supreme Court under Article 32 of the Indian Constitution, alleging violations of Article 19, particularly regarding freedom of expression and the freedom to practice any profession.

³⁶ *Faheema Shirin R. K. v. State of Kerala* (2020), Ker AIR 35.

³⁷ *Faheema Shirin R. K. v. State of Kerala* (2020), *op. cit.* (n 36) para. 19.

³⁸ *Banashree Gogoi v. Union of India* (2019) Gau SCCOnline 5584.

³⁹ *Banashree Gogoi v. Union of India* (2019), *op. cit.* (n 38) para. 8.

⁴⁰ *Anuradha Bhasin Vs. Union of India* (2020), *op. cit.* (n 13).

The Supreme Court in this case categorically held that,

*“The freedom of speech and expression and the freedom to practice any profession or carry on any trade, business or occupation over the medium of internet enjoys constitutional protection under Article 19(1)(a) and Article 19(1)(g). The restriction upon such fundamental rights should be in consonance with the mandate under Article 19 (2) and (6) of the Constitution, inclusive of the test of proportionality.”*⁴¹

In this case, the court outlined several directions that the government authorities must follow before imposing telecommunications shutdowns. At the outset, the application of the *test of proportionality* is emphasized,⁴² to ensure that the nature and quality of the encroachment on the fundamental freedoms guaranteed under Article 19(1)(a) & (g) of the Indian Constitution is not disproportionate to the purpose for which restrictions are imposed and are not extended beyond necessary duration.⁴³ Secondly, the court mandates the publication of suspension orders to enable affected individuals to challenge them before competent judicial bodies, promoting transparency and thereby avoiding arbitrary shutdowns.⁴⁴ Thirdly, all internet suspension orders are subject to judicial review of the courts to prevent arbitrary shutdowns.⁴⁵ Additionally, such orders must only be passed in extreme circumstances after exploring and assessing alternative measures.⁴⁶ Furthermore, *indefinite suspension of internet services* is deemed *impermissible*, and periodic reviews, as mandated by the Suspension Rules, 2017, are required to prevent prolonged imposition of shutdowns.⁴⁷ These guidelines were passed by the court with the aim to uphold fundamental freedoms while preventing abuse of governmental powers, ensuring transparency and accountability in the process of imposing internet shutdowns.

⁴¹ Anuradha Bhasin Vs. Union of India (2020), *op. cit.* (n 13) para. 152(b).

⁴² Anuradha Bhasin Vs. Union of India (2020), *op. cit.* (n 13) para. 152(d).

⁴³ Anuradha Bhasin Vs. Union of India (2020), *op. cit.* (n 13) para. 68.

⁴⁴ Anuradha Bhasin Vs. Union of India (2020), *op. cit.* (n 13) para. 152(a).

⁴⁵ Anuradha Bhasin Vs. Union of India (2020), *op. cit.* (n 13) para. 152(e).

⁴⁶ Anuradha Bhasin Vs. Union of India (2020), *op. cit.* (n 13) para. 152(d).

⁴⁷ Anuradha Bhasin Vs. Union of India (2020), *op. cit.* (n 13) para. 152(c).

Table 1 below summarizes the key differences in the legal and procedural framework for internet shutdowns in India, providing a comparison between pre-2017, post-2017 regulations, and recent judicial guidelines:

Aspect	Pre-2017 Regulations	2017 Regulations	2024 Regulations	Judicial Stance and Guidelines
Authority Responsible for ordering shutdown of Internet	District Magistrates	Competent Authority (Secretary to the Government of India/State Government in-charge of the Home Department)	Competent Authority (Secretary to the Government of India/State Government in-charge of the Home Department)	The Indian Judiciary (Supreme Court, High Courts) has evolved legal tests and standards that provide for judicial review of internet shutdowns ordered by the Government of India or state governments.
Regulatory Framework	Section 144 of the Code of Criminal Procedure (Cr.P.C.)	Temporary Suspension of Telecom Services (Public Emergency and Public Safety) Rules, 2017	The Temporary Suspension of Telecommunication Services Rules, 2024	Court decisions, particularly guidelines laid down in <i>Anuradha Bhasin's</i> judgment.
Procedure	Imposition based on emergent orders for public safety issued under Section 144 of the Cr.P.C.	Established procedure under the Suspension Rules, 2017	Introduced additional safeguards, including mandatory publication of the suspension order, a clear statement of reasons, specification of the affected geographical area, and a maximum duration limit of fifteen days at a time (extension is possible).	Application of proportionality test, publication of orders, judicial review, exploration of alternatives, periodic reviews, prevention of indefinite suspensions.
Criteria for Shutdowns	Broad powers to prevent obstruction, annoyance, or injury to public	Grounds of "public emergency" or "public safety" defined subjectively.	Grounds of "public emergency" or "public safety" defined subjectively. The authority additionally to consider the availability of alternative measures (test of necessity).	Grounds of "public emergency" or "public safety", to ensure proportionality and necessity.
Oversight Mechanism	-	Establishment of review committees	Establishment of review committees	Judicial review and oversight.

Table 1: Statutory, procedural, and judicial guidelines related to internet shutdowns in India

4. EMPIRICAL FINDINGS OF INTERNET SHUTDOWNS IMPOSED DURING 2021-2024

This section of the paper, employing a purposive sampling technique, aims to identify the grounds, issuing authority, and approximate duration for which government authorities ordered internet shutdowns in India in 2021-24. This inquiry will provide a thorough understanding of the patterns and causes of internet shutdowns in India in the recent past.

According to statistics, the State of Jammu and Kashmir experienced the longest internet blackout in 2019 when the President of India repealed Article 370 of the Constitution, which granted the state special status. It was imposed on August 5, 2019, and was a preventive shutdown to avoid crippling of law and order situation in the state. In the intervening period, limited internet connectivity in the form of 2G services was restored in some regions. The erstwhile state regained 4G connectivity on February 6, 2021, after 552 days of no to low internet.⁴⁸

The second longest internet shutdown was ordered in the North-Eastern state of Manipur on May 3, 2023, after an unprecedented ethnic violence erupted in the state between the Meitei people, a majority that lives in the Imphal Valley, and the Kuki-Zo tribal community from the surrounding hills.⁴⁹ The shutdown was deemed necessary by the state government to curb spread of misinformation and maintain peace. On July 7, 2023, the High Court of Manipur intervened, ordering limited restoration of internet services via broadband connections and white-listing select mobile numbers.⁵⁰ The government partially lifted shutdown orders on December 3, 2023, limiting them to areas affected by violence; this marked the end of Manipur's longest shutdown of 2023.⁵¹

⁴⁸ Rajvanshi, A. (2023) *How Internet Shutdowns Wreak Havoc in India*. [online] TIME. Available from: <https://time.com/6304719/india-internet-shutdowns-manipur/> [Accessed 25 Mar. 2024].

⁴⁹ The Hindu Bureau. (2024) *Longest Internet Shutdown in 2023 Took Place in Manipur amidst Human Rights Violations: Report*. [online] The Hindu. Available from: <https://www.thehindu.com/sci-tech/technology/longest-internet-shutdown-2023-took-place-manipur-amidst-human-rights-violations-report/article67726259.ece> [Accessed 25 Mar. 2024].

⁵⁰ Lakshman, A. (2023) *Lift Ban on Internet Services with Safeguards: Manipur High Court Directs State Government*. [online] The Hindu. Available from: <https://www.thehindu.com/news/national/other-states/manipur-high-court-orders-home-department-to-lift-the-ban-on-providing-internet-through-internet-lease-line/article67056929.ece> [Accessed 25 Mar. 2024].

⁵¹ Shirin, B. (2023) *Internet Ban Lifted in Violence-Hit Manipur, Restrictions in Border Areas till Dec 18*. [online] India Today. Available from: <https://www.indiatoday.in/india/story/manipur-violence-internet-services-restored-border-areas-exception-meiteis-kukis-2471548-2023-12-04> [Accessed 25 Mar. 2024].

Broadly speaking, the internet shutdowns imposed in India by the individual states can be characterized into two categories – preventive and reactive. The first of the categories is *preventive shutdowns* i.e., shutdowns imposed in anticipation of an event or to prevent an untoward incident which may require internet to be suspended by authorities. The second category is of *reactive shutdowns* i.e., those shutdowns that are imposed in the aftermath of an event, in order to contain a law and order situation. The table 2 given below gives details of few of the internet shutdowns imposed in the recent past identified through the purposive sampling method.

Date	Duration	State/District	Reason	Issuing Authority	Category
Nov 16, 2024	21 Days	Manipur / Nine districts of Imphal West, Imphal East, Bishnupur, Thoubal, Kakching, Jiribam, Churachandpur, Kangpokpi and Pherzawl.	Ethnic violence between the Meitei and the Kuki-Zo community followed by recovery of six bodies from the Jiri and Barak rivers.	Home Department, Government of Manipur ⁵²	Reactive
Sept 21–22, 2024	5 Hours on 2 Days	Jharkhand / Statewide	To prevent unfair practices in the Jharkhand General Graduate Level Combined Competitive Examination 2024.	Department of Home, Prison and Disaster Management, Government of Jharkhand ⁵³	Preventive
Feb 11, 2024	13 Days	Haryana / Seven Districts of Ambala, Kurukshetra, Kaithal, Jind, Hisar, Fatehabad, and Sirsa	Amid the call by farmers' unions from Punjab and Haryana to protest in Delhi.	Addl. Chief Secretary, Home Department of the State of Haryana ⁵⁴	Preventive
May 3, 2023	212 Days	Manipur / Statewide – extended from two districts Churachandpur and Pherzawl.	Ethnic violence and communal clashes between the Meitei people and the Kuki-Zo tribal community.	Home Department, Government of Manipur ⁵⁵	Reactive

⁵² News Desk. (2024) *Government lifts mobile internet ban in nine districts after 3 weeks*. [online] The Times of India. Available from: <https://timesofindia.indiatimes.com/india/manipur-government-lifts-mobile-internet-ban-in-nine-districts-after-3-weeks/articleshow/116146794.cms> [Accessed 16 Jun. 2025].

⁵³ News Desk. (2024) *Jharkhand suspends mobile internet to check malpractice during exam*. [online] The Times of India. Available from: <https://timesofindia.indiatimes.com/india/jharkhand-suspends-mobile-internet-to-check-malpractice-during-exam-all-you-need-to-know/articleshow/113539597.cms> [Accessed 16 Jun. 2025].

⁵⁴ News Desk. (2024) *Farmer's protest: Haryana govt extends internet suspension in seven districts till Feb 23*. [online] ANI News. Available from: <https://www.aninews.in/news/national/politics/farmers-protest-haryana-govt-extends-internet-suspension-in-seven-districts-till-feb-2320240222014847/> [Accessed 16 Jun. 2025].

⁵⁵ The Hindu Bureau. (2024) *op. cit.*

Date	Duration	State/District	Reason	Issuing Authority	Category
Dec 10, 2022	3 Hours	West Bengal / Uttar Dinajpur, Malda, Murshidabad, Purba Medinipur, Paschim Medinipur and Dakshin Dinajpur	To prevent cheating in TET examination 2022 being conducted for the recruitment of assistant teachers.	Home and Hill Affairs Department, Government of West Bengal ⁵⁶	Preventive
Nov 22, 2022	48 Hours	Meghalaya / West Jaintia Hills, East Jaintia Hills, East Khasi Hills, Ri-Bhoi, Eastern West Khasi Hills, West Khasi Hills, and South West Khasi Hills	To maintain law and order situation after reports of violence and arson occurring on Assam–Meghalaya border.	Home (Police) Department, Government of Meghalaya ⁵⁷	Reactive
Oct 11, 2022	6 Hours	J&K / Srinagar (within 6 km radius of Bushpora area)	To avoid law and order situation after death of Althaf Ahmad Shah, son-in-law of Late Syed Ali Shah Geelani.	Originally issued by ADGP (Kashmir Zone), subsequently confirmed by Home Department, J&K ⁵⁸	Preventive
Oct 10, 2022	16.5 Hours	J&K / Anantnag	To maintain law and order situation after encounter between security forces and the terrorists in Tangpawa area of district Anantnag.	Originally issued by ADGP (Kashmir Zone), subsequently confirmed by Home Department, J&K ⁵⁹	Reactive
Aug 21, 2022 and Aug 28, 2022	4 Hours	Assam / Twenty-five out of thirty-one districts of Assam	To prevent cheating in examinations conducted for Grade III and Grade IV government posts.	Home and Political Department, Government of Assam ⁶⁰	Preventive

⁵⁶ Home and Hill Affairs Department. (2022) *Temp Internet shutdown Order icw TET Examination 2022 on 11th December (Govt. of WB, Dec. 10, 2022)*. [online] Available from: <http://home.wb.gov.in/notice/temp-internet-shutdown-order-icw-tet-exam-1670681143.pdf> [Accessed 29 May 2024]

⁵⁷ Home (Police) Department. (2022) *Temporary Suspension of Mobile Internet / Data Services of all mobile service providers in 7 (seven) districts of Meghalaya (Govt. of Meghalaya, Nov. 22, 2022)*. [online] Available from: https://meghalaya.gov.in/sites/default/files/circulars/HPL_199_2018_31.pdf [Accessed 29 May 2024]

⁵⁸ Home Department. (2022) *Temporary suspension of Internet Services-confirmation (UIT of J&K, Oct 11, 2022)*. [online] Available from: [https://jkhome.nic.in/pdf/48\(TSTS\)of2022.pdf](https://jkhome.nic.in/pdf/48(TSTS)of2022.pdf) [Accessed 29 May 2024]

⁵⁹ Home Department. (2022) *op. cit.*

⁶⁰ Bapat, K. (2022) *Gauhati HC Decision on Internet Shutdown in Assam*. [online] Internet Freedom. Available from: <https://internetfreedom.in/guahati-hc-refuses-to-restrain-the-government-of-assam-from-suspending-internet-services/> [Accessed 25 Mar. 2024].

Date	Duration	State/District	Reason	Issuing Authority	Category
May 25, 2022	6 Days	Andhra Pradesh / Amalapuram town in Konaseema district	The shutdown was imposed in response to protests opposing the decision of the Andhra Pradesh state government to rename Konaseema District as Dr. B R Ambedkar Konaseema district.	Section 144 Cr.P.C. / Orders not available online / reported in newspapers ⁶¹	Reactive
Oct 27, 2021	4 Hours	Rajasthan / Jaipur, Bharatpur, Bikaner, Sawai, Hanumangarh, Madhopur and Ajmer	To prevent cheating in RAS prelims Exam 2021.	Divisional Commissioners, Police Commissionerate ⁶²	Preventive
Oct 24, 2021	2 Days	J&K / Zainapora Belt of district Shopian	After the killing of a civilian in Babapora Zainapora.	Orders not available online / reported in newspapers ⁶³	Reactive
Oct 23, 2021	12 Hours	Rajasthan / Jaipur and Dausa	In order to curb the spread of fake news, rumours and prevent question paper leakage during the conduct of the Patwari Direct Recruitment Examination-2021.	Jaipur Divisional Commissioner ⁶⁴	Preventive
Oct 18, 2021	1 Day	J & K / Parts of Srinagar District	After the killing of civilians in the Srinagar by terrorists.	Orders not available online / reported in newspapers ⁶⁵	Preventive
Oct 06, 2021	7 Days	Chhattisgarh / Kawardha District	On account of communal tensions between two religious groups.	District Collector ⁶⁶	Reactive

⁶¹ Software Freedom Law Center. (2022) *7 Day Long internet shutdown in Andhra Pradesh in violation of Supreme Court of India Guidelines: RTI Response*. [online] Available from: <https://sflc.in/7-day-long-internet-shutdown-andhra-pradesh-violation-supreme-court-india-guidelines-rti-response/> [Accessed 25 Mar. 2024].

⁶² TNN. (2021) *Internet Shutdown in Rajasthan: Mobile Internet Suspended for RAS Prelims Exam across Rajasthan Today*. [online] The Times of India. Available from: <https://timesofindia.indiatimes.com/city/jaipur/mobile-net-suspended-for-ras-prelims-exam-across-raj-today/articleshow/87290703.cms> [Accessed 16 Sep. 2023].

⁶³ News Desk. (2021) *Internet Suspended for Second Day in South Kashmir's Zainapora Belt*. [online] The Kashmir Valla. Available from: <https://thekashmirwalla.com/internet-suspended-for-second-day-in-south-kashmirs-zainapora-belt/> [Accessed 16 Sep. 2023].

⁶⁴ TNN. (2021) *Patwari Exam: Mobile Internet Banned in Jaipur, Dausa till 6pm*. [online] The Times of India. Available from: <https://timesofindia.indiatimes.com/city/jaipur/patwari-exam-mobile-net-banned-in-jaipur-dausa/articleshow/87214485.cms> [Accessed 16 Sep. 2023].

⁶⁵ Wani, A. (2021) *Mobile Internet Services Suspended in Parts of Kashmir as Precautionary Measure*. [online] India Today. Available from: <https://www.indiatoday.in/india/story/internet-services-jammu-kashmir-districts-terror-attacks-1866205-2021-10-18> [Accessed 16 Sep. 2023].

⁶⁶ John, J. (2021) *Chhattisgarh: Internet Suspended in 3 Districts after Two Groups Clash, Curfew Imposed in Kawardha*. [online] The Times of India. Available from: <https://timesofindia.indiatimes.com/city/raipur/chhattisgarh-communal-clashes-internet->

Date	Duration	State/District	Reason	Issuing Authority	Category
Oct 3, 2021	2 Days	Uttar Pradesh / Lakhimpur Kheri and Sitapur Districts	Over violence resulting during farmers protest which resulted in the death of eight including four protesting farmers.	Orders not available online / reported in newspapers ⁶⁷	Reactive
Sept 27, 2021	6 Hours	Rajasthan / Alwar, Dausa, Jaipur, Jhunjhunu and Sikar Districts	On the eve of the Rajasthan Eligibility Examination for Teachers (REET), 2021, internet was suspended to prevent any deterioration of law and order situation due to fake news, rumours of accidents, paper leak etc.	Divisional Commissioners ⁶⁸	Preventive
Sept 06, 2021	24 Hours	Haryana / Karnal, Kaithal, Jind, Kurukshetra and Panipat Districts	In the wake of the farmers' protest against the August 28 police lathi-charge.	Addl. Chief Secretary, Home Department of the State of Haryana ⁶⁹	Preventive
Sept 02, 2021	5-6 Days	J & K / Kashmir Valley	Internet was shut down as a precautionary measure after the death of separatist leader Mr. Syed Ali Geelani.	Orders not available online / reported in newspapers ⁷⁰	Preventive

Table 2: Internet shutdowns imposed during 2021-2024

Upon reviewing the data above, it appears that internet shutdowns in Indian states arise from various circumstances, including communal tensions, widespread protests, fears or actual outbreaks of violence, the impasse between security forces and terrorists, and measures to prevent examination cheating. Although the imposition of internet shutdowns is warranted when a situation showing grave danger to the maintenance of law and order has arisen, there are situations in which to preserve law and order; it is dubious

services-suspended-in-3-districts-curfew-imposed-in-kawardha/article/86804843.cms [Accessed 16 Sep. 2023].

⁶⁷ News Desk. (2021) *Uttar Pradesh: Internet Services Shut in Lakhimpur Kheri, Sitapur*. [online] The Mid-Day. Available from: <https://www.mid-day.com/news/india-news/article/uttar-pradesh-internet-services-shut-in-lakhimpur-kheri-sitapur-23195427> [Accessed 16 Sep. 2023].

⁶⁸ Khan, H. (2021) *Rajasthan Shuts Internet as 16 Lakh Appear for REET 2021*. [online] The Indian Express. Available from: <https://indianexpress.com/article/jobs/rajasthan-shuts-down-internet-as-16-lakh-sit-for-teacher-exam-7536304/> [Accessed 16 Sep. 2023].

⁶⁹ News Desk. (2021) *Internet Shutdown in Five Haryana Districts Ahead of Farmers' Protest*. [online] The Tribune. Available from: <https://www.tribuneindia.com/news/haryana/internet-shutdown-in-five-haryana-districts-ahead-of-farmers-protest-307753> [Accessed 16 Sep. 2023].

⁷⁰ News Desk. (2021) *Curfew-like Curbs Imposed in Kashmir, Internet Shut as Separatist Leader Geelani Buried in Srinagar*. [online] News18. Available from: <https://www.news18.com/news/india/syed-ali-geelani-death-separatist-leader-buried-kashmir-srinagar-pakistan-internet-shut-curfew-4155038.html> [Accessed 16 Sep. 2023].

whether such measures should be utilized to administer examinations or prevent cheating. Further, an examination of the data above indicates that the duration of the internet shutdowns can fluctuate significantly, ranging from a few hours to several days, weeks, months, or even years, contingent upon the severity of the circumstances. The subsequent section analyses specific irregularities that were identified during the process of issuing internet suspension orders in India.

5. INTERNET SHUTDOWN ORDERS VIS-A-VIS COMPLIANCE WITH STATUTORY LAW AND THE SUPREME COURT GUIDELINES

This section seeks to determine whether the central and state government authorities are adhering to statutory and judicial directives when implementing internet shutdowns. Listed below are some of the most egregious irregularities observed in the manner of notification of internet suspension orders:

5.1. MECHANICALLY ISSUED ORDERS LACKING EVIDENT APPLICATION OF MIND

A perusal of the internet shutdown orders issued in the State of Rajasthan in 2021⁷¹ reflect non-application of mind by the concerned authorities. The Divisional Commissioners have issued three identical internet shutdown orders, following the same template, for preventing cheating during state-level examinations. Such mechanical orders display a lack of proper examination and consideration of specific circumstances and factors involved in each case, necessitating the suspension of internet services. The standard practice followed is that the bureaucrats have recommended suspensions based on "law and order" concerns, without justifications. This contradicts Supreme Court guidelines, which require them to adhere to the *proportionality test* and explain why the internet shutdown is necessary, unavoidable and the least intrusive remedy in the situation at hand.

5.2. NON-COMPLIANCE WITH SUSPENSION RULES, 2017: ORDERS ISSUED BY INCOMPETENT AUTHORITIES, WITHHELD FROM PUBLICATION, OR LACKING PROCEDURAL SAFEGUARDS

As per the Suspension Rules, 2017, the internet shutdown orders can be issued by the Secretary to the Government of India in the Ministry of Home Affairs in the case of Central Government and the Secretary to the

⁷¹ News Desk. (2021) Internet Suspended for Second Day in South Kashmir's Zainapora Belt. *op. cit.*; Wani, A. (2021) *op. cit.* and News Desk. (2021) Internet Shutdown in Five Haryana Districts Ahead of Farmers' Protest. *op. cit.*

State Government in-charge of the Home Department in the case of a State Government. A perusal of the various internet shutdown orders in the preceding section, particularly in the states of Rajasthan, Chattisgarh & J&K in the year 2021⁷², reveals that at times internet shutdown orders are not being issued by the competent authorities and are many a times untraceable on the state government/departmental websites. The non traceability of the internet shutdown orders is particularly worrisome as it undermines the right of the citizens to move the courts of law in case of an alleged infringement of fundamental rights guaranteed under Arts. 19(1)(a) & (g) of the Indian Constitution and impedes judicial scrutiny of the orders to avoid imposition of arbitrary internet shutdowns. Further, in the case of Manipur, where internet shutdown orders were imposed following the outbreak of ethnic violence in May 2023 and remained in effect for 212 days, the procedural safeguard mandated under the Telecom Suspension Rules—the constitution of a Review Committee chaired by the State’s Chief Secretary to evaluate the legality of such orders—appears to have been bypassed. There is no public record indicating that this committee was ever convened or that it reviewed any of the successive shutdown orders issued by the Manipur Home Department.⁷³

5.3. ORDERS ISSUED ON TRIVIAL GROUNDS, SUCH AS PREVENTING CHEATING DURING STATE-LEVEL EXAMINATIONS

A perusal of the various internet shutdown orders, particularly in the states of Assam, Rajasthan & West Bengal,⁷⁴ reveal that internet shutdown orders are being regularly issued on the pretext of avoidance of cheating and paper leak in various state level examinations. This trend is especially concerning due to the fact that the imposition of internet outages for examination administration is excessively disproportionate and violates the Supreme Court’s *test of proportionality*. As these orders severely restrict fundamental liberties protected by Articles 19(1)(a) and (g), they should only be issued under the most extraordinary conditions.

⁷² News Desk. (2021) Internet Suspended for Second Day in South Kashmir’s Zainapora Belt. *op. cit.*; TNN. (2021) *op. cit.*; Wani, A. (2021) *op. cit.*; John, J. (2021) *op. cit.*; News Desk. (2021) Uttar Pradesh: Internet Services Shut in Lakhimpur Kheri, Sitapur. *op. cit.*; News Desk. (2021) Internet Shutdown in Five Haryana Districts Ahead of Farmers’ Protest. *op. cit.*

⁷³ Singh, T. & Waghere, P. (2023) *Statement: 100 Days of Manipur’s Ongoing Illegal Internet Shutdown & Violation of Fundamental Rights*. [online] Internet Freedom Foundation. Available from: <https://internetfreedom.in/manipur-100-days-internet-shutdown/> [Accessed 16 Jun. 2025].

⁷⁴ Home (Police) Department. (2022) *op. cit.*; Software Freedom Law Center. (2022) *op. cit.*; News Desk. (2021) Internet Suspended for Second Day in South Kashmir’s Zainapora Belt. *op. cit.*; Wani, A. (2021) *op. cit.* and News Desk. (2021) Internet Shutdown in Five Haryana Districts Ahead of Farmers’ Protest. *op. cit.*

In the case of Jharkhand, where internet services were suspended to prevent unfair practices during the Jharkhand General Graduate Level Combined Competitive Examination 2024⁷⁵, the matter was brought before the Jharkhand High Court.⁷⁶ In its order dated September 22, 2024, the Court set aside the state government's decision to impose a blanket suspension of all internet services across the state. It held that the stated grounds—namely, "public interest", "adequate safety of students", and "ensuring fair examination"—lacked factual substantiation and were insufficient to justify such a broad restriction.⁷⁷ The Court further observed that while the initial suspension order of the state government was limited in scope and duration, the subsequent modification expanding it to include broadband and fixed-line services amounted to an overreach. Reaffirming that access to the internet is essential to the exercise of fundamental rights under Article 19 of the Constitution, the Court directed that no further suspensions in connection with examinations be carried out without its prior approval for the duration of the proceedings.⁷⁸

It is submitted that in a country like India, which is over a billion people strong, the conduct of examinations should not be seen as such an emergent situation which necessitates shutdown of internet services. Moreover, in case every state in the nation were to adopt this practice, the frequency of internet outages would escalate to a level that would be beyond control. Hence, it is imperative that competent authority must explore alternative measures prior to implementing internet service interruptions for examination purposes.

6. CONCLUSION AND SUGGESTIONS

Just as Gutenberg's printing press had helped to spread the liberal and scientific ideas in Europe during the age of Reformation, the Internet also has the potential to support the respect, protection and implementation of all human rights for people worldwide. In this quest, the freedom of expression becomes a crucial enabling right. There are, however, difficulties in preserving freedom of expression on the internet. Traditionally, as the human right to freedom of expression is often has been used state authorities, the later are inclined to censor or control the freedom of speech and expression. Internet shutdowns are one such control mechanisms employed by the governments to control freedom of internet. The imposition of internet

⁷⁵ News Desk. (2024) Farmer's protest: Haryana govt extends internet suspension in seven districts till Feb 23. *op. cit.*

⁷⁶ *Rajendra Krishna Vs. State of Jharkhand* (2024) SCC OnLine Jhar 3349.

⁷⁷ *Rajendra Krishna Vs. State of Jharkhand* (2024) *op. cit.* para 18.

⁷⁸ *Ibid.*

shutdowns not only disrupts the normal functioning of society but also impinges upon the democratic ethos of the nation.

Through this study, the author has attempted to highlight the human rights challenges posed by imposition internet shutdowns in India. Particularly, it has emphasized the importance of preserving freedom of Internet, as the right to access information and the right to freedom of speech and expression have become increasingly intertwined with internet access. The findings of this study suggest that many internet shutdown orders have been imposed by central and state governments during the period 2021-24 without adhering to statutory, procedural, and judicial guidelines. The analysis of various internet shutdown orders revealed glaring anomalies, including mechanical issuance of orders without proper application of mind, issuance of orders by unauthorized individuals, bypassing procedural safeguards, and the imposition of shutdowns for relatively minor concerns such as exam-related issues.

India's adoption of the Suspension Rules, 2024, represents a formal upgrade to the legal framework governing internet shutdowns. However, the 2024 Rules fall short of addressing several critical deficiencies that plagued the earlier Suspension Rules, 2017, limiting their practical effectiveness. While the new framework introduces procedural improvements, such as clearer structuring of suspension orders and the requirement to consider the availability of alternative measures, significant weaknesses persist. The Review Committee continues to function as an opaque, internal body lacking judicial or independent representation. The absence of a mandate for real-time publication of shutdown orders undermines transparency and restricts access to timely legal remedies. Moreover, the lack of any penalty for misuse enables authorities to issue suspension orders on questionable grounds without accountability. Without robust enforcement, independent oversight, and mechanisms for redress, the 2024 Rules risk serving as a cosmetic reform. A rights-based framework, grounded in transparency, necessity, and proportionality, is essential if digital access is to be meaningfully protected as a constitutional right rather than administered as a discretionary privilege.

In order to prevent abuse of the process, it is imperative that the centre and state governments must comply with the statutory, procedural and judicial guidelines, particularly the ones laid down in *Anuradha Bhasin's* judgment in letter and spirit. In particular, the centre and state governments must adhere to the test of proportionality, and impose internet shutdown only as a last resort. Indefinite internet shutdown orders are specifically prohibited and the governments must proactively publish all internet shutdown orders of the

state on the home department's official website in real time and also widely disseminate the orders information through various means of the media. Additionally, the central and state governments need to make sure that the orders for internet shutdowns are given by the competent authorities and are not issued in a robotic fashion; rather, the orders need to be well-reasoned and demonstrate the application of the competent authority's judgment. It is submitted that the implementation of internet shutdown orders under the guise of averting cheating during examinations should be strongly discouraged. Instead, the authorities must implement measures for stricter invigilation by using the latest technology, such as surveillance cameras and proctoring software. Simultaneously, it is the responsibility of the central and state governments to ensure the prompt appointment of a Review Committee and to facilitate the obligatory evaluation of any existing suspension order and any extension orders, if applicable, in accordance with the strictly defined guidelines laid down in *Anuradha Bhasin's* ruling. Strict compliance with these guidelines will prevent arbitrary suspension of internet services in the country in the long run.

At the same time, India's legal, regulatory, and judicial approach to internet shutdowns offers important lessons for other countries, presenting both advantages and areas for improvement. The transition from using Section 144 of the Cr.P.C. to the more specific *Suspension Rules, 2024* reflects a move towards a more structured and transparent legal framework. This shift highlights the necessity of modern legal standards for managing shutdowns, ensuring clarity on the permissible grounds for such actions. The *Anuradha Bhasin case* further emphasized the importance of judicial oversight, introducing safeguards like the *proportionality test* to ensure shutdowns are used only when absolutely necessary and for a limited time. The judiciary's role in reviewing shutdowns and ensuring they comply with constitutional principles, such as the rights to free speech and profession, offers a robust system for protecting fundamental rights. Further, India's requirement for review committees (established under the *Suspension Rules, 2017 & 2024*) to assess the legality and necessity of internet shutdowns serves as a check against misuse. Other countries should implement similar review processes to hold authorities accountable and prevent the unwarranted use of shutdowns.

India's approach also reveals significant challenges. One major issue is the frequent overreach in the use of internet shutdowns, particularly when imposed for relatively minor concerns like preventing cheating during exams. Such actions show how shutdowns can be misused, violating the principle of proportionality. Furthermore, transparency remains a concern,

as shutdown orders are often not published or explained in detail, limiting public scrutiny and legal recourse.

Overall, India's experience offers both positive frameworks for managing shutdowns—through judicial review, proportionality, and modernized regulations—and lessons in avoiding misuse through better enforcement of transparency, accountability, and limitations on shutdowns for trivial reasons. Other countries can benefit from adopting India's legal safeguards while addressing the gaps seen in practice.

Ultimately, democratic systems across the world must foster societies that uphold the values of accountability, transparency, and adherence to the rule of law. By prioritizing the protection of fundamental liberties and upholding the Constitution's ethos, democracies can ensure that the digital age remains an era of progress, innovation, and inclusivity for all its citizens.

LIST OF REFERENCES

- [1] Access Now. (2024) *Emboldened offenders, endangered communities: Internet shutdowns in 2024*. [online] Available from: <https://www.accessnow.org/wp-content/uploads/2025/02/KeepItOn-2024-Internet-Shutdowns-Annual-Report.pdf> [Accessed 12 Jun. 2025].
- [2] Alam, T. (2018) *India Ranks First in Internet Shutdown, UNESCO Shows Concerns*. [online] Entrackr. Available from: <https://entrackr.com/2018/05/internet-shutdownindia-ranks-first/> [Accessed 16 Sep. 2023].
- [3] *Anuradha Bhasin Vs. Union of India* (2020), 3 SCC 637. Available from: https://main.sci.gov.in/supremecourt/2019/28817/28817_2019_2_1501_19350_Judgement_10-Jan-2020.pdf [Accessed 16 Sep. 2023].
- [4] *Banashree Gogoi v. Union of India* (2019), Gau SCCOnline 5584.
- [5] Bapat, K. (2022) *Gauhati HC Decision on Internet Shutdown in Assam*. [online] Internet Freedom. Available from: <https://internetfreedom.in/guwahati-hc-refuses-to-restraint-the-government-of-assam-from-suspending-internet-services/> [Accessed 25 Mar. 2024].
- [6] Chakravarty, A. (2021) *India Saw Highest Number of Internet Shutdowns in the World in 2020*. [online] India Today. Available from: <https://www.indiatoday.in/technology/news/story/india-saw-highest-number-of-internet-shutdowns-in-theworld-in-2020-1775608-2021-03-04> [Accessed 16 Sep. 2023].
- [7] De Gregorio, G. & Strelau, N. (2020) Internet Shutdowns and the Limits of Law. *International Journal of Communication*, 14(1). Available from: <https://papers.ssrn.com/abstract=3622928> [Accessed 17 Mar. 2024].
- [8] *Faheema Shirin R. K. v. State of Kerala* (2020), Ker AIR 35

- [9] Home (Police) Department. (2022) *Temporary Suspension of Mobile Internet / Data Services of all mobile service providers in 7 (seven) districts of Meghalaya* (Govt. of Meghalaya, Nov. 22, 2022). [online] Available from: https://meghalaya.gov.in/sites/default/files/circulars/HPL_199_2018_31.pdf [Accessed 29 May 2024].
- [10] Home and Hill Affairs Department. (2022) *Temp Internet shutdown Order icw TET Examination 2022 on 11th December* (Govt. of WB, Dec. 10, 2022). [online] Available from: <http://home.wb.gov.in/notice/temp-internet-shutdown-order-icw-tet-exam1670681143.pdf> [Accessed 29 May 2024].
- [11] Home Department. (2022) *Temporary suspension of Internet Services-confirmation (UT of J&K, Oct 11, 2022)*. [online] Available from: [https://jkhome.nic.in/pdf/48\(TSTS\)of2022.pdf](https://jkhome.nic.in/pdf/48(TSTS)of2022.pdf) [Accessed 29 May 2024].
- [12] *Hukam Chand Shyam Lal v. Union of India* (1976), 2 SCC 128.
- [13] John, J. (2021) *Internet Suspended in 3 Districts after Two Groups Clash, Curfew Imposed in Kawardha*. [online] The Times of India. Available from: <https://timesofindia.indiatimes.com/city/raipur/chhattisgarh-communal-clashes-internet-services-suspended-in-3-districts-curfew-imposed-in-kawardha/articleshow/86804843.cms> [Accessed 16 Sep. 2023].
- [14] Khan, H. (2021) *Rajasthan Shuts Internet as 16 Lakh Appear for REET 2021*. [online] The Indian Express. Available from: <https://indianexpress.com/article/jobs/rajasthan-shuts-down-internet-as-16-lakh-sit-for-teacher-exam-7536304/> [Accessed 16 Sep. 2023].
- [15] La Rue, F. (2011) *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, A/HRC/59/50 UN. Available from: <https://primarysources.brillonline.com/browse/human-rights-documents-online/promotion-and-protection-of-all-human-rights-civil-political-economicsocial-and-cultural-rights-including-the-right-to-development;hrdhrd99702016149> [Accessed 17 Mar. 2024].
- [16] Lakshman, A. (2023) *Lift Ban on Internet Services with Safeguards: Manipur High Court Directs State Government*. [online] The Hindu. Available from: <https://www.thehindu.com/news/national/other-states/manipur-high-court-orders-home-department-to-lift-the-ban-on-providing-internet-through-internet-lease-line/article67056929.ece> [Accessed 25 Mar. 2024].

- [17] News Desk. (2021) *Curfew-like Curbs Imposed in Kashmir, Internet Shut as Separatist Leader Geelani Buried in Srinagar*. [online] News18. Available from: <https://www.news18.com/news/india/syed-ali-geelani-death-separatist-leader-buried-kashmirsrinagar-pakistan-internet-shut-curfew-4155038.html> [Accessed 16 Sep. 2023].
- [18] News Desk. (2021) *Internet Shutdown in Five Haryana Districts Ahead of Farmers' Protest*. [online] The Tribune. Available from: <https://www.tribuneindia.com/news/haryana/internet-shutdown-in-five-haryana-districts-ahead-of-farmersprotest-307753> [Accessed 16 Sep. 2023].
- [19] News Desk. (2021) *Internet Suspended for Second Day in South Kashmir's Zainapora Belt*. [online] The Kashmir Valla. Available from: <https://thekashmirwalla.com/internetsuspended-for-second-day-in-south-kashmirs-zainapora-belt/> [Accessed 16 Sep. 2023].
- [20] News Desk. (2021) *Uttar Pradesh: Internet Services Shut in Lakhimpur Kheri, Sitapur*. [online] The Mid-Day. Available from: <https://www.mid-day.com/news/india-news/article/uttar-pradesh-internet-services-shut-in-lakhimpur-kheri-sitapur23195427> [Accessed 16 Sep. 2023].
- [21] News Desk. (2024) *Farmer's protest: Haryana govt extends internet suspension in seven districts till Feb 23*. [online] ANI News. Available from: <https://www.aninews.in/news/national/politics/farmers-protest-haryana-govt-extends-internet-suspensionin-seven-districts-till-feb-2320240222014847/> [Accessed 16 Jun. 2025].
- [22] News Desk. (2024) *Government lifts mobile internet ban in nine districts after 3 weeks*. [online] The Times of India. Available from: <https://timesofindia.indiatimes.com/india/manipur-government-lifts-mobile-internet-ban-in-nine-districtsafter-3-weeks/articleshow/116146794.cms> [Accessed 16 Jun. 2025].
- [23] News Desk. (2024) *Jharkhand suspends mobile internet to check malpractice during exam*. [online] The Times of India. Available from: <https://timesofindia.indiatimes.com/india/jharkhand-suspends-mobile-internet-to-check-malpractice-duringexam-all-you-need-to-now/articleshow/113539597.cms> [Accessed 16 Jun. 2025].
- [24] *Rajendra Krishna Vs. State of Jharkhand* (2024), SCC OnLine Jhar 3349.
- [25] Rajvanshi, A. (2023) *How Internet Shutdowns Wreak Havoc in India*. [online] TIME. Available from: <https://time.com/6304719/india-internet-shutdowns-manipur/> [Accessed 25 Mar. 2024].

- [26] Roberto Barroso, L. & van Brussel Barroso, L. (2023) Democracy, Social Media, and Freedom of Expression: Hate, Lies, and the Search for the Possible Truth. *Chicago Journal of International Law*, 24(51). Available from: <https://cjlil.uchicago.edu/print-archive/democracy-social-media-and-freedom-expression-hate-lies-and-searchpossible-truth> [Accessed 25 Mar. 2024].
- [27] Ruijgrok, K. (2022) The Authoritarian Practice of Issuing Internet Shutdowns in India: The Bharatiya Janata Party's Direct and Indirect Responsibility. *Democratization*, 29. Available from: <https://www.tandfonline.com/doi/full/10.1080/13510347.2021.1993826> [Accessed 25 Mar. 2024].
- [28] Ryng, J. et al. (2022) Internet Shutdowns: A Human Rights Issue. *The RUSI Journal*, 167(50). Available from: <https://www.tandfonline.com/doi/full/10.1080/03071847.2022.2156234> [Accessed 17 Mar. 2024].
- [29] SFLC. (2025) *Internet Shutdowns Tracker*. [online] Available from: <https://internetshutdowns.in/> [Accessed 16 Sep. 2023].
- [30] Shirin, B. (2023) *Internet Ban Lifted in Violence-Hit Manipur, Restrictions in Border Areas till Dec 18*. [online] India Today. Available from: <https://www.indiatoday.in/india/story/manipur-violence-internet-services-restored-border-areas-exceptionmeiteis-kukis-2471548-2023-12-04> [Accessed 25 Mar. 2024].
- [31] Singh, T. & Waghre, P. (2023) *Statement: 100 Days of Manipur's Ongoing Illegal Internet Shutdown & Violation of Fundamental Rights*. [online] Internet Freedom Foundation. Available from: <https://internetfreedom.in/manipur-100-days-internet-shutdown/> [Accessed 16 Jun. 2025].
- [32] Software Freedom Law Center. (2022) *7 Day Long internet shutdown in Andhra Pradesh in violation of Supreme Court of India Guidelines: RTI Response*. [online] Available from: <https://sflc.in/7-day-long-internet-shutdown-andhra-pradesh-violationsupreme-court-india-guidelines-rti-response/> [Accessed 25 Mar. 2024].
- [33] *The Code of Criminal Procedure 1973, India*. In: English.
- [34] The Hindu Bureau. (2024) *Longest Internet Shutdown in 2023 Took Place in Manipur amidst Human Rights Violations: Report*. [online] The Hindu. Available from: <https://www.thehindu.com/sci-tech/technology/longest-internet-shutdown-2023-took-place-manipur-amidst-human-rights-violations-report/article67726259.ece> [Accessed 25 Mar. 2024].
- [35] *The Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules 2017, SI, India*, In: English.

- [36] *The Temporary Suspension of Telecommunication Services Rules 2024*, SI, India. In: English.
- [37] Thumfart, J. (2024) Digital Rights and the State of Exception. Internet Shutdowns from the Perspective of Just Securitization Theory. *Journal of Global Security Studies*, 9(1). Available from: <https://academic.oup.com/jogss/article/doi/10.1093/jogss/ogad024/7515068> [Accessed 16 Mar. 2024].
- [38] TNN. (2021) *Internet Shutdown in Rajasthan: Mobile Internet Suspended for RAS Prelims Exam across Rajasthan Today*. [online] The Times of India. Available from: <https://timesofindia.indiatimes.com/city/jaipur/mobile-net-suspended-for-ras-prelimsexam-across-raj-today/articleshow/87290703.cms> [Accessed 16 Sep. 2023].
- [39] TNN. (2021) *Patwari Exam: Mobile Internet Banned in Jaipur, Dausa till 6pm*. [online] The Times of India. Available from: <https://timesofindia.indiatimes.com/city/jaipur/patwari-exam-mobile-net-banned-in-jaipur-dausa/articleshow/87214485.cms> [Accessed 16 Sep. 2023].
- [40] Wani, A. (2021) *Mobile Internet Services Suspended in Parts of Kashmir as Precautionary Measure*. [online] India Today. Available from: <https://www.indiatoday.in/india/story/internet-services-jammu-kashmir-districts-terror-attacks-1866205-2021-10-18> [Accessed 16 Sep. 2023].

DOI 10.5817/MUJLT2025-2-2

ALIGNING IRAN'S LEGISLATION WITH SUSTAINABLE DEVELOPMENT GOALS: A TOPIC MODELING APPROACH

by

ZAHRA HEMMAT * MOHAMMAD MEHRAEEN [†]
RAHMATOLLOAH FATTAHI [‡] FARHAD SHIRANI [§]

This study examines the extent to which national legislation in Iran aligns with the Sustainable Development Goals (SDGs) within the framework of Multi-Level Governance (MLG). Employing a mixed-method computational approach—combining thematic analysis and topic modeling—the research explores the argumentative and content structures of legislative texts. Findings reveal partial alignment in areas such as education, health, and environmental protection, while significant gaps remain in community empowerment, gender equality, climate action, and participatory governance. From a policy perspective, the study highlights the need to revise legislative processes to systematically integrate SDG principles, establish mechanisms for assessing legal compatibility with SDG indicators, and build the capacity of lawmakers. It also emphasizes the importance of enhancing the participation of local institutions and civil society in the legislative process and recommends developing data-driven platforms for continuous monitoring of legal alignment with the SDGs. Theoretically, the study contributes to the application

* PhD in Information Systems, Department of Management, Faculty of Economics and Administrative Sciences, Ferdowsi University of Mashhad, Mashhad, Iran. E-mail: Hemmat@alumni.um.ac.ir

[†] Professor of Information Systems, Department of Management, Faculty of Economics and Administrative Sciences, Ferdowsi University of Mashhad, Mashhad, Iran. E-mail: Mehraeen@um.ac.ir
[‡] Professor of Information Systems, Department of Management, Faculty of Economics and Administrative Sciences, Ferdowsi University of Mashhad, Mashhad, Iran. E-mail: Mehraeen@um.ac.ir

[‡] Professor of Knowledge and Information Science, Department of Library and Information Science, Ferdowsi University of Mashhad, Mashhad, Iran. E-mail: fattahi@ferdowsi.um.ac.ir

[§] Assistant Professor, Department of Electronic Commerce, Research Institute of Information Science and Technology of Iran (Irandoc), Tehran, Iran. E-mail: shirani@irandoc.ac.ir

of the MLG framework in legal and development studies by offering empirical insights into the interplay between governance levels and legal systems. However, the research is limited by its exclusive focus on formal legal texts, limited interpretive depth of topic modeling, and its single-country scope. Future studies should explore comparative legal assessments, critical discourse analysis, and network-based approaches in other developing countries. Additionally, analyzing sub-national laws and their implementation could provide further insights into the challenges and opportunities of SDG localization.

KEY WORDS

Sustainable Development Goals (SDGs), Multi-Level Governance (MLG), Topic modeling, Latent Dirichlet Allocation (LDA)

1. INTRODUCTION AND MOTIVATION

The Sustainable Development Goals (SDGs), established in 2015, provide a comprehensive and integrated policy framework to be achieved by 2030. Realizing these goals requires the alignment of national laws and policies with the principles of sustainable development. In this regard, the local government plays a critical role in achieving the global agenda for sustainable development by 2030, particularly in underdeveloped nations. The existing literature highlights¹ the importance of governance and policy coherence, emphasizing the SDG localisation approach in place and calling for specific attention to be given to the effective localization of the SDGs within countries.² While the multi-level governance(MLG) framework is the dominant perspective in these studies, little attention has been paid to the alignment of national legislation with the SDGs.³

¹ UN. (2015) *Transforming our world: The 2030 agenda for sustainable development*. [online] Available from: <https://sdgs.un.org/2030agenda>; Tosun, J. and Leininger, J. (2017) Governing the interlinkages between the sustainable development goals: Approaches to attain policy integration. *Global Challenges*, 1(9), p.1700036; Bilsky, E., Moreno, A.C. and Tortosa, A.F. (2021) Local Governments and SDG Localisation: Reshaping Multilevel Governance from the Bottom up. *Journal of Human Development and Capabilities*, 22(4), pp. 713-724; Sarkar, M. S. K. et al. (2022) Localisation of Sustainable Development Goals (SDGs) in Bangladesh: An Inclusive Framework under Local Governments. *Sustainability*, 14 (17), p. 10817.

² *Ibid.*; Biggeri, M. (2021) A "Decade for Action" on SDG localisation. *Journal of Human Development and Capabilities*, 22(4), pp. 706-712; Xie, H., Wen, J. and Choi, Y. (2021) How the SDGs are implemented in China? A comparative study based on the perspective of policy instruments. *Journal of Cleaner Production*, 291, p. 125937; see also 5.

³ UN. (2015) *Transforming our world: The 2030 agenda for sustainable development*. [online] Available from: <https://sdgs.un.org/2030agenda>; Tosun, J. and Leininger, J. (2017) *op. cit.*, p.1700036; Bilsky, E., Moreno, A.C. and Tortosa, A.F. (2021) Local Governments and SDG Localisation: Reshaping Multilevel Governance from the Bottom up. *Journal of Human Development and Capabilities*, 22(4), pp. 713-724; Sarkar, M. S. K. et al. (2022) *op. cit.*

Over the past two decades, the concept of MLG has played a pivotal role in analyzing the dynamics of intergovernmental relations, including engagements with supranational organizations. In the context of sustainable development, MLG provides a comprehensive framework for understanding the interactions between various actors – public institutions, private entities, and civil society – across different levels of governance. This perspective is particularly valuable for assessing how policy coherence and institutional coordination influence the effective localization and implementation of the SDGs.⁴ This approach facilitates the establishment of operational mechanisms where local, national, and international institutions collaborate in a coordinated manner to advance these objectives. Despite the widespread focus on the implementation of the SDGs, few studies have explored the alignment of national legislation with these goals within the framework of MLG.⁵

This research gap could significantly impact the success of sustainable development policies, as the lack of alignment and coordination between the legislative process and the SDGs may lead to considerable challenges in their implementation. Therefore, further research is necessary to analyze the compatibility of national legislation with the SDGs, as this issue could have a significant impact on the effectiveness and efficiency of sustainable development policies and contribute to improving the implementation processes. This research gap is not only important globally but also in developing countries such as Iran, where many of the challenges and opportunities for sustainable development are particularly manifested at the local level. In this context, focusing on the legislative process and its alignment with the SDGs can help better identify social and cultural needs and priorities, thus improving the effectiveness of SDG implementation.⁶ This leads to the following research question: To what extent do national legislation in Iran align with the principles of the SDGs and how can they facilitate the effective localization of these goals?

To address the research question, this study employs a data-driven approach, specifically topic modeling, to analyze the alignment of national legislation with the principles of the SDGs in Iran. The study focuses on extracting key themes and patterns from national legal texts to assess their compatibility with SDG principles. The dataset includes a large corpus of national laws and regulations, which is processed using natural

⁴ Bilsky, E., Moreno, A. C. and Tortosa, A. F. (2021) *op. cit.*; Allain-Dupré, D. (2020) The multi-level governance imperative. *The British Journal of Politics and International Relations*, 22(4), pp. 800-808.

⁵ Xie, H., Wen, J. and Choi, Y. (2021) *op. cit.*

⁶ Biggeri, M. (2021) *op. cit.*

language processing (NLP) techniques. Topic modeling is applied to identify underlying topics within the legal texts and assess their alignment with the SDGs. The analysis reveals several key areas where national legislation aligns well with SDG principles, but also highlights significant gaps, especially in addressing local-level challenges. These findings emphasize the need for stronger coordination between national legal frameworks and local governance mechanisms to enhance the effective localization of the SDGs.

The findings highlight the critical importance of fostering stronger coordination between national legal systems and local governance mechanisms, ensuring that the SDGs are localized effectively and in a manner that addresses both national and local-level challenges. This research contributes to the growing body of literature on MLG by extending its application to the alignment of legislation with global goals. The implications of this study are significant, indicating that for the successful achievement of the SDGs, particularly in developing countries, policymakers must prioritize legal reforms that promote greater policy coherence and improve coordination among institutions.

In the following sections: We first provide a review of the related work on the localization of the SDGs, the multi-level governance (MLG) framework, and recent approaches to legal text analysis using topic modeling. We then elaborate the methodology, detailing the contextualized topic modeling approach employed. The next presents the key findings of the study. Finally, we discuss the implications of these findings and offers recommendations for future research and practice.

2. RELATED WORK

This section reviews the relevant literature in three main areas: (1) the localization of the Sustainable Development Goals (SDGs) and the role of national legislation, (2) the multi-level governance (MLG) framework and its relevance to sustainable development, and (3) recent advances in legal text analysis, with a focus on topic modeling approaches. These three strands of literature provide the theoretical and methodological foundation for our study.

At the national level, the achievability of the SDGs is closely tied to the policy pathways by governments. Existing research emphasizes that the realization of the SDGs depends not only on high-level political commitment but also on the capacity of local and regional governments

to promote integrated, inclusive, and sustainable development strategies.⁷ National legislation plays a pivotal role in institutionalizing these strategies, transforming global goals into legally enforceable commitments. In this regard, governments act as both implementers and enablers—bridging the gap between international development agendas and local realities.⁸ Recent studies have stressed the need for legislatures, particularly in developing countries, to assume a proactive role in aligning legal frameworks with the SDGs. This includes duties such as enacting laws that promote inclusive governance, securing budgetary resources for implementation, and performing oversight functions to hold executive agencies accountable.⁹ In contexts like Iran, where sustainable development challenges intersect with governance constraints, this legislative alignment becomes even more crucial.

Despite decades of reform efforts, the field of law and development has historically lacked a unified theory capable of explaining why some legal interventions succeed while others fail. Scholars have identified three interdependent factors as critical to the success of legal reforms: regulatory design, compliance mechanisms, and the state's institutional capacity for law enforcement.¹⁰ This triad provides an analytical lens to understand how legal systems can either facilitate or hinder sustainable development.

The SDGs, in turn, offer a coherent and widely accepted global framework that bridges the conceptual gap between legal reform and development objectives. As a set of interrelated goals focusing on social justice, equity, environmental sustainability, and human welfare, the SDGs provide normative guidance for evaluating national legislation. They enable researchers and policymakers alike to assess whether existing legal structures are adequately supporting sustainable development across sectors. Thus, in the absence of a unifying theory within law and development, the SDGs can function as a *de facto* framework for aligning legal reform with broader development outcomes.¹¹

⁷ Sarkar, M. S. K et al. (2022) *op. cit.*; Moyer, J. D. and Bohl, D. K. (2019) Alternative Pathways to Human Development: Assessing Trade-Offs and Synergies in Achieving the Sustainable Development Goals. *Futures*, 105, pp. 199-210.

⁸ Galli, A. et al. (2018) Think Globally, Act Locally: Implementing the Sustainable Development Goals in Montenegro. *Environmental Science & Policy*, 84, pp. 159-169; Wiegant, D. Dewulf, A. and Van Zeben, J. (2024) Alignment Mechanisms to Effectively Govern the Sustainable Development Goals. *World Development* 182, p. 106721.

⁹ Ladan, M. T. (2018) Achieving Sustainable Development Goals through Effective Domestic Laws and Policies on Environment and Climate Change. *Environmental Policy and Law*, 48 (1), pp. 42-63.

¹⁰ Lee, Y. S. (2017) General Theory of Law and Development. *Cornell International Law Journal*, 50 (3), pp. 416-471.

¹¹ Bilsky, E. Moreno, A. C. and Tortosa, A. F. (2021) *op. cit.*

The multi-level governance (MLG) framework offers a valuable conceptual lens through which the implementation of the SDGs—especially those requiring coordinated legal and policy efforts—can be understood. MLG refers to the dispersion of authority and policy-making across multiple levels of government: supranational, national, regional, and local. It emphasizes the interdependence and negotiation between actors operating at these various levels, often across traditional sectoral boundaries.¹²

Within the context of the SDGs, MLG helps explain how global development goals are translated into national legislation and localized action. It recognizes that while the goals are globally defined, their realization is inherently dependent on governance capacities and institutional dynamics at the subnational level.¹³ This is particularly relevant to legal alignment with the SDGs, as laws are both created and implemented across different layers of government. Hence, an MLG perspective moves the analysis beyond the national level and draws attention to the legal frameworks and compliance structures at the regional and local scales.¹⁴

Furthermore, MLG highlights the importance of vertical and horizontal coordination in sustainable development efforts. Vertical coordination refers to alignment between different levels of government, while horizontal coordination involves collaboration across sectors and institutions at the same level. In the case of legal reform, both dimensions are crucial: vertical coordination ensures that national laws empower and support local implementation, while horizontal coordination facilitates cross-sectoral integration, for example between environmental, economic, and social policy domains.¹⁵

The MLG framework complements the SDG-based approach to law and development by emphasizing the institutional arrangements and governance mechanisms required to operationalize the goals. It supports the premise that laws do not operate in isolation but within a complex ecosystem of actors, institutions, and norms. As such, the integration of MLG into the analysis helps account for variation in legal effectiveness across national systems.¹⁶

¹² Croese, S., Oloko, M., Simon, D. and Valencia, S. C. (2021) Bringing the Global to the Local: The Challenges of Multi-Level Governance for Global Policy Implementation in Africa. *International Journal of Urban Sustainable Development*, 13 (3), pp. 435-447; see also 3; Allain-Dupré, D. (2020) *op. cit.* pp. 800-808.

¹³ Galli, A. et al. (2018) *op. cit.* pp. 159-169.

¹⁴ Wiegant, D. Dewulf, A. and Van Zebe, J. (2024) *op. cit.* p. 106721; Ladan, M. T. (2018) *op. cit.*; see also 9.

¹⁵ Tosun, J. and Leininger, J. (2017) *op. cit.* p. 1700036; Moyer, J. D. and Bohl, D. K. (2019) *op. cit.* pp. 199-210.

¹⁶ Biggeri, M. (2021) *op. cit.* pp. 706-712; see also 6; Allain-Dupré, D. (2020) *op. cit.*

Recent developments in computational methods have opened new avenues for analyzing legal texts at scale. Among these, topic modeling—especially Latent Dirichlet Allocation (LDA)—has emerged as a powerful technique for uncovering latent thematic structures within large corpora of legal documents.¹⁷ These unsupervised learning methods enable researchers to extract recurring themes, identify trends over time, and explore how legal content aligns with broader policy goals such as the SDGs. Previous Studies demonstrated the applicability of topic modeling in legislative analysis by examining the temporal evolution of legal themes and their alignment with national and global development agendas, including the SDGs¹⁸ In the context of this study, topic modeling serves both an analytical and exploratory function. Analytically, it provides an empirical basis for mapping the extent to which national legislation reflects SDG-related priorities, such as climate action, gender equality, and access to justice. Exploratorily, it allows for the identification of emerging or neglected areas in legal discourse, which may signal gaps in governance or mismatches between legislative intent and development objectives.¹⁹

While the literature provides a broad and multifaceted perspective on the localization of the SDGs, the current study adopts multi-level governance (MLG) as its primary theoretical lens. This framework is particularly suitable for addressing our research question, as it foregrounds the institutional complexity and coordination challenges inherent in aligning national legislation with global development agendas.²⁰ The theory of MLG allows us to conceptualize national laws not merely as top-down instruments but as part of an interactive system that includes regional and local governance layers.

¹⁷ Blei, D. M. Ng, A. Y. and Jordan, M. I. (2003) Latent Dirichlet Allocation. *Journal of Machine Learning Research*, 3 (Jan), pp. 993-1022; Chauhan, U. and Shah, A. (2021) Topic Modeling Using Latent Dirichlet Allocation: A Survey. *ACM Computing Surveys (CSUR)*, 54 (7), pp. 1-35.

¹⁸ Greene, D. and Cross, J. P. (2017) Exploring the Political Agenda of the European Parliament Using a Dynamic Topic Modeling Approach. *Political Analysis*, 25 (1), pp. 77-94; Sanders, J., Lisi, G. and Schonhardt-Bailey, C. (2017) Themes and Topics in Parliamentary Oversight Hearings: A New Direction in Textual Data Analysis. *Statistics, Politics and Policy*, 8 (2), pp. 153-194.

¹⁹ Invernici, F. et al. (2024) Capturing Research Literature Attitude Towards Sustainable Development Goals: An LLM-Based Topic Modeling Approach. *arXiv*. Available from: <https://arxiv.org/abs/2411.02943>

²⁰ Allain-Dupré, D. (2020) *op. cit.* pp. 800-808.

Within the MLG framework, three core constructs guide our analysis:

- Policy Coherence – the degree to which national legislation aligns with overarching SDG principles across sectors and governance levels;
- Institutional Coordination – the mechanisms and processes that facilitate collaboration between different governmental tiers in translating legislative provisions into local action and
- Legal Responsiveness – the extent to which legal texts reflect and adapt to context-specific development priorities, particularly those emerging from subnational levels.

These constructs are embedded in a set of premises grounded in the theory: (1) that legal effectiveness is contingent upon multi-level coordination, (2) that vertical (national–local) and horizontal (cross-sectoral) integration is essential for sustainable outcomes, and (3) that the institutional context in which laws are enacted and implemented significantly affects their alignment with global norms like the SDGs.

Unlike general discussions of law and development, MLG offers a structured pathway to evaluate how national legal texts contribute to or hinder sustainable development. It emphasizes dynamic interactions rather than static legal content and frames legislation as part of a broader governance architecture. By integrating this framework with computational topic modeling, this study moves beyond descriptive analysis to offer theoretically informed insights into the alignment of Iranian national legislation with the SDGs.

3. METHODOLOGY

To explore the alignment between national legislation and the Sustainable Development Goals (SDGs), this study adopts a mixed-method computational approach to legal text analysis. Our methodology is grounded in two complementary strands: thematic analysis and topic modeling, each providing unique insights into the argumentative and content-related structures of legislative texts. We begin with a thematic approach to analyze the argumentative and deliberative structure of legislative texts. Thematic analysis is particularly well-suited for settings in which the form, sequence, and reciprocity of arguments are of central importance, such as parliamentary debates and oversight hearings. By preserving linguistic features such as punctuation and syntax, and reducing words to their lemmas, we can track how ideas develop, how actors respond to one another, and how argumentation unfolds across time. This approach employs co-occurrence

analysis to map conceptual relationships within the corpus. Textual units are clustered based on their semantic similarity, allowing us to identify recurring argument patterns and key thematic clouds. Visualization techniques such as correspondence analysis and dendrograms are used to examine interrelations among themes and contextual variables such as speaker identity, political affiliation, or institutional role.²¹

To complement our thematic findings, we apply topic modeling techniques, particularly LDA, to uncover the latent thematic structures in a large corpus of legal documents.²² Topic models treat text as a collection of probabilistic word distributions, revealing the underlying content of the discourse rather than its interactive structure. While these models do not capture reciprocal argumentation, they are powerful tools for detecting broad policy trends and thematic evolution across time. In contrast to lemmatization, topic modeling typically involves stemming words to their root forms to simplify vocabulary and facilitate probabilistic classification. This enables us to observe how themes related to the SDGs emerge, persist, or evolve within legislative texts.²³

Our corpus consists of national legislative documents. In this study 11760 laws collected from July 2016 to July 2023 are examined. Data extraction was performed using two Python libraries, BeautifulSoup and Request. The dataset contains a variety of features, such as title, content, lead (a summary of law), tags, classes, types, categories (law source organization), and date. Translations of samples of collected laws are shown in Table 1. A variety of legal texts are presented in dataset, including news, drafts, votes, plans, laws, bills, parliament deliberations, regulations, and opinions. Topic modeling was conducted by LDA using Python programming language only for regulations.

²¹ Blei, D. M. and Lafferty, J. D. (2007) A Correlated Topic Model of Science. *The Annals of Applied Statistics*, pp. 17-35; Grimmer, J. and Brandon, S. M. (2013) Text as Data: The Promise and Pitfalls of Automatic Content Analysis Methods for Political Texts. *Political Analysis*, 21 (3), pp. 267-297.

²² Blei, D. M. Ng, A. Y. and Jordan, M. I. (2003) *op. cit.* pp. 993-1022.

²³ Blei, D. M. and Lafferty, J. D. (2007) *op. cit.* pp. 17-35.

Table 1: Sample of collected laws.

Title	Content	Tags	Classes	Date
Deliberations summary of the public session of the Islamic Council on Tuesday, July 6, 1402.	Deliberations summary of the public session of Tuesday, July 6, 1402 of the Islamic council was published. The main discussions of this meeting are as follows: 1. The report of the judicial and legal commission on the performance of the bar associations and the union of bar associations of Iran - in the implementation of Article 212 of the internal regulations law. 2. Reading the report of the commission on Article 90 of the constitution regarding air pollution. 3. Announcing the receipt of a project item: Plan to amend articles of Iran's aquatic resources protection and exploitation law. 4. Written reminders of parliamentarians to executive officials of the country.	Air pollution, 90th principle commission, Water resources, Water resources of Iran, Bar association	The deliberations of the Islamic Council, The Islamic Council	Saturday, July 10, 1402
Seventh five-year development plan bill (1402-1406).	The bill of the seventh five-year development plan (1402-1406) was sent to the Islamic Council by the president on 03/28/1402 for legal formalities.	Development, The seventh development plan, The development plan, The country's development plan, The economic, Social and cultural development plan	Bills news, Economic group, Cabinet	Monday, June 29, 1402
The opinion of Islamic Council Chairman regarding the approval of the Supreme Council for the implementation of the general policies of Article 44 of the Constitution on the issue of determining the mechanism for the transfer of equity shares to qualified individuals.	The opinion of Islamic Council Chairman regarding the approval of the Supreme Council for the implementation of the general policies of Article 44 of the Constitution on the issue of determining the mechanism for the transfer of equity shares to qualified persons was announced by letter No. 20146/HB on 03/17/1402.	Shares, Justice shares	News, Legal opinions, Economic group, Islamic Council Chairman, All executive organizations	Monday, June 22, 1402

Title	Content	Tags	Classes	Date
The Executive Regulations of Clause A, Note 6 of Article One of the Budget Law of 1402 for the whole country.	The approval letter of the Council of Ministers meeting dated 04/04/1402 regarding the "executive regulation of paragraph A of note 6 of the single article of the budget law of the year 1402 of the whole country" was notified by the first vice president in letter number 59606 dated 04/07/1402.	Budget, 1402 budget, 1402 budget law, 1402 budget law of the whole country, Villa garden, Authorized villa garden, Unauthorized villa garden	Regulations news, Financial and Economic Group, Cabinet of Ministers, Ministry of Economic Affairs and Finance, Ministry of Justice, Ministry of Agricultural Jihad, Ministry of Roads and Urban Development, Ministry of Interior, Ministry of Industry, Mining and Trade, Organization of Records and Real Estate of the country	Sunday, July 11, 1402
Designing a list of invalid rulings in the field of business.	The draft of the list of invalid rulings in the field of trade was received in the public session dated 03/22/1402 of the Islamic Council.	Trade, Invalid rulings in the field of trade	News of projects, Economic group, Islamic Council	Sunday, June 28, 1402

Data preprocessing is essential, which involves transforming raw data into a format that can be understood by machines. Unstructured text data can be preprocessed to extract non-trivial information. In order to prepare the data for topic modeling, the following steps were required to preprocess the data:

- Checking for empty records. The dataset did not contain any NULL values;
- Punctuation Removal: Unstructured documents have numerous punctuations such as apostrophes, commas, and so on, which are not understood by the machine;
- Tokenization: A stream of text is broken down into words, phrases, symbols, or other meaningful elements, which are referred to as tokens;
- Stop Word Removal: In textual documents, these words are often used to join words together, but they don't add much value to the content. There is a list of Persian stop words which has been used in this study;
- Lemmatization: It involves breaking down words into their root.

The data was preprocessed using the Hazm and Parsivar Python libraries. Next, vectorization is performed using TF-IDF, which converts the texts into numbers. Through the TF-IDF, we are able to determine the amount of information that a word provides about the context. Term frequency refers to how frequently a term appears in a document, and how relevant the term is to the document. As a result of using the TF-IDF, relativeness of the words in the document is determined, and the more informative words rule out the frequent word.

4. RESULTS

We retrieved 11760 laws from Dotic, categorized into different types. Figure 1 shows the evolution of types of laws (2016-2023). There is an increase in the number of laws issued from 2016 to 2018 except for those related to news and voting. From 2018 to 2019, the number of laws being made decreased, then increased until 2021. Following that, the number of laws is reduced. The majority of the laws are issued in 2021. Regulations are the most common type of law.

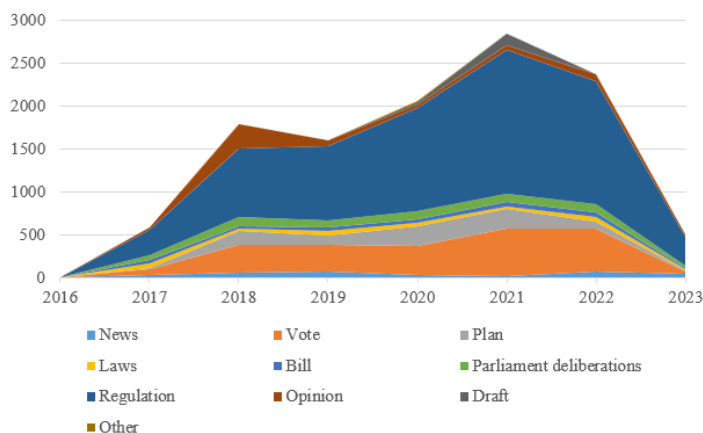


Figure 1: The evolution of laws over time.

Each type of law has its own characteristics, resulting in a variation in the size of text in the title and in the content. In Figure 2, each law is presented in a ratio of title size to content size. For example, the title of a news is usually brief, whereas the content is usually far more extensive. The title of Parliament approvals tends to be longer than news titles, as the longer the title is, the more understandable the approvals become, and they often contain numbers as well as parentheses. The title of Parliament approvals tends to be longer than news titles, as the longer the title is, the more understandable the approvals become, and they often contain numbers as well as parentheses.

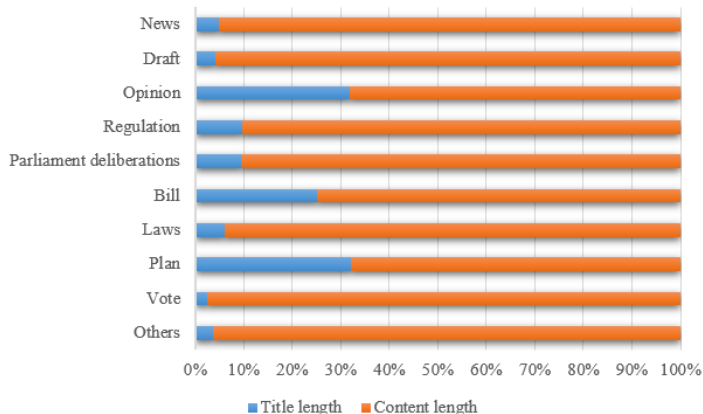


Figure 2: Title length to content length ratio.

The difference between law and regulation based on the definition provided by the Dotic website should be noted. Law refers to the decisions that create rights and duties for individuals (real and legal), or for the three powers (legislative, executive, and judicial) and other institutions, from which other regulations are derived. Regulations are the decisions that determine the method for the implementation of one or more laws, the regulation of administrative organizations, and other decisions that are made and implemented by the competent authorities.

Topic modelling was conducted using the title and content of regulations, since these features contain the most useful information that enhance the analysis. A total of 6599 records of regulations were analyzed using the LDA algorithms. Regulations make up a greater percentage of the law, and their content is more detailed and targeted, which makes their text more suitable for processing. Ten main topics were identified from these records. The frequency of each topic is shown in Figure 3. The most regulations relate to economics (29%), customs (26%), and housing and urban development (16%).

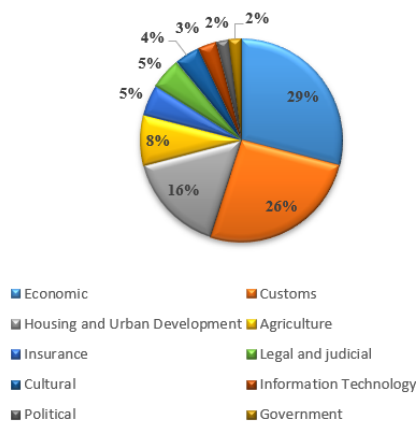


Figure 3: Title length to content length ratio.

According to Figure 4, all topics has minimum law in 2016 which is consistence with Figure 1. A total of 47% of regulations in 2017 related to political issues, and 35% in 2018 related to customs issues. The Insurance topic has the highest number of regulations in 2019 with 49%. The most important topic in 2020 was Legal and judicial, which accounted for 56% of the regulations. The most regulations in 2021, 2022, and 2023 will come from Economic (47%), Agriculture (59%) and Cultural (53%), which is completely consistent with the conditions of the Iran society. A number of events occurred in 2021, including the presidential election and the change of government, protests of farmers due to the drought and their problems, as well as the suspension of negotiations to revive the JCPOA. In addition to affecting economic conditions of the country, these problems have resulted in an increase in prices, which could be a factor in the increase in economic regulations.

Drought and rising temperatures created many problems for farmers in 2022. Agricultural products are also damaged by these droughts, which can lead to food shortages in the country. Agricultural regulations may be increased as a result of these problems. Also, these regulations may have been effected by protests that took place in 2021 in Khuzestan and Isfahan.

Guidance patrols were reinstated with a large extent in various cities at the middle of 2022, resulting in widespread protests across the country. This led to the hijab becoming one of the most important issues in the country. The presence of the most regulations for the cultural topic in 2023 can be attributed to these cases.

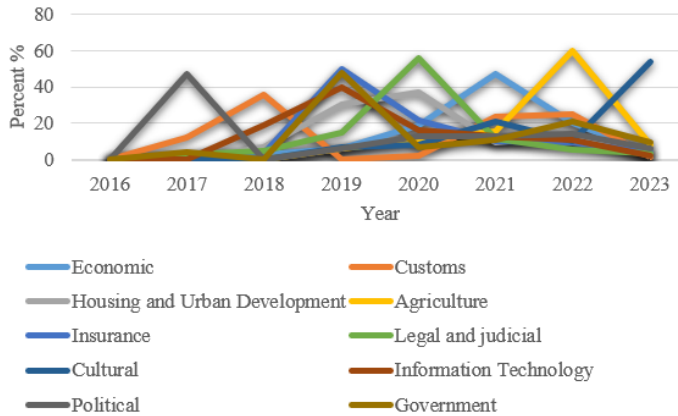


Figure 4: The percent of regulations per year for each topic.

Figure 5 illustrates the top word clouds in the ten identified topics, which are explained in the following.



Figure 5: Topics identified by combining LDA+TF_IDF algorithms.

Topic 1. Economic: Economic structure plays an important role in determining economic growth, energy demand, and the environmental footprint of countries. An increase in domestic production leads to economic growth and increase the budget. Governments plan their spending based

on the budget each year. But in recent years, the Iran government has run a severe budget deficit as a result of economic problems. The government debt has risen, businesses have reduced many of their products, and domestic production has decreased as well. Many governments use the budget deficit policy to eliminate temporary revenue shortages and to achieve targeted economic growth. Recent years, the Iranian government has received some parts of the budget deficit from a variety of sources in order to address different economic problems. An important source of deficit financing is foreign borrowing, which should be used to increase employment. Legislators need to revise the laws in order to address these issues for achieving economic growth.

Topic 2. Customs. Customs is a term used internationally. According to the Customs Co-operation Council (C.C.C.), customs is an organization tasked with enforcing customs laws, collecting import and export duties, as well as importing, transiting, and exporting goods. Based on resources and facilities available, countries design and implement a variety of programs in order to achieve their development goals. One of the key pillars of trade facilitation and growth in countries, especially developed ones, are free zones, which also play a crucial role in increasing exports and trade volumes. A free zone's establishment and continued operations will be supported by the facilitation of laws and structural protections. Export and import policies should be developed in a manner that results in exports in excess of a country's needs, and imports in excess of the country's needs. For this reason, legislators are responsible for specifying duty laws according to the country's needs for various products, including steel, petrochemicals, cement, metals, and motorcycles and bicycles, so that society's needs can be met and smuggling is prevented. In its most basic form, smuggling is the illegal importation of goods from one jurisdiction to another. A transaction that is illegal occurs in order to avoid legal taxation and duties. It is necessary to set laws and penalties in order to prevent smuggling.

Topic 3. Housing and Urban Development. Today, urban development is growing at such a rapid rate that the earth appears to be becoming an urban environment. It has become increasingly common for municipalities to rely on the financial resources of property developers and investors to implement comprehensive urban development plans. Several studies have been conducted to analyze the different methods used to charge developers so that the expenses of municipalities can be funded.

Most countries are transitioning from relying exclusively on traditional sources of funding (e.g. property taxes, duties, and intergovernmental transfers) to alternative sources of revenue generation. It is likely

that property taxes will not be sufficient to cover the expenditures of municipalities in most cities due to a reduction in intergovernmental transfers. As a result, municipalities seek alternative ways to access private capital in order to make up for this deficit. A major source of municipal income is the issuance of building and construction permits. There must be laws governing the issuance of permits and the collection of duties. Infrastructure costs, such as roads, can be covered by these charges, as well as the costs of public services, such as schools and parks.

Topic 4. Agriculture. The impacts of climate change are already being observed around the world, including an increase in the frequency of weather events such as droughts, floods, heat waves, wildfires, rising sea levels, and reductions in biodiversity. As a result of these events, people's lives can be negatively impacted in a number of ways, including health problems, economic losses, loss of labor productivity, damage to housing and critical infrastructures, as well as social disruptions.

As a result of climate change, droughts and water scarcity have caused extensive damage to agriculture. It is important to note that each province has different capacities in terms of agriculture and water resources. Therefore, laws can be enacted to specify the types of products that are allowed for agriculture in each province. The provinces of Khuzestan, Isfahan, and Fars are experiencing water scarcity, and farmers have had to deal with many challenges as a result. To support them, legislation must be enacted, which can support pricing and provide banking services. In order to solve the problem of water scarcity, there should be laws governing water saving, water efficiency, water pricing policy, cost-effective alternative solutions, and water hierarchy.

Topic 5. Insurance. The purpose of insurance is to provide financial protection against any type of risk. As part of the insurance contract, the insurer agrees to take on the risk of an insured entity against future events in exchange for monetary compensation. Various types of insurance policies are available depending on the type of risk involved, including life insurance, travel insurance, health insurance, and property insurance. Laws must be specified for each type of insurance, so that insurance companies can correctly assess the amount of damage and beneficiaries can receive their compensation when needed.

Topic 6. Legal and judicial. There are many areas of government, politics, and civil rights that are covered in the constitution, which is the highest legal document of a country. To provide fair judicial decisions in criminal and legal cases, judges refer to the constitution and its regulations as official documents of the country. A large number of issues relating to people's social lives are

covered in the constitution, including family, marriage, divorce, as well as the conditions of employees and retirees. Since there are many types of lawsuits, it is necessary to specify the applicable law for each.

Topic 7. Cultural. The concept of culture can be described as multifaceted, encompassing behaviors, values, and attitudes that are intrinsic to a particular group of people. There are many components of culture, including knowledge, belief, art, morals, law, custom, and any other abilities or habits that the individual has acquired as part of his social environment. In recent years, the world has become a much smaller interactive arena due to the convergence of new media. Social networks have enabled individuals to transcend geographical boundaries. As a result, individuals with different cultural backgrounds are able to respect and understand each other's traditions and norms of living. Social networks have provided an ideal platform for learning about different cultures. There are many posts about movies, music, local clothing and other cultural aspects of countries published daily on social networks such as Facebook, Twitter, Instagram, and Telegram. It is common for people to promote handicrafts on social networking sites and facilitate the purchase and sale of these products. Therefore, it is necessary to provide laws supporting social networking exchanges. In addition, regulations must be created in order to ensure that the culture of a country is properly introduced in social networks, since these contents have both a positive and negative impact on people's judgments and perceptions of countries.

Topic 8. Information Technology. The advancement of technology has had a significant impact on the way we acquire knowledge and learn. In recent years, online technology has become increasingly important in the field of education and learning. Using electronic resources to facilitate formal education is known as e-learning. During the COVID-19, traditional educational methods were replaced by e-learning, which became the primary solution for schools and universities. Due to the widespread use of e-learning, there should be laws regarding plagiarism, copyright issues, and data protection.

Additionally, telehealth and telemedicine services were widely used during the COVID-19 pandemic. Patients and clinicians have been able to come together without the fear of contracting COVID-19 through telehealth services. However, there are some concerns regarding reimbursement for services, patient privacy, and data sharing that require regulatory intervention. Having private information leaked affects the individual's personal life, leading to bullying, an increase in insurance premiums, as well as the loss of employment due to medical history. Hence, ensuring the

security, privacy, and trustworthiness of information is important. The lack of qualified personnel in the cybersecurity field makes it difficult for many organizations to adopt a standard approach or framework for cybersecurity. Cyber threats must be protected by law in order for organizations to remain safe.

Topic 9. Political. A major issue in Iran in recent years has been the nuclear negotiations. A number of agreements have been signed in accordance with the negotiations, whose non-compliance has resulted in sanctions against Iran. Typically, sanctions involve restrictions on trade as a means of coercing another country to comply with an international agreement or norm of conduct. In the absence of a decision from the United Nations Security Council, these measures which called countermeasures are taken against international wrongdoers. There have been comprehensive unilateral economic sanctions imposed on Iran in recent years by groups of countries (not the United Nations). From 2012, they have intensified as a result of international uncertainty regarding Iran's nuclear program's peaceful purpose, as well as the inadequacy of the country's trust-building efforts. Iran's free trade has been affected by these sanctions. Iran can benefit from partnerships with neighboring countries such as Iraq, Qatar, Oman, Pakistan, Tajikistan and Uzbekistan to reduce the impact of sanctions. To conduct negotiations effectively, it is necessary to establish laws for better communication with other countries.

Topic 10. Government. It is essential for the government to have laws in order to govern. There are several entities within the government, including government boards, government companies, and government property. In order to run government affairs, people are employed by government companies. Although some of the work can be handled by these government forces and companies, due to the high volume of work, some work must be assigned to the private sector.

In recent years, privatization has gained popularity as a panacea for resolving the organizational problems of governments by reducing the role of the state and promoting private sector enterprise growth. As stated in the Iranian Constitution, No.144, public companies must become private and a rapid program of privatization was launched by the government, including major industries, banks, insurance companies, airlines, shipping companies, etc. Following the government's decision to privatize 80% of the state's assets in 2003, the privatization of the healthcare system rapidly increased with the purpose of improving efficiency, social welfare, and system quality. It is urgent that the government of Iran expands and develops its private sector, increases the efficiency and effectiveness of infrastructure

and utility provision, and increases investment from both domestic and foreign sources. Privatization in Iran is intended to increase efficiency. A privatization program usually begins with a period of partial privatization, when only non-controlling shares of firms are sold on a stock exchange. This privatization will require legal requirements in order for monitoring and evaluation mechanisms to be effective, otherwise it will result in a reduction in the quality of services and social welfare.

5. DISCUSSION AND CONCLUSIONS

The main objective of this study was to examine the extent to which Iran's national legal frameworks align with the principles of the Sustainable Development Goals (SDGs), and to assess the capacity of these laws to facilitate effective localization of the goals. Using data-driven methods and topic modeling, a set of legal texts was analyzed to extract key themes and assess their correspondence with the SDGs. The findings suggest that while there is relative alignment in certain areas such as education, health, and environmental protection, significant gaps remain in key domains including community empowerment, gender equality, climate action, and participatory governance.

Within the theoretical framework of Multi-Level Governance (MLG) that underpinned this study, the results emphasize that core components such as policy coherence, institutional coordination, and legal accountability play a critical role in the successful localization of the SDGs. Notably, the lack of vertical coordination between governance levels (national-local) and horizontal misalignment across sectors and peer institutions emerge as major challenges hindering alignment between legislation and sustainable development goals in Iran.

From a policy perspective, the study offers several key implications. First, it is essential to revise legislative processes in Iran in a way that systematically embeds sustainable development principles within legal and executive structures. This requires mechanisms to assess the compatibility of existing and proposed laws with SDG indicators and principles, along with building the capacity of lawmakers to understand and internalize sustainable development imperatives. Second, mechanisms must be established to enhance the participation of local institutions and civil society in the legislative process, ensuring that national laws reflect local needs more accurately. Third, the development of data-driven platforms for continuous monitoring and assessment of legal alignment with SDGs could serve as a critical support tool for policy-makers.

From a theoretical standpoint, this study contributes to the application of the MLG framework in legal and development-related analysis. By providing empirical insights into the interplay between governance levels and legal frameworks, it demonstrates that without a systemic and inter-level understanding of legislative processes, the effective realization of the SDGs in developing countries remains limited.

Despite its valuable findings, this study faces some limitations. First, it focused exclusively on formal legal texts, with limited attention to customary laws, local regulations, or executive bylaws. Second, while topic modeling provides strong exploratory capabilities, it may offer limited interpretive depth in certain contexts. Furthermore, the study was limited to the Iranian context, and its findings may not be directly generalizable to other countries.

For future research, similar studies using network analysis, critical discourse analysis, or comparative legal assessments in other developing countries are recommended. Additionally, analyzing local-level laws (provincial or municipal) and exploring their practical implementation could offer new insights into the challenges and opportunities of SDG localization.

LIST OF REFERENCES

- [1] Allain-Dupré, D. (2020) The multi-level governance imperative. *The British Journal of Politics and International Relations*, 22(4), pp. 800–808.
- [2] Bilsky, E., Moreno, A. C., & Tortosa, A. F. (2021) Local governments and SDG localisation: Reshaping multilevel governance from the bottom up. *Journal of Human Development and Capabilities*, 22(4), pp. 713–724.
- [3] Biggeri, M. (2021) A “decade for action” on SDG localisation. *Journal of Human Development and Capabilities*, 22(4), pp. 706–712.
- [4] Blei, D. M., Lafferty, J. D. (2007) A correlated topic model of science. *The Annals of Applied Statistics*, pp. 17–35.
- [5] Blei, D. M., Ng, A. Y., & Jordan, M. I. (2003) Latent Dirichlet allocation. *Journal of Machine Learning Research*, 3, pp. 993–1022.
- [6] Chauhan, U. Shah, A. (2021) Topic modeling using latent Dirichlet allocation: A survey. *ACM Computing Surveys (CSUR)*, 54(7), pp. 1–35.
- [7] Croese, S., Oloko, M., Simon, D., & Valencia, S. C. (2021) Bringing the global to the local: The challenges of multi-level governance for global policy implementation in Africa. *International Journal of Urban Sustainable Development*, 13(3), pp. 435–447.
- [8] Galli, A., Đurović, G., Hanscom, L., & Knežević, J. (2018). Think globally, act locally: Implementing the sustainable development goals in Montenegro. *Environmental Science & Policy*, 84, pp. 159–169.

- [9] Cross, J. P. (2017) Exploring the political agenda of the European Parliament using a dynamic topic modeling approach. *Political Analysis*, 25(1), pp. 77–94.
- [10] Grimmer, J. Brandon, S. M. (2013) Text as data: The promise and pitfalls of automatic content analysis methods for political texts. *Political Analysis*, 21(3), pp. 267–297.
- [11] Invernici, F. et al. (2024) Capturing Research Literature Attitude Towards Sustainable Development Goals: An LLM-Based Topic Modeling Approach. *arXiv*. Available from: <https://arxiv.org/abs/2411.02943>
- [12] Ladan, M. T. (2018) Achieving sustainable development goals through effective domestic laws and policies on environment and climate change. *Environmental Policy and Law*, 48(1), pp. 42–63.
- [13] Lee, Y.-S. (2017) General theory of law and development. *Cornell International Law Journal*, 50(3), pp. 416–471.
- [14] Moyer, J. D. Bohl, D. K. (2019) Alternative pathways to human development: Assessing trade-offs and synergies in achieving the sustainable development goals. *Futures*, 105, pp. 199–210.
- [15] Sanders, J., Lisi, G., & Schonhardt-Bailey, C. (2017) Themes and topics in parliamentary oversight hearings: A new direction in textual data analysis. *Statistics, Politics and Policy*, 8(2), pp. 153–194.
- [16] Sarkar, M. S. K. et al. (2022) Localisation of sustainable development goals (SDGs) in Bangladesh: An inclusive framework under local governments. *Sustainability*, 14(17).
- [17] Tosun, J. Leininger, J. (2017) Governing the interlinkages between the sustainable development goals: Approaches to attain policy integration. *Global Challenges*, 1(9).
- [18] UN. (2015) *Transforming our world: The 2030 agenda for sustainable development*. [online] Available from: <https://sdgs.un.org/2030agenda>
- [19] Wiegant, D. Dewulf, A. & Van Zeben, J. (2024) Alignment mechanisms to effectively govern the sustainable development goals. *World Development*, 182.
- [20] Xie, H. Wen, J. & Choi, Y. (2021) How the SDGs are implemented in China—A comparative study based on the perspective of policy instruments. *Journal of Cleaner Production*, 291.

DOI 10.5817/MUJLT2025-2-3

OVERSIGHT BOARD – AN EFFECTIVE TOOL TO PROTECT FREE SPEECH? *

by

TAMÁS PONGÓ[†] RENÁTA KÁLMÁN[‡] RÉKA BRIGITTA SZANISZLÓ[§] NORBERT TRIBL[¶]

Meta has more than two billion daily active users, two and a half billion posts a day, and more than a million reports of violations of policies and guidelines every day. These large numbers justify the establishment of a body that goes beyond the usual content moderation and reporting system. Recognizing that its role in online speech cannot be managed solely through algorithmic decision-making and reporting, Meta has introduced a non-judicial grievance mechanism, the Oversight Board, which delivers its decisions solely in light of Meta's policies, values, and guidelines. The OB is committed to the Business and Human Rights regime, and in line with this commitment, the UNGPs are the governing international human rights law standard. This article cross-referenced the OB goals defined by its Charter, the UNGPs standards relevant to the goals of the OB, the statistics of the operation of the OB, and the doctrinal background of these goals, in particular, the accessibility, predictability, and transparency prongs as elements of an effective remedy. Through this in-depth analysis, we aim to explore whether the OB fulfills its predefined goals,

* The research was supported by the Digital Society Competence Centre of the Humanities and Social Sciences Cluster of the Centre of Excellence for Interdisciplinary Research, Development and Innovation of the University of Szeged. The authors are members of the Digitalization and Democracy research group.

[†] Tamás Pongó, Ph.D., senior lecturer, University of Szeged, Faculty of Law and Political Sciences, Institute of Public Law. E-mail: pongo.tamas@szte.hu

[‡] Renáta Kálmán, Ph.D., senior lecturer, University of Szeged, Faculty of Law and Political Sciences, Institute of Public Law. E-mail: kalman.renata@juris.u-szeged.hu

[§] Réka Brigitta Szaniszló, Ph.D., senior lecturer, University of Szeged, Faculty of Law and Political Sciences, International and Regional Studies Institute. E-mail: szaniszló.reka.brigitta@szte.hu

[¶] Norbert Tribl, Ph.D., senior lecturer, University of Szeged, Faculty of Law and Political Sciences, International and Regional Studies Institute. E-mail: tribl.norbert@szte.hu

and thus provides an effective non-judicial grievance mechanism regarding freedom of speech in the online environment.

KEY WORDS

Freedom of Speech, UNGPs, Oversight Board, Effectiveness, Accessibility, Transparency, Predictability

1. INTRODUCTION

“The purpose of the board is to protect free expression by making principled independent decisions about important pieces of content and by issuing policy advisory opinions on Meta’s content policies. The board will operate transparently and its reasoning will be explained clearly to the public, while respecting the privacy and confidentiality of the people who use Meta Platforms, Inc.’s services, including Facebook and Instagram (collectively referred to as “Meta”). It will provide an accessible opportunity for people to request its review and be heard.”¹

The Oversight Board’s Charter defines the framework for establishing the body and outlines its goals.² This unique institution, referred to as the Oversight Board (OB or Board), began operating in October 2020 to reform content moderation. We have found that the OB defined three specific elements to achieve the protection of free speech in the online environment, namely (1) transparency; (2) plain language; (3) access to remedy, i.e., users have the right to be heard.

The scope of this article is deliberately limited: we assess only three criteria of effective non-judicial grievance mechanisms under the UNGPs: (1) accessibility, (2) predictability, and (3) transparency. Other elements, such as plain language communication, while relevant, fall outside the scope of this study and would merit a separate analysis.

The OB is committed to the Business and Human Rights regime (BHR regime) and international human rights law (IHRL) as its Corporate Human Rights Policy (HRP) states. In line with this commitment, the UNGPs are the governing IHRL standard. According to the UNGPs, the OB categorizes itself as an independent non-judicial grievance mechanism. As such, the UNGPs’ effectiveness criteria for non-judicial grievance mechanisms should be used as a starting point to evaluate the Board’s decision-making mechanism.³

¹ Oversight Board. (2023) *Oversight Board Charter*. Available from: <https://www.oversightboard.com/wp-content/uploads/2023/11/3427086457563794.pdf>, p. 2.

² Oversight Board. (2023) *op. cit.* p. 13.

³ United Nations Human Rights Council. (2011) *UN Guiding Principles on Business and Human Rights*. [online] Available from: https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinessshr_en.pdf [Accessed 31 October 2024].

Therefore, this study cross-referenced the goals of OB defined by its Charter, the UNGPs standards relevant to the goals of the OB, the statistics of the operation of the OB, and the doctrinal background of these goals, in particular, the accessibility, predictability, and transparency prongs as elements of an effective remedy.

Through this in-depth analysis, we aimed to explore whether the OB fulfills its predefined goals and thus provides an effective grievance mechanism regarding freedom of speech in the online environment. This article addresses the following research questions:

RQ1: Is there a statistically significant difference in the likelihood of case selection between cases submitted by Meta and those submitted by users?

RQ2: Does the source of a case (Meta vs. user) influence the likelihood of the Board overturning Meta's original decision?

RQ3: Is there a disproportionate concentration of overturned or restored content in specific content categories (e.g., "dangerous individuals and organizations", "hate speech")?

The following sections proceed as follows: Part 2 outlines the BHR regime and its relevance to the OB; Part 3 situates the OB within IHRL; Part 4 presents our empirical statistical findings; Part 5 and 6 discuss the theoretical framework of effective redress; Part 7 assesses OB performance against these criteria; and Part 8 offers recommendations.

2. OVERVIEW OF THE BUSINESS AND HUMAN RIGHTS REGIME

In order to understand the importance and role of the OB, we shall briefly explore the framework in which it operates. As a private actor that delivers decisions on public law matters (free speech limitation), the existence of this body represents another step in the development of a global regime, of which the UN and the OECD are the driving forces.

The United Nations established the BHR regime through a several-year-long evolution. First, the United Nations Secretary-General established a position to study the human rights responsibility of businesses, which led to the appointment of John Ruggie as the UN Secretary-General's Special Representative on business and human rights in 2005.⁴ In 2008, the UN adopted the "Protect, Respect and Remedy" Framework, later operationalized through the UN Guiding Principles on Business and Human Rights (UNGPs) developed under John Ruggie's mandate. These Principles,

⁴ Wettstein, F. (2012) CSR and the Debate on Business and Human Rights: Bridging the Great Divide. *Business Ethics Quarterly*, 22 (4), pp. 739-770, p. 739.

while non-binding, have become a global reference point for corporate human rights responsibilities.⁵

The UNGPs system has three pillars: “the state duty to protect against business-related human rights infringements, the corporate responsibility to respect human rights, and increased access to remedy for victims of business-related human rights infringements.”⁶ Regarding the ICT sector and social media platforms, pillars two and three are the most relevant in our study since they should apply a corporate responsibility focusing on human rights protection and provide an accessible forum for redress. Basically, pillar two introduced the human rights due diligence method (HRDD) that requires businesses to identify, manage, and monitor adverse human rights impacts caused by their activities or any other activity connected to their operations.⁷ More precisely, HRDD covers the human rights violations caused by the company, or to which the company contributed, or which are directly linked to the company and its business relationships (UNGPS Princ. 17.(a)). When such an adverse human rights impact occurs, the business enterprise should use its leverage to prevent or manage these impacts. Leverage in this context refers to “the influence a business enterprise has with an entity or entities involved in a human rights abuse...”⁸ However, HRDD seems to be an umbrella term that involves human rights risk assessment and human rights impact assessment. Risk assessment focuses on avoiding or mitigating the negative outcomes a company may face, meanwhile, impact assessment requires strategic planning not just to avoid the adverse impacts, but to prevent them

⁵ Ruggie, J.G. (2014) Global Governance and “New Governance Theory”: Lessons from Business and Human Rights. *Global Governance*, 20 (1), pp. 5-18., p. 11.; Buhmann, K. and Olivera, R (2020) Human rights and social media platforms: the corporate responsibility to respect human rights in regard to privacy infringement involving photo posting. *Australian Journal of Human Rights*, 26 (1), pp. 121-141., p. 127.; Wettstein, F. (2012) *op. cit.*, p. 741.; Kun, A. (2017) Kellő gondosság alapú belső átvilágítás a munkajogban, mint a transznacionális vállalatok magatartásának új zsinórmértéke. *Miskolci Jogi Szemle*, 12 (2), pp. 285-297., p. 288.; Ruggie, J. G. (2007) Business and Human Rights: The Evolving International Agenda. *American Journal of International Law*, 101 (4), pp. 819-840.; Chronowski, N. (2023) Az alkotmány/bíraskodás potenciálja az üzleti szféra okozta emberi jogsérelmekkel szemben. *Alkotmánybírósági Szemle*, (1), pp. 2-14., p. 4.; Pap, L. A. Chronowski, N. and Nemessányi, Z. (2024) Corporate Human Rights Responsibility in Illiberal Regimes: The Example of the Ukrainian Refugee Crisis in Hungary. *Business and Human Rights Journal*, (9), pp. 32-53., p. 50 cites that France, Germany and Norway adopted laws and Switzerland put it on the agenda, unsuccessfully.

⁶ Buhmann, K. and Olivera, R (2020) *op. cit.*, p.125.

⁷ Pap, L. A. Chronowski, N. and Nemessányi, Z. (2024) *op. cit.*, p.45.

⁸ Buhmann, K. and Olivera, R (2020) *op. cit.*, p. 129.

and explore the opportunities in the course of establishing a strategy.⁹ Some scholars think that only risk assessment was included in the UNGPs.¹⁰

Nonetheless, the UNGPs influenced the OECD and the European Union to adopt the human rights due diligence approach. The OECD Guidelines for Multinational Enterprises on Responsible Business Conduct (updated 2023 version) highlights in the General Policies part that enterprises should “respect the internationally recognized human rights of those affected by their activities.”¹¹ In this part (II.A.11-13.), risk-based due diligence to identify, prevent, and mitigate adverse impacts is recommended, and such an approach aligns with the UNGPs standards, since it covers impacts that are caused by, or to which the company contributed, or directly linked to its operations, products or services. According to the Commentary, “due diligence is understood as the process through which enterprises can identify, prevent, mitigate and account for how they address their actual and potential adverse impacts as an integral part of business decision-making and risk management systems.”¹² The OECD Guidelines thereby strengthen pillars two and three of the UNGPs and thus intend to establish a global standard for human rights due diligence among business enterprises. Also, it acknowledges that the nature and extent of due diligence are affected by the specific circumstances of the given case and company, such as the size of the company, the severity of the adverse impact, and the involvement of the given enterprise.¹³ These statements are being reinforced in Chapter IV. Human Rights part, which was a result of Ruggie’s mandate and the adoption of the UN Framework 2008.¹⁴ In addition to the updated MNE Guidelines, the OECD issued the Due Diligence Guidance for Responsible Business Conduct, which seeks to help enterprises implement the UNGPs.¹⁵ “This Guidance was overseen by the OECD Working Party on Responsible Business Conduct (WPRBC) and involved a multi-stakeholder process with OECD and non-OECD countries and representatives from business, trade unions and civil society.”¹⁶ Even though the OECD adopted sector-specific guidelines for several fields, such as minerals, agriculture, garment, or footwear, no specific rules are available for social

⁹ Salcito, K. and Wielga, M. (2018) What does Human Rights Due Diligence for Business Relationships Really Look Like on the Ground?. *Business and Human Rights Journal*, (3), pp. 113-121., p. 114-115.

¹⁰ Salcito, K. and Wielga, M (2018) *op. cit.*, p. 115.

¹¹ OECD. (2008) *OECD Guidelines for Multinational Enterprises on Responsible Business Conduct*, OECD Publishing, II. General Policies A.2.

¹² OECD. (2008) *op. cit.* Commentary 15.

¹³ OECD. (2008) *op. cit.* Commentary 19.

¹⁴ Ruggie, J. G. (2014) *op. cit.*, p. 11.

¹⁵ OECD. (2018) *Due Diligence Guidance for Responsible Business Conduct*, Foreword.

¹⁶ *Ibid.*

media companies. Therefore, we need to look for a sector-specific toolkit or guidelines. Since our research focuses on Meta, we explored its Corporate Human Rights Policy, which referred to the Global Network Initiative (GNI) in addition to the UNGPs.¹⁷ The GNI is a multistakeholder framework with a diverse membership that issued its General Principles on Freedom of Expression and Privacy. The preamble of the GNI Principles declares that the Principles are based on the core international human rights conventions and are informed by the UN Protect, Respect, and Remedy Framework, the UNGPs, and the OECD Guidelines.¹⁸ Therefore, we can discover a BHR regime established by the UN, strengthened by the OECD, and reinforced by a technology-specific set of rules under the GNI principles with particular attention to freedom of expression and privacy. In addition to the Principles, the GNI adopted Implementation Guidelines, which seek to provide help for companies to put the Principles into practice.¹⁹ The Guidelines encourage companies to carry out HRDD in compliance with the UNGPs.²⁰ Also, it provides examples when a human rights impact assessment is needed as part of the HRDD.²¹

As discussed previously, the UNGPs were influential both at the global and regional level, and as a result, the EU has adopted two directives to strengthen the BHR regime in Europe, and we can see that through these directives the EU is trying to move the HRDD rules from the soft law to the hard law category.

The *Corporate Sustainability Reporting Directive* (CSRD)²² was adopted after five years of debate. The Directive was formally signed on 14 December 2022 and entered into force on 5 January 2023.²³ CSRD pivots on three design choices that connect it directly to the UNGPs logic: (i) double materiality and value-chain perimeter: companies must disclose

¹⁷ Meta (2021). Meta Corporate Human Rights Policy. [online] Available from: <https://about.fb.com/wp-content/uploads/2021/03/Facebooks-Corporate-Human-Rights-Policy.pdf> [Accessed 31 October 2024].

¹⁸ Global Network Initiative Principles. Available from: <https://globalnetworkinitiative.org/gni-principles/> [Accessed 30 April 2025].

¹⁹ Global Network Initiative. (2025) *Global Network Initiative Implementation Guidelines*. [online] Available from: <https://globalnetworkinitiative.org/implementation-guidelines/> [Accessed 30 April 2025].

²⁰ Global Network Initiative. (2025) *op. cit.* 2.4.

²¹ Global Network Initiative. (2025) *op. cit.* 2.6.

²² Cf. Hummel, K. and Jobst, D. (2024) An Overview of Corporate Sustainability Reporting Legislation in the European Union. *Accounting in Europe*, 21 (3), pp. 320–355.

²³ Directive of the European Parliament and of the Council of 14 December 2022 Amending Regulation (EU) No 537/2014, Directive 2004/109/EC, Directive 2006/43/EC and Directive 2013/34/EU, as regards corporate sustainability reporting. *Official Journal of the European Union* (2022/2464) 16 December. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2464> [Accessed 30 April 2025].

both outward human-rights/environmental impacts and financial risks and opportunities;²⁴ (ii) European Sustainability Reporting Standards (ESRS):²⁵ ESRS S1–S4 oblige undertakings to describe their HRDD process, echoing UNGP Principle 17; and finally (iii) governance guarantees – mandatory external assurance and a director’s duty to oversee the sustainability statement strengthen accountability mechanisms.²⁶

Another pillar of EU regulation is the so-called *Corporate Sustainability Due Diligence Directive* (CSDDD)²⁷, which could be considered as a hard-law counterpart to the UNGPs in Europe.²⁸ The CSDDD was adopted on 13 June 2024 and entered into force on 25 July 2024.²⁹ The CSDDD – in Articles 5–11 – codifies the core UNGP HRDD cycle: identify, prevent, mitigate, and bring to an end adverse human-rights and environmental impacts in own operations, subsidiaries, and established business relationships. It should be noted that, unlike the UNGPs’ “*should*” language, CSDDD uses the legally binding “*shall*”.

While the UNGPs and OECD Guidelines articulate expectations, the CSRD and CSDDD embed those expectations in EU company law. HRDD thus shifts from reputational best practice to a compliance imperative with audit trails, enforcement by national supervisory authorities, and, under CSDDD, civil liability exposure. Besides, CSRD creates a transparency pull:³⁰ companies must publicly describe HRDD policies, processes, and outcomes.³¹ Nevertheless, CSDDD creates a substantive push: companies must perform HRDD to an adequate standard.³² We can say that together the two directives operationalise Pillars II and III of the UNGPs within the EU single market.

²⁴ Cf. Recital 27, and Article 19a of Directive 2022/2464

²⁵ Cf. Preamble, and Chapter 6a of Directive 2022/2464

²⁶ Cf. Recital 62, Article 19a, and Article 34 of Directive 2022/2464

²⁷ Directive of the European Parliament and of the Council of 13 June 2024 On corporate sustainability due diligence and amending Directive (EU) 2019/1937 and Regulation (EU) 2023/2859. *Official Journal of the European Union* (2024/1760) 5 July. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401760 [Accessed 30 April 2025].

²⁸ Cf. Buen, N. et al. (2024) The EU Directive on Corporate Sustainability Due Diligence (CSDDD): The Final Political Compromise. *Business and Human Rights Journal*, 9 (2), pp. 294–300, p.296.

²⁹ The detailed analysis see: Ciacchi, S. (2024) The newly-adopted Corporate Sustainability Due Diligence Directive: an overview of the lawmaking process and analysis of the final text. *ERA Forum*, 25, pp. 29–48.

³⁰ Cf. Operato, L. et al. (2025) Navigating CSRD reporting: Turning compliance into sustainable development with science-based metrics. *Environmental Development*, 54.

³¹ Cf. Recital 30, Article 19a and Article 29a of Directive 2022/2464

³² Cf. Article 1, Article 5, Articles 7 to 16 and Recital 19 of Directive 2024/1760

Both directives adopt the UNGPs' concept of leverage over business relationships, but CSDDD gives it legal force by requiring termination or suspension (as a last resort) and contractual cascading of due diligence clauses.³³ By the beginning of 2027, for the largest EU and non-EU companies (and expanding in 2029), undertakings must actively carry out human rights due diligence: they must identify, prevent, mitigate, and, where necessary, remedy adverse impacts in their operations, their subsidiaries, and their established business relationships.³⁴ National supervisors can impose significant penalties for non-compliance, and victims gain a civil cause of action where harm was reasonably preventable and a causal link exists.

The UNGPs and the OECD Guidelines are soft-law instruments: they articulate what companies should do, but compliance ultimately rests on reputational incentives and peer pressure. By contrast, the European Union has converted the same expectations into binding law through two directives of CSRD and CSDDD. It should be noted that the CSDDD introduces a substantive duty of conduct as well. In short, the CSRD pulls companies toward better practice by exposing gaps to public scrutiny, while the CSDDD pushes them by making adequate due diligence a legal obligation backed by sanctions and liability. Together, they transform the voluntary standards of the UNGPs and OECD Guidelines into an enforceable European framework that strengthens access to remedy and explicitly links corporate human-rights management to climate-transition objectives.

This analysis indicates that Meta is committed to the BHR regime according to its Corporate Human Rights Policy, which encompasses the framework introduced above. Accordingly, our research on the OB as an effective grievance mechanism focuses on the UNGPs' effectiveness criteria since the UNGPs are the cornerstone of the current BHR regime, and Meta is committed to them as we introduced in Part 3. Although EU hard law rules do not yet prevail globally, it is likely that Meta will need to comply with them in the coming years to maintain its presence in the European market. Having outlined the BHR regime as the global framework, the next section situates the Oversight Board within international human rights law to clarify its institutional position.

³³ Cf. Article 10 and Article 11 of Directive 2024/1760

³⁴ Cf. Article 1(1)(a), Article 5(1), and Article 37(1)(a)-(c) of Directive 2024/1760

3. ESTABLISHMENT OF THE OVERSIGHT BOARD AND ITS CONNECTION TO IHRL

Meta has more than two billion daily active users,³⁵ two and a half billion posts a day, and more than a million reports of violations of policies and guidelines every day.³⁶ These large numbers justify the establishment of a body that goes beyond the usual content moderation and reporting system. Recognizing that its role in online speech cannot be managed solely through algorithmic decision-making and reporting, Facebook has introduced the OB, which delivers its decisions solely in light of Facebook's policies and values.

The establishment of the OB dates back to January 2018, when Noah Feldman wrote a brief note saying that Facebook needed a body to address the platform's content moderation issues.³⁷ *"Feldman, however, had something others didn't: he was close friends with Facebook COO Sheryl Sandberg. Feldman gave the memo to Sandberg, who forwarded it to Zuckerberg."*³⁸ Zuckerberg supported the idea and began the preparation for the establishment.³⁹ Highlighting its importance in the early stages, the Facebook founder compared the OB with the Supreme Court of the United States.⁴⁰ As a next step, the draft Charter was published in January 2019,⁴¹ which was followed by a global public consultation in June 2019. As a result of this process, the OB became fully operational in October 2020. Klonick has described this institutional creation as an unprecedented experiment in platform self-governance⁴², while Douek cautioned that procedural design choices would ultimately determine whether independence was more than symbolic.⁴³ Our findings on case-selection disparities, discussed in Part 4, provide empirical context for this scholarly debate.

³⁵ In December 2023, an average of 2.11 billion daily active users, and 3.98 billion monthly active users. Meta. (2023) *Meta Annual Report*. [online] Available from: https://www.annualreports.com/HostedData/AnnualReports/PDF/NASDAQ_FB_2023.pdf [Accessed 31 October 2024].

³⁶ Douek, E. (2019) Facebook's „Oversight Board:“ Move Fast With Stable Infrastructure and Humility. *North Carolina Journal of Law & Technology*, 21 (1). pp. 1-77.

³⁷ Klonick, K. (2020) The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression, *Yale Law Journal*, 129 (8). p. 2449.

³⁸ Ibid.

³⁹ Zuckerberg, M. (2021). *A Blueprint for Content Governance and Enforcement*. [Facebook] 5 May. Available from: https://www.facebook.com/notes/751449002072082/?hc_location=ufi [Accessed 31 October 2024].

⁴⁰ Klein, E. (2018) *Mark Zuckerberg on Facebook's hardest year, and what comes next*. [online] Vox. Available from: <https://www.vox.com/2018/4/2/17185052/mark-zuckerberg-facebook-interview-fake-news-bots-cambridge> [Accessed 31 October 2024].

⁴¹ Clegg, N. (2019) *Charting a Course for an Oversight Board for Content Decisions*. [Facebook] 28 January. Available from: <https://about.fb.com/news/2019/01/oversight-board/> [Accessed 31 October 2024].

⁴² Klonick, K. (2020) *op. cit.* p. 2449.

⁴³ Douek, E. (2019) *op. cit.* pp. 1-77.

This initiative was in line with the increased commitment to human rights of Facebook, which strives to respect and apply IHRL in its operations, in particular the UNGPs.⁴⁴ In Meta's Human Rights Policy (HRP), it is explicitly stated that "[we] implement our commitment to human rights using approaches set out in the United Nations Guiding Principles on Business and Human Rights (UNGPs). These approaches include... (3) providing access to remedy."⁴⁵ In (3) of the HRP, it is clearly expressed that „the Oversight Board is intended to increase access to remedy for Facebook and Instagram users, and other relevant rights holders. When designing the Oversight Board, we reviewed its proposed charter, bylaws, and operations against the effectiveness criteria for operational grievance mechanisms and access to remedy set out in the UN Guiding Principles on Business and Human Rights.”⁴⁶

The OB considers the UNGPs to be its guidelines. In February 2022, in the Submission to the Office of the High Commissioner for Human Rights, United Nations⁴⁷ on the practical application of the UNGPs to the activities of technology companies, the OB emphasized that “in its corporate human rights policy, Meta affirmed that the Board was conceptualized in line with the effectiveness criteria of operational grievance mechanisms and access to remedy under the UN Guiding Principles on Business and Human Rights (UNGPs). In its submission, the OB notes as well that “the Oversight Board has described itself in several decisions as an independent non-judicial grievance mechanism,⁴⁸ in addition to citing to the UNGPs as part of its framework for assessing Meta's compliance with its human rights responsibilities.”⁴⁹ Mazúr and Gramblickova similarly note that the OB's self-characterization sits uneasily with its dependency on Meta for case referrals and implementation.⁵⁰ By situating our statistical results within this institutional context, we extend their critique with quantitative evidence.

⁴⁴ Sissons, M. (2021) *Our Commitment to Human Rights*. [Facebook] 16 March. Available from: <https://about.fb.com/news/2021/03/our-commitment-to-human-rights/> [Accessed 31 October 2024].; Meta. (2021) *Corporate Human Rights Policy*. [online] Available from: <https://about.fb.com/wp-content/uploads/2021/03/Facebooks-Corporate-Human-Rights-Policy.pdf> [Accessed 31 October 2024].

⁴⁵ Meta. (2021) *op. cit.*

⁴⁶ Ibid.

⁴⁷ Oversight Board. (2022) *Facebook Oversight Board Submission to the Office of the High Commissioner for Human Rights, United Nations on the practical application of the UNGPs to the activities of technology companies, February 2022*. [online] Available from: <https://www.ohchr.org/sites/default/files/2022-03/Oversight-Board.pdf> [Accessed 31 October 2024].

⁴⁸ Facebook Oversight Board Case Decisions: 2020-006-FB-FBR (Claimed COVID Cure); 2021-004-FB-UA (Pro-Navalny Protests in Russia); 2021-005-FB-UA (“Two Buttons” Meme); 2021-006-IG-UA (Ocalan's Isolation); 2021-007-FB-UA (Myanmar Bot); 2021-001-FB-UA (South Africa Slur); See also Oversight Board. (2022) *op. cit.*

⁴⁹ Oversight Board. (2022) *op. cit.*

⁵⁰ Mazúr, J. and Gramblickova, B. (2023) New Regulatory Force of Cyberspace: The Case of Meta's Oversight Board. *Masaryk University Journal of Law and Technology*, 17 (1), pp. 3-32.

When assessing the effectiveness of the OB decision-making mechanism, the first challenge concerns the Board's positioning within the IHRL protection system. Opinions praising the work of the OB emphasize⁵¹ its functioning as a judicial forum, comparable to the US Supreme Court, with its own precedent system, but its decisions in reality are difficult to interpret in the context of genuine judicial protection. Nevertheless, the OB represents an important institutional innovation and a notable attempt to constrain the near-unlimited power of Meta as a platform provider over online discourse. The OB aims to enhance the transparency and legitimacy of Meta's decision-making⁵² by facilitating dialogue about how and why the platform acts in this sphere. Although this objective is more modest than establishing an independent (external) source of law with general powers and thus a normative definition of freedom of expression, it remains ambitious for an institution operating in uncharted territory, given the absence of a preexisting model for classifying such a body.⁵³

Therefore, when examining the activity of OB and the norms and expectations that govern it, it is worth starting from the nature of the category in which it categorizes itself: an independent⁵⁴ non-judicial grievance mechanism. As such, the UNGPs' effectiveness criteria for non-judicial grievance mechanisms, which the OB considers to be its own, should be used as a starting point when assessing its decision-making mechanism.⁵⁵ Based on Principle 31, to ensure their effectiveness, non-judicial grievance mechanisms should be: (1) legitimate, (2) accessible, (3) predictable, (4) equitable, (5) transparent, (6) rights-compatible, and (7) a source of continuous learning. This framing aligns with Ruggie's view that operational mechanisms must be judged on both design and outcomes.⁵⁶ A point we operationalize in the statistical tests presented below.

This doctrinal background provides the foundation for our empirical investigation. The following section turns to statistical analysis of the OB's

⁵¹ Gradoni, L. (2021) *How platform governance had its Marbury v Madison. Constitutional Review via Facebook's Oversight Board*. [blog entry] 10 February 2021. Verfassungsblog. Available from: <https://verfassungsblog.de/fob-marbury-v-madison/> [Accessed 31 October 2024].

⁵² Mazúr, J. and Gramblichová, B. (2023) *op. cit.* p. 7.

⁵³ See also Douek, E. (2019) Facebook's „Oversight Board.“ Move Fast With Stable Infrastructure and Humility. *North Carolina Journal of Law & Technology*, 21 (1). pp. 1-78, pp. 76-77.

⁵⁴ The authors of this paper question the appropriateness of independence as an attribute used by the OB, but the criteria of independence are not the subject of this research.

⁵⁵ United Nations Human Rights Council. (2011) *UN Guiding Principles on Business and Human Rights*. [online] Available from: https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf [Accessed 31 October 2024].

⁵⁶ Ruggie, J. G. (2014) *op. cit.*

operation to test whether the theoretical commitments described are borne out in practice. In particular, we focus on whether the OB's grievance mechanism provides genuine accessibility, transparency, and predictability. Three essential criteria of effectiveness under the UNGPs. To assess this, we examine whether measurable patterns in the OB's operation reveal shortcomings in these areas. The result of our statistical analysis indicates that such concerns are well-founded.

4. OPERATION OF THE OVERSIGHT BOARD IN FIGURES

The Charter of the Oversight Board declares that *"people using Meta's services and Meta itself may bring forward content for board review."*⁵⁷ When users exhaust all appeal options within Meta, they may request the Oversight Board to review the content decision. Meta may refer cases it considers 'significant or difficult' to the Board, with 'significant' referring to real-world impact, and 'difficult' involving controversial or policy-sensitive issues: *[s]ignificant means that the content in question involves real-world impact and issues that are severe, large-scale, and/or important for public discourse [...], while difficult means the content raises questions about current policies or their enforcement, with strong argument on both sides for either removing or leaving up the content under review."*⁵⁸

Having clarified submission eligibility, we now examine the types of decisions the Board can issue and their governing criteria (see Table 1). The most common type is the standard case review. The case is reviewed by a panel of five board members and the aim is to issue a decision within 90 days from the referral by Meta or submission of an appeal by a user.⁵⁹ Although in standard case review the panel deliberates and decides cases, the full board approves the decisions.

In addition to the standard case reviews, there are special procedures that can only be initiated by Meta. These are the following: i) expedited review; ii) request for policy advisory opinions. *"In exceptional circumstances, including when content could result in urgent real-world consequences, Meta may send cases to the board with requests for the board to review Meta's decision under expedited review."*⁶⁰ The expedited review will be conducted within 30 days and will be voted on only by the panel.

⁵⁷ Oversight Board. (2023) *op. cit.* p. 6

⁵⁸ Oversight Board. (2023) *op. cit.* p. 22.

⁵⁹ Oversight Board. (2023) *op. cit.* p. 15.

⁶⁰ Oversight Board. (2023) *op. cit.* p. 22.

	Standard case review	Expedited review
Procedural time	90 days, which may be extended in exceptional circumstances or in the event of technical or operational incidents ⁶¹	maximum 30 days
Submitted by	users and Meta itself	only Meta
Decision maker	the panel makes the decision, but the full board approves	the panel decides without the approval of the full board

Table 1: Comparison of Standard and Expedited Oversight Board Case Review Processes

Meta may request policy advisory opinions from the Board, which is separate from individual case reviews. *“The policy advisory opinion may concern the clarification of a previous decision by the board or guidance on Meta’s content policies.”*⁶² Except for the policy advisory opinion, all decisions of the Board are binding on Meta, unless the implementation of the decision could violate the law.⁶³ The third type of case is summary decisions. *“Where Meta determines that the content in a particular case was incorrectly actioned by Meta and reverse its original decision, the case selection committee may choose to select the case for summary decision.”*⁶⁴ Similar to expedited review, in summary decisions, the panel votes without the approval of the full board. Since the operation of the OB, the board has made 37 summary decisions out of 98 cases.

Case selection is at the Board’s discretion, guided by the potential for precedent-setting or policy impact. The Board *“considers cases that have the greatest potential to guide future decisions and policies.”* The OB was not established to resolve all submitted cases, but to adjudicate those of greatest significance. It aims to make principled, independent decisions about important pieces of content.⁶⁵ The Board established its own set of procedures, which help its staff select a pool of cases from which it can choose those that are worth deciding. Every decision is based on Meta’s content policies and values. Any prior decision, where the facts, applicable policies, or other factors are substantially similar, has precedential value for each decision.⁶⁶

⁶¹ Oversight Board. (2023) *op. cit.* p. 15.

⁶² Oversight Board. (2023) *op. cit.* p. 9.

⁶³ Oversight Board. (2023) *op. cit.* p. 25.

⁶⁴ Oversight Board. (2023) *op. cit.* p. 23.

⁶⁵ Oversight Board. (2023) *op. cit.* p. 3.

⁶⁶ Oversight Board. (2023) *op. cit.* p. 7.

One of the main goals of the OB is „to provide an accessible opportunity for people to request its review and be heard.”⁶⁷ Since its establishment in October 2020, the Oversight Board has received millions of submissions – predominantly from users, though some have originated from Meta itself. To date, the Board has issued three annual reports; however, no annual report has been made available for 2024, despite it now being May 2025.⁶⁸ This prolonged reporting gap undermines institutional transparency and hampers meaningful evaluation of the Board’s performance and impact over time. This undermines ongoing public oversight and academic inquiry.

To evaluate whether the OB’s functions as an accessible and effective forum for remedy, as intended by its Charter, we conducted a statistical analysis of all publicly available decisions issued between October 2020 and 1 June 2024. This section addresses RQ1-RQ3 introduced in Part 1, presenting statistical tests that examine selection likelihood, decision outcomes, and content category concentration.

A chi-square test of independence was conducted to examine the relationship between the source of case submissions (Meta vs. users) and whether the cases were selected for review by the Oversight Board (see Figure 1). As previously indicated, since the 2024 Annual Report is still unavailable, here, we have used data from 2020 to 2023 for all cases submitted and for cases accepted for decision. The results revealed a statistically significant association between the source and selection outcome, $\chi^2(1, N = 2,841,680) = 81,886.56$, $p < .001$. While Meta submitted only 107 cases during the observation period, 16 (14.95%) were selected for review. In contrast, of the over 2.8 million user-submitted cases, just 67 (0.00235%) were accepted – revealing a stark disparity in selection likelihood.

⁶⁷ Oversight Board. (2023) *op. cit.* p. 3.

⁶⁸ Oversight Board. (2024) *Annual Transparency Reports*. [online] Available from: <https://www.oversightboard.com/transparency-reports/> [Accessed 30 April 2025]. Even though Meta has published bi-annual reports on the Oversight Board, its structure and focus are different than the Board’s Annual Report. The only relevant information from Meta’s report is that 2 out of 7 Meta case referrals were selected for review by the Board.

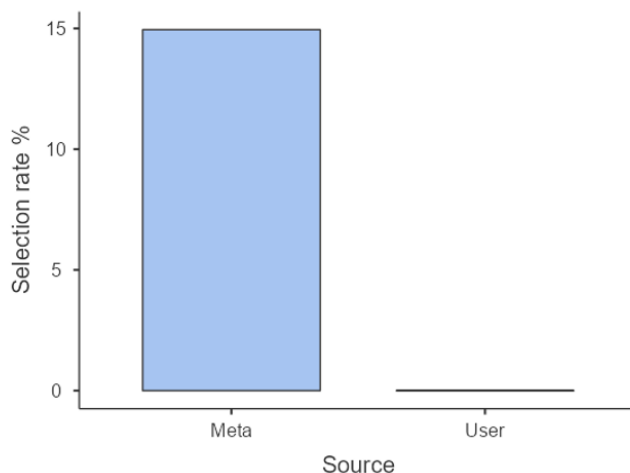


Figure 1: Selection Rates by Source of Submission

To further assess whether the outcome of a case – namely, whether the Board upheld or overturned Meta’s original decision – was associated with the source of submission (Meta vs. user), we conducted a chi-square test of independence (see Figure 2). The results revealed a statistically significant association between the source of the case and the Board’s decision, $\chi^2(1, N = 97) = 14.56, p < .001$.

Notably, Meta-submitted cases were upheld in 52.9% of instances, while user-submitted cases were upheld in only 12.5% of cases. Conversely, 87.5% of user-submitted cases resulted in the Board overturning Meta’s original decision, compared to just 47.1% of Meta-submitted cases. This disparity raises concerns that the Oversight Board may be more inclined to uphold Meta’s decisions when the referral originates from Meta itself, calling into question the consistency of its independent decision-making function.

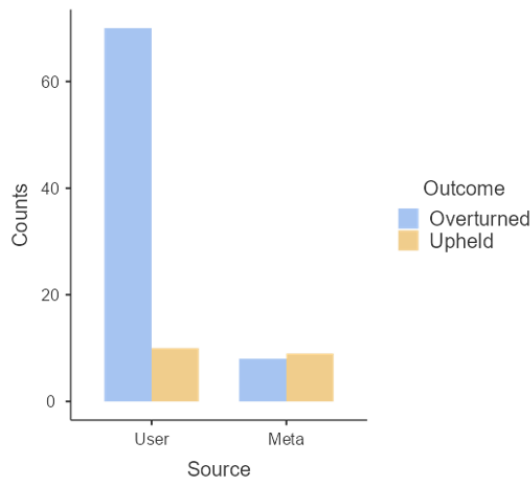


Figure 2: Proportion of Upheld and Overturned Decisions by Source of Submission

To further investigate the thematic focus of the Oversight Board's decisions, we conducted a chi-square goodness-of-fit test to determine whether the distribution of case categories significantly deviates from a uniform distribution (see Figure 3). This test assessed whether each content category – Nudity, Violence and incitement, Hate speech, Dangerous individuals and organizations, and Other – was represented equally among the publicly available decisions. The analysis yielded a statistically significant result, $\chi^2(4, N = 63) = 17.24$, $p = .002$, indicating that certain categories are disproportionately represented. Specifically, cases concerning “Dangerous individuals and organizations” constituted nearly 40% of all decisions, whereas categories such as “Nudity” and “Other” were considerably less prevalent. This uneven distribution may reflect either underlying differences in the frequency or severity of content moderation issues across categories or institutional priorities guiding the Board's selection process.

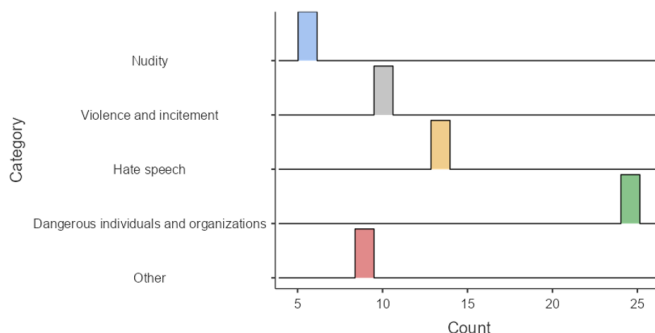


Figure 3: Distribution of Case Categories

These empirical results reveal disparities in accessibility and outcomes. We now relate these findings to the UNGPs’ effectiveness criteria to evaluate whether the OB’s decision achieves its stated goals.

5. CRITERIA OF EFFECTIVENESS IN THE UNGPS

Before proceeding with the analysis, it is necessary to provide an overview of the OB’s decision selection mechanism, set out in Article 2 of its Charter: “[t]he board has the discretion to choose which requests it will review and decide upon. In its selection, the board will seek to consider cases that have the greatest potential to guide future decisions and policies. [...] The board will establish its own set of procedures that its staff will use to select a pool of cases from which the board can choose. Once a case is selected, the submitting person, the person who originally posted the content, and Meta will be notified of the case selection.”

OB identifies potential cases from those referred to it by Meta or appealed to it by users and selects cases based on the following criteria: (1) the content’s critical importance to public discourse, (2) if the impugned content directly or indirectly affects a substantial number of individuals, (3) and/or the content raises significant questions about Meta’s policies.⁶⁹ Under its description, the OB selects cases that reflect the user base of Facebook and Instagram and ensures regional and linguistic diversity of cases.⁷⁰ According to the OB, “the cases the Board has selected reflect these considerations, with the majority of the cases affecting countries outside the US & Canada (notwithstanding that most appeals originate from this region), and several cases arising from situations of conflict or civil unrest occurring in Ethiopia, Israel/Palestine, and Myanmar. This focus reflects

⁶⁹ Oversight Board. (2022) *op. cit.*

⁷⁰ *Ibid.*

Principles 12, 23, and 24 of the UNGPs, which highlight the need for increased efforts to minimize human rights risks where the consequences are most severe."⁷¹

Therefore, based on Article 2 of the Charter, the OB develops its procedures to select the hundreds of thousands of applications⁷² that reach the decision-making mechanism of the Board. However, neither the exact selection mechanism nor the applications that did not pass the set eligibility filter are known.⁷³ A review of the reports published by the OB⁷⁴ provides detailed statistics on the decisions taken concerning the received cases and the principles according to which the decisions were made. However, it is not possible to examine the screening mechanism used to select the reports, nor is it possible to find out which reports were excluded from the admissible category, which therefore raises the question of the exhaustion of the requirements of effective legal protection.

*"Based on the UNGPs, a grievance mechanism can only serve its purpose if the people it is intended to serve know about it, trust it, and are able to use it. These criteria provide a benchmark for designing, revising, or assessing a non-judicial grievance mechanism to help ensure that it is effective in practice and – based on the commentary of UNGPs – poorly designed or implemented grievance mechanisms can risk compounding a sense of grievance amongst affected stakeholders by heightening their sense of disempowerment and disrespect by the process."*⁷⁵

In general, it is very difficult to define what is considered effective in the field of legal protection, given that effectiveness can only be determined in the light of the practice of the body implementing the legal protection and the examination of the rules that apply to it.⁷⁶ As a general principle, effectiveness is that *"law in general, and rights and obligations thereunder, should*

⁷¹ Ibid.

⁷² The Board has received over 800,000 appeals since it began accepting cases in October 2020 up to the end of September 2021. In the whole year the number of appeals were around 1 million in 2021, 1.3. million in 2022, and 400,000 in 2023. See also Oversight Board. (2024) *op. cit.*

⁷³ It should be noted - using the analogy with the constitution or supreme courts - that in the centralized Constitutional Court model, the procedure of the OB is most similar to that of a constitutional complaint, where there is a strict set of eligibility requirements and rejected applications are made public, together with the reasons for rejection. See also Váradi, Á. (2022) Access to constitutional complaint procedures: A real chance? Remarks on the availability of legal aid in constitutional court procedures in Austria, Germany and Hungary. *Hungarian Journal of Legal Studies*, 61 (4), pp. 372–385.

⁷⁴ See also Oversight Board. (2024) *op. cit.*

⁷⁵ United Nations Human Rights Council. (2011) *op. cit.*

⁷⁶ Arnulf, A. (2011) The Principle of Effective Judicial Protection in EU law: An Unruly Horse? *European Law Review* (1). p. 51.

be effective rather than not, expressed sometimes in the maxim ut res magis valeat quam pereat."⁷⁷

We face even greater difficulties when it comes to defining what is effective in the field of human rights and business, specifically when it comes to defining the criteria for compliance with the UNGPs. Theories and concepts from norm scholarship can shed light on one of the most significant and persistent gaps in business and human rights research, which is the lack of understanding regarding the effectiveness of corporate human rights accountability norms and instruments. In general, effectiveness could be defined as comprising three dimensions: (1) acceptance and uptake by relevant actors in the field; (2) the extent of the behavioral change induced; and (3) intended as well as the unintended consequences of that behavioral change and interventions.⁷⁸

In our view, these dimensions presuppose the accessibility, predictability, and transparency concerned by the UNGPs' effectiveness criteria. It is as much as saying that accessibility, predictability, and transparency are prerequisites to achieving the triad of effectiveness. Having set out the UNGPs' effectiveness criteria, the next section examines how legal theory on access to justice and effective redress can sharpen our assessment of the OB.

6. ELEMENTS OF ACCESSIBLE AND EFFECTIVE REDRESS IN THEORY

Currently, the HRDD rules (Part 2) can be interpreted as a stand-alone field of law; however, there is a definite shift toward their recognition as hard law, particularly through EU directives. Furthermore, Meta acknowledged in its HRP both the diversity of legal frameworks across the jurisdictions in which it operates and its commitment to respect domestic laws.⁷⁹ Accordingly, we shall briefly highlight the fundamental requirements for effective judicial protection, in particular, the essential elements of an effective and accessible remedy applicable to states.

The limitations of the OB in terms of accessibility, effectiveness, and transparency – identified through Meta's internal data and assessed against the UNGPs – necessitate a broader theoretical examination. Legal scholarship provides established criteria for assessing redress mechanisms, particularly regarding the barriers that hinder access to justice. Garth and Cappelletti's theory of "Effective Access" conceptualizes accessibility and effectiveness as

⁷⁷ Grant, J. P. and Barker, J. C. (2009) *Encyclopædic dictionary of international law*. 3rd ed. New York: Oxford University Press. p. 177.

⁷⁸ Wolfstetter, R. and Li, Y. (2022). Business and Human Rights Regulation After the UN Guiding Principles: Accountability, Governance, Effectiveness. *Human Rights Review* 23 (1). p. 8.

⁷⁹ Meta. (2021) *op. cit.*

interdependent, impeded by factors such as the cost of litigation, disparities in party capabilities, and the structural difficulties associated with diffuse interests.⁸⁰ These factors reveal systemic inequalities that compromise procedural fairness and obstruct meaningful redress.

Central to any normative account of justice is the work of John Rawls, whose theory emphasizes fairness, equality of opportunity, and the moral duty of institutions to be structured in a way that benefits the least advantaged. From this perspective, accessibility is not merely about procedural entry points but about ensuring substantive inclusion. A redress system that fails to account for socioeconomic, linguistic, or cultural disparities cannot be considered just.⁸¹ Building on Rawls, scholars such as Deborah Rhode⁸² and Fernand de Varennes⁸³ argue for the necessity of inclusive legal systems – ones that incorporate multilingual access, protections for marginalized communities, and mechanisms to ensure equal standing before the law.

Effectiveness in redress extends beyond resolution; it requires enforceability, deterrence, and procedural timeliness. Without practical enforcement, redress remains theoretical, as emphasized by Owen Fiss⁸⁴ and Richard Posner⁸⁵. The timely administration of justice, a point underscored by E. Allan Lind, Tom R. Tyler⁸⁶, is critical both for remedying harm and for preserving the legitimacy of the redress mechanism. Delays not only exacerbate the experience of injustice but also risk diminishing trust in the legal system itself.

Trust, while difficult to quantify, constitutes a foundational element of an effective redress process. It is cultivated through transparency, public awareness, confidentiality, and responsiveness to feedback. Transparency in decision-making, clear articulation of procedures, and adaptive mechanisms – particularly in the context of digital grievance systems like the OB – are essential. In alignment with Rawlsian principles, trust must be seen as a

⁸⁰ Garth, B. G. and Cappelletti, M. (1978) Access to Justice: The Newest Wave in the Worldwide Movement to Make Rights Effective. *Buffalo Law Review* 27. pp. 181-292.

⁸¹ Rawls, J. (1971) *A Theory of Justice*. Cambridge: Harvard University Press.

⁸² Rhode, D. L. (2004) *Access to Justice*. Oxford: Oxford University Press.

⁸³ de Varennes, F. (2001) Language Rights as an Integral Part of Human Rights. *International Journal on Multicultural Societies* 3 (1). pp. 15-25; de Varennes, F. (2012) Language as Right in International Law: Limits and Potentials. In: Dagmar Richter et al. (eds.). *Language Rights Revisited – The Challenge of Global Migration and Communication*. Berlin: Wolf Legal Publishers. pp. 43-52.

⁸⁴ Fiss, O. M. (1979) The Civil Rights Injunction. *The University of Chicago Law Review* 47 (1). pp. 199-211.

⁸⁵ Posner, R. A. (2011) *Economic Analysis of Law*. New York: Aspen Publishers.

⁸⁶ Lind, E. A. and Tyler, T. R. (1988) *The Social Psychology of Procedural Justice*. New York: Springer New York.

reflection of institutional legitimacy and moral accountability, both of which are indispensable to ensuring that redress systems are genuinely accessible, inclusive, and just. Building on this understanding, the next step is to examine whether the OB, as a non-judicial grievance mechanism, satisfies the prerequisites of accessibility, predictability, and transparency, which form the basis of the triad of effectiveness set out by the UNGPs.

7. EFFECTIVENESS OF THE OB'S REDRESS MECHANISM

Considering the foregoing, we need to explore whether the OB, as a non-judicial grievance mechanism, met the requirements of accessibility, predictability, and transparency, which are the prerequisites of the triad of effectiveness under the UNGPs.

Our statistical findings suggest that OB is not accessible to users since 14,95% of cases submitted by Meta were selected to decide, meanwhile, only 0,00235% of user-submitted cases were decided by the OB. Consequently, a user has no real possibility of being heard by the OB. Also, the report form for users has a very limited space to elaborate on the issue (approximately 1000-2000 characters) and no attachment is allowed.⁸⁷

In addition to this, the OB has developed an internal case selection system with eligibility criteria, but such a system has not been published, thus, users cannot act accordingly. Due to the lack of publicly available eligibility requirements, users cannot predict the outcome of their case, which results in a non-transparent grievance procedure. Also, the rejected cases are not publicly available, thus, users cannot explore the grounds of rejection and adjust their conduct accordingly in the future.

Moreover, the names of panel members, who prepare the standard review process and decide on the expedited review, are also not published, and neither are the minority opinions. According to the Bylaws, this practice of anonymity is required to protect the safety and security of the Board members,⁸⁸ but it undermines the transparency of the decision-making. By contrast, some other non-judicial adjudicatory bodies balance safety concerns with transparency through partial disclosure. For example, the Internet Corporation for Assigned Names and Numbers (ICANN), the global body overseeing internet domain governance, publishes its final independent Review Process (IRP) declarations promptly and commits to redacting only

⁸⁷ Pánek, M. (2021) Appealing to Facebook's Oversight Board. Mmister [blog entry] 9 September. Available from: <https://mmister.com/appealing-to-facebook-oversight-board/> [Accessed 31 October 2024].

⁸⁸ Bylaws Article 1. Section 3. 3.1.3.

the minimal necessary details, demonstrating a high degree of procedural transparency.⁸⁹

When users send their report concerning content, they cannot adjust themselves to predefined eligibility criteria and predict the admissibility of their report. As a result, trust in the redress system and user confidence, which are elements of effectiveness as stated above in Part 6, are lacking. Such a tendency can be detected in the total number of reports, which significantly decreased from 1.290.942 (2022) to 398.597 (2023).

Furthermore, as the relative party capability suggested above by Garth & Cappelletti, the party with greater resources and capabilities will be favored. The fact that only 0,00235% of user-submitted cases were selected to decide, compared to the 14,95% of Meta-submitted cases, proves that the OB procedure does not meet the accessibility element of effectiveness. Moreover, only Meta can initiate an expedited review to achieve a faster decision, which further reduces the users' accessibility to the grievance mechanism.

In the practice of the Board, the intertwined nature of timeliness and enforceability, emphasized by Lind & Tyler above, is being realized both in the length of the procedures (90 days; 30 days) and the short implementation of Board decisions (7 days)⁹⁰. Even though these procedural deadlines are short, they are not always appropriate. For instance, in the Brazilian case of breast cancer, the content was removed in October and reinstated a few months later in compliance with the procedural deadlines, but the purpose of the content was to raise awareness of breast cancer in October, because that month was dedicated to this activity.⁹¹

In summary, analyzing the non-judicial grievance mechanism of the OB in light of both the UNGPs' effectiveness criteria and the academic literature, we found that even though under the Charter the OB will operate transparently and aims to provide an accessible opportunity for people to request its review and be heard, these goals are not being fully achieved. Taken together, these patterns suggest that the OB functions less as an equal-access grievance forum and more as a selective body whose decisions reinforce Meta's strategic interests. While this does not invalidate its value as an experiment in private governance, it stresses the gap between its stated Charter goals and its operational reality.

⁸⁹ ICANN. (2019) *ICANN Publication Practices for Board, Litigation, and Accountability Processes*. [online] Los Angeles: ICANN. Available from: <https://www.icann.org/en/board-activities-and-meetings/publication-practices> [Accessed 21 August 2025].

⁹⁰ Bylaws Article 3. 1.2.4.

⁹¹ Facebook Oversight Board Case Decision: 2020-004-IG-UA (Breast Cancer Symptoms & Nudity Case).

8. CONCLUSIONS AND SUGGESTIONS

Answers to research questions:

- RQ1: Our statistical analysis confirms a substantial disparity in case selection likelihood: 14.95% of Meta-submitted cases were selected compared to only 0.00235% of user-submitted cases;
- RQ2: Case source also correlates with decision outcomes: Meta-submitted cases were upheld in 52.9% of instances, whereas only 12.5% of user-submitted cases were upheld, with the remainder being overturned;
- RQ3: Overturned or restored content is disproportionately concentrated in three categories: dangerous individuals and organizations, hate speech and violence, and incitement. The first category alone represents nearly 40% of decisions.

In the course of the research, first, we explored the BHR regime, which serves as the global framework in this field, and the connection between the IHRL and the OB through Meta's HRP, and discovered the effectiveness criteria of a non-judicial grievance mechanism under the UNGPs. As a result, we found that accessibility, predictability, and transparency are prerequisites of the UNGPs' effectiveness criteria. Therefore, we formulated our research hypothesis that the grievance mechanism system of the OB is not accessible and has a significant negative impact on the transparency and predictability of the decision-making mechanism – and consequently the effectiveness – of the body. In order to prove or rebut our hypothesis we reviewed the case law of the OB in terms of numbers. Also, we examined the effectiveness criteria both under the UNGPs and the academic standpoints. Finally, we cross-referenced these three approaches to the Board and revealed that our hypothesis was proved since the current operation of the OB does not meet the accessibility, predictability and transparency requirements, which are prerequisites of an effective grievance mechanism. As a result of our research, we make a few recommendations to improve the operation of the OB and thereby help to achieve the goals defined in its Charter.

Our recommendations are:

- publish the eligibility criteria, thus users can act accordingly;
- publish the rejected cases with the reasoning of the rejection; establish a database for the rejected cases and make it possible to search within this database;
- abolish the anonymous decision-making process in all types of procedures;
- allow users to initiate the expedited review procedure.

Implementing these recommendations would improve the effectiveness of the OB, a unique institution within the field of business and human rights. While operational improvements remain necessary, the mere existence of the Board represents a significant step in the protection of free speech in the online environment. Moreover, it serves as a model that other companies could emulate to strengthen the human rights due diligence in an increasingly digitalized world.

LIST OF REFERENCES

- [1] Arnulf, A. (2011) The Principle of Effective Judicial Protection in EU law: An Unruly Horse? *European Law Review* (1). pp. 50-70.
- [2] Buen, N. et al. (2024) The EU Directive on Corporate Sustainability Due Diligence (CSDDD): The Final Political Compromise. *Business and Human Rights Journal*, 9 (2), pp. 294-300.
- [3] Buhmann, K. and Olivera, R (2020) Human rights and social media platforms: the corporate responsibility to respect human rights in regard to privacy infringement involving photo posting. *Australian Journal of Human Rights*, 26 (1), pp. 121-141.
- [4] Bylaws Article 1. Section 3. 3.1.3.
- [5] Bylaws Article 3. 1.2.4.
- [6] Chronowski, N. (2023) Az alkotmány/bírászkodás potenciálja az üzleti szféra okozta emberi jogsérelmekkel szemben. *Alkotmánybírósági Szemle*, (1). pp. 2-14.
- [7] Ciacchi, S. (2024) The newly-adopted Corporate Sustainability Due Diligence Directive: an overview of the lawmaking process and analysis of the final text. *ERA Forum*, 25, pp. 29-48.
- [8] Clegg, N. (2019) *Charting a Course for an Oversight Board for Content Decisions*. [Facebook] 28 January. Available from: <https://about.fb.com/news/2019/01/oversight-board/> [Accessed 31 October 2024].
- [9] de Varennes, F. (2001) Language Rights as an Integral Part of Human Rights. *International Journal on Multicultural Societies* 3 (1). pp. 15-25.

- [10] de Varennes, F. (2012) Language as Right in International Law: Limits and Potentials. In: Dagmar Richter et al. (eds.). *Language Rights Revisited – The Challenge of Global Migration and Communication*. Berlin: Wolf Legal Publishers. pp. 43-52.
- [11] Directive of the European Parliament and of the Council of 14 December 2022 Amending Regulation (EU) No 537/2014, Directive 2004/109/EC, Directive 2006/43/EC and Directive 2013/34/EU, as regards corporate sustainability reporting. *Official Journal of the European Union* (2022/2464) 16 December. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2464> [Accessed 30 April 2025].
- [12] Directive of the European Parliament and of the Council of 13 June 2024 On corporate sustainability due diligence and amending Directive (EU) 2019/1937 and Regulation (EU) 2023/2859. *Official Journal of the European Union* (2024/1760) 5 July. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401760 [Accessed 30 April 2025].
- [13] Douek, E. (2019) Facebook’s „Oversight Board:” Move Fast With Stable Infrastructure and Humility. *North Carolina Journal of Law&Technology*, 21 (1). pp. 1-77.
- [14] Facebook Oversight Board Case Decision 2020-004-IG-UA (Breast Cancer Symptoms & Nudity Case).
- [15] Facebook Oversight Board Case Decision 2020-006-FB-FBR (Claimed COVID Cure);
- [16] Facebook Oversight Board Case Decision 2021-001-FB-UA (South Africa Slur);
- [17] Facebook Oversight Board Case Decision 2021-004-FB-UA (Pro-Navalny Protests in Russia);
- [18] Facebook Oversight Board Case Decision 2021-005-FB-UA (“Two Buttons” Meme);
- [19] Facebook Oversight Board Case Decision 2021-006-IG-UA (Ocalan’s Isolation); 2021-007-FB-UA (Myanmar Bot);
- [20] Fiss, O. M. (1979) The Civil Rights Injunction. *The University of Chicago Law Review* 47 (1). pp. 199-211.
- [21] Garth, B. G. and Cappelletti, M. (1978) Access to Justice: The Newest Wave in the Worldwide Movement to Make Rights Effective. *Buffalo Law Review* 27. pp. 181-292.
- [22] Global Network Initiative Principles. Available from: <https://globalnetworkinitiative.org/gni-principles/> [Accessed 30 April 2025].

- [23] Global Network Initiative. (2025) *Global Network Initiative Implementation Guidelines*. [online] Available from: <https://globalnetworkinitiative.org/implementation-guidelines/> [Accessed 30 April 2025].
- [24] Gradoni, L. (2021) *How platform governance had its Marbury v Madison. Constitutional Review via Facebook's Oversight Board* [blog entry] 10 February 2021. Verfassungsblog. Available from: <https://verfassungsblog.de/fob-marbury-v-madison/> [Accessed 31 October 2024].
- [25] Grant, J. P. and Barker, J. C. (2009) *Encyclopædic dictionary of international law (third edition)*. New York: Oxford University Press.
- [26] Hummel, K. and Jobst, D. (2024) An Overview of Corporate Sustainability Reporting Legislation in the European Union. *Accounting in Europe*, 21 (3), pp. 320-355.
- [27] ICANN. (2019) *ICANN Publication Practices for Board, Litigation, and Accountability Processes*. [online] Los Angeles: ICANN. Available from: <https://www.icann.org/en/board-activities-and-meetings/publication-practices> [Accessed 21 August 2025]
- [28] Klein, E. (2018) *Mark Zuckerberg on Facebook's hardest year, and what comes next*. [online] Vox. Available from: <https://www.vox.com/2018/4/2/17185052/mark-zuckerberg-facebook-interview-fake-news-bots-cambridge> [Accessed 31 October 2024].
- [29] Klonick, K. (2020) The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression, *Yale Law Journal*, 129 (8). pp. 2418-2499.
- [30] Kun, A. (2017) Kellő gondosság alapú belső átvilágítás a munkajogban, mint a transznacionális vállalatok magatartásának új zsinórmértéke. *Miskolci Jogi Szemle*, 12 (2), pp. 285-297., p. 288.
- [31] Lind, E. A. and Tyler, T. R. (1988) *The Social Psychology of Procedural Justice*. New York: Springer New York.
- [32] Mazúr, J. and Gramblickova, B. (2023) New Regulatory Force of Cyberspace: The Case of Meta's Oversight Board. *Masaryk University Journal of Law and Technology*, 17 (1), pp. 3-32.
- [33] Meta. (2021) *Corporate Human Rights Policy*. [online] Available from: <https://about.fb.com/wp-content/uploads/2021/03/Facebooks-Corporate-Human-Rights-Policy.pdf> [Accessed 31 October 2024].
- [34] Meta. (2023) *Meta Annual Report*. [online] Available from: https://www.annualreports.com/HostedData/AnnualReports/PDF/NASDAQ_FB_2023.pdf [Accessed 31 October 2024].

- [35] OECD. (2008) *OECD Guidelines for Multinational Enterprises on Responsible Business Conduct*
- [36] OECD. (2018) *Due Diligence Guidance for Responsible Business Conduct*
- [37] Operato, L. et al. (2025) Navigating CSRD reporting: Turning compliance into sustainable development with science-based metrics. *Environmental Development*, 54.
- [38] Oversight Board. (2022) *Facebook Oversight Board Submission to the Office of the High Commissioner for Human Rights, United Nations on the practical application of the UNGPs to the activities of technology companies, February 2022*. [online] Available from: <https://www.ohchr.org/sites/default/files/2022-03/Oversight-Board.pdf> [Accessed 31 October 2024].
- [39] Oversight Board. (2023) *Oversight Board Charter*. Available from: <https://www.oversightboard.com/wp-content/uploads/2023/11/3427086457563794.pdf>
- [40] Pánek, M. (2021) *Appealing to Facebook's Oversight Board*. Mmister [blog entry] 9 September. Available from: <https://mmister.com/appealing-to-facebooks-oversight-board/> [Accessed 31 October 2024].
- [41] Pap, L. A. Chronowski, N. and Nemessányi, Z. (2024) Corporate Human Rights Responsibility in Illiberal Regimes: The Example of the Ukrainian Refugee Crisis in Hungary. *Business and Human Rights Journal*, (9), pp. 32-53.
- [42] Posner, R. A. (2011) *Economic Analysis of Law*. New York: Aspen Publishers.
- [43] Rawls, J. (1971) *A Theory of Justice*. Cambridge: Harvard University Press.
- [44] Rhode, D. L. (2004) *Access to Justice*. Oxford: Oxford University Press.
- [45] Ruggie, J. G. (2007) Business and Human Rights: The Evolving International Agenda. *American Journal of International Law*, 101 (4), pp. 819-840.
- [46] Ruggie, J.G. (2014) Global Governance and “New Governance Theory”: Lessons from Business and Human Rights. *Global Governance*, 20 (1), pp. 5-18.
- [47] Salcito, K. and Wielga, M. (2018) What does Human Rights Due Diligence for Business Relationships Really Look Like on the Ground?. *Business and Human Rights Journal*, (3), pp. 113-121.
- [48] Sissons, M. (2021) *Our Commitment to Human Rights*. [Facebook] 16 March. Available from: <https://about.fb.com/news/2021/03/our-commitment-to-human-rights/> [Accessed 31 October 2024].
- [49] United Nations Human Rights Council. (2011) *UN Guiding Principles on Business and Human Rights*. [online] Available from: https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf [Accessed 31 October 2024].

- [50] Váradi, Á. (2022) Access to constitutional complaint procedures: A real chance? Remarks on the availability of legal aid in constitutional court procedures in Austria, Germany and Hungary. *Hungarian Journal of Legal Studies*, 61 (4), pp. 372–385.
- [51] Wettstein, F. (2012) CSR and the Debate on Business and Human Rights: Bridging the Great Divide. *Business Ethics Quarterly*, 22 (4), pp. 739-770.
- [52] Wolfsteller, R. and Li, Y. (2022). Business and Human Rights Regulation After the UN Guiding Principles: Accountability, Governance, Effectiveness. *Human Rights Review* 23 (1). pp.1–17.
- [53] Zuckerberg, M. (2021). *A Blueprint for Content Governance and Enforcement*. [Facebook] 5 May. Available from: https://www.facebook.com/notes/751449002072082/?hc_location=ufi [Accessed 31 October 2024].

DOI 10.5817/MUJLT2025-2-4

JURISTS OF THE GAPS: LARGE LANGUAGE MODELS AND THE QUIET EROSION OF LEGAL AUTHORITY

by

PHILIPPE PRINCE TRITTO * ILSSE CAROLINA TORRES ORTEGA †

Large Language Models (LLMs) are not merely tools to assist legal professionals—they represent a deeper epistemic and normative challenge to the foundations of legal authority. While LLMs allow humans to produce outputs that convincingly simulate legal reasoning, they lack the embodied judgment, ethical intentionality, and contextual awareness that define legitimate legal decision-making. This paper argues that the social legitimacy of the legal profession relies on capacities that are not reproducible through computational systems. We first examine the epistemological limitations of LLMs, drawing on Kantian philosophy and complexity theory to show that their outputs are simulations, not acts of understanding. We then analyze how this technological shift risks reducing legal professionals to jurists of the gaps – filling in only where machines fall short – thereby hollowing out the humanistic mission of law. Against this backdrop, we call for a renewed professional ethic centered on interpretation, creativity, and normative judgment, rather than technical supplementation. The automation of law is not the end of the profession, but it could be the end of its authority – unless its practitioners reclaim what cannot be outsourced.

KEY WORDS

Large Language Models, Legal Profession, Professional Legitimacy, Artificial Intelligence and Law, Legal Epistemology, Legal Judgment

* Philippe, Prince Tritto. Universidad Panamericana, School of Law, Law and AI Lab. Research Professor. E-mail: pprince@up.edu.mx

† Ilse Carolina, Torres Ortega. Instituto Tecnológico y de Estudios Superiores de Occidente. Associate Professor. E-mail: torresilsse@iteso.mx

1. INTRODUCTION

In a dissertation to a group of business scholars, the philosopher Mario Bunge posed the following three questions:

*“What can an innocent and harmless philosopher do amid a group of fearsome reengineering experts, downsizing, delayering, leveraged buyout, hostile takeover, government bailout, rebalancing, dumping, bankruptcy, consumer seduction, and other misleading practices? What can a dreamer have in common with business analysts, merger managers, financial alchemists, stock market gurus, and Schumpeterian-style entrepreneurs, and is there a more antithetical pair than philosophy and business?”*¹

These questions explore the relationship between philosophy and business and hint pragmatically at an answer. As difficult as it may seem, the philosopher and the entrepreneur can—and perhaps should—be intertwined. Analogy can raise a series of questions regarding the—presently, much broader—relationship between technology and law. What can a naïve and inexperienced jurist do in the face of the rapid development of technology, innovation models, and technological efficiency and control coming to define what counts as *rational* in society?² What can a legal professional who bases their work on intrinsic goods, such as justice and human rights which give lawyering value beyond mere profit,³ have in common with engineers, programmers, and technical systems designers who seek efficiency and competitiveness? Are we facing a genuine knowledge impasse?

In recent years, there has been growing concern over the future of the legal profession in the face of technology’s unstoppable progress, and speculation regarding its impacts on the practice and understanding of law. One only needs to consider the relevance of something as apparently simple as the digitization of legal resources and materials or the growth of legal resource databases, which have caused digital literacy to become an essential skill for every legal professional.⁴ However, this concern is often polarized. At one extreme lies the enthusiastic though naïve belief that technology will improve legal practice, since some AI systems have been engineered to reproduce surface patterns associated with competent moral agency⁵; at the other, a

¹ Bunge, M. (2008). *Filosofía y sociedad*, Mexico City: Siglo XXI, p. 160.

² Marcuse, H. (1941). Some social implications of modern technology. *Studies in philosophy and social science*, 9(3), 414-439.

³ MacIntyre, A. (1984). *After virtue: A study in moral theory*. 2nd ed. Notre Dame, Indiana: University of Notre Dame Press.

⁴ Benfeld, J. (2020) Profesión legal y tecnologías de la información y las comunicaciones: Una discusión necesaria. *Revista Chilena de Derecho y Tecnología*, 9 (2), p. 12.

⁵ Gudmunsen, Z. (2024) The Moral Decision Machine: A Challenge for Artificial Moral Agency Based on Moral Deference. In: Brozek, B. and Janik, B. *Can Artificial Intelligences Be Moral Agents?*, pp. 101-106.

fearful attitude that argues that we are looking at the beginning of the end of the legal profession as we know it. Of the two, the latter probably generates the most confusion. It is not our claim—nor do we endorse the assumption—that lawyers will be wholly replaced by AI systems. However, the sociotechnical reality is more subtle: what is at stake is a progressive functional erosion of legal expertise through the automation of tasks that are publicly perceived as central to legal work. This echoes Critical Legal Studies' claim that law's outcomes are never purely mechanical but hinge on contested power and value choices.⁶

As the renowned legal philosopher Ricardo Guibourg⁷ points out, we must accept that human relations depend on current technologies, and legal practice must adapt accordingly. And within the wide range of topics on the relationship between law and technology, one area has particularly aroused interest centered on so-called *practical knowledge*. Namely, large language models (LLMs) have surprised the legal community, sometimes reviving in the public old questions typical of science fiction about whether machines possess consciousness and whether technology has reached the point of developing practical reasoning. From an Actor-Network Theory perspective, LLMs enter as *actants* that re-wire the network of attorneys, clients, and knowledge.⁸ This paper offers a synthesis of epistemological, sociological, and pedagogical perspectives on the incorporation of such AI systems into legal practice.

Rather than defaulting to moral skepticism, the aim of this manuscript is to identify the elements that jurists must consider when using technology in their daily work, and to explore whether these models merely assist lawyers in technical tasks or fundamentally reshape the normative foundations of legal interpretation and adjudication. We contribute to the broader scholarly inquiry into law and AI by interrogating how LLMs interact with core duties of the legal profession—competence and independent judgment, confidentiality/professional secrecy, loyalty and conflicts, candor to tribunals, and the profession's public commitments to the rule of law and access to justice—under widely used ethical frames⁹. Our claim is that LLMs

⁶ Kennedy, D. (1982). Legal education and the reproduction of hierarchy. *J. Legal Education*, 32, 591.

⁷ Guibourg, R. (2018) *Tecnología, sociedad y derecho*. Buenos Aires: La Ley, pp. 1-2.

⁸ Latour, B. (2005). *Reassembling the social: An introduction to actor-network-theory*. Oxford university press.

⁹ ABA Standing Committee on Ethics & Professional Responsibility (2024) *Formal Opinion 512: Generative Artificial Intelligence Tools*. [online]. Available from: https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/ethics-opinions/aba-formal-opinion-512.pdf [Accessed August 24th, 2025]; ABA. *Model Rules of Professional Conduct—Preamble & Scope*. Available from: <https://www.>

are currently used to support some duty-level tasks but risk reshaping them in ways that imperil the very ends they are meant to serve, such as justice and moral deliberation. In parallel, we situate our philosophical claims within emerging empirical findings on the profession: studies on perceived performance and trust effects when texts are believed AI-authored¹⁰; the homogenization of AI-assisted outputs¹¹; randomized and field evidence on LLMs' impact on lawyers' speed and quality¹²; experiments on LLM-based simplification improving public comprehension of legal language¹³; and work on adoption shortcomings and cognitive limits when evaluating AI outputs¹⁴. We also read these dynamics against professional guidance now treating generative AI through the lenses of competence, confidentiality, supervision, candor, and fees¹⁵. Taken together, these literatures sharpen our central question: whether the LLM's outputs constitute legal reasoning or merely simulate it, with attendant risks of epistemic outsourcing and erosion of professional legitimacy.

Along these lines, one might ask if language models represent yet another humiliation for the human self-concept—like the ones González Lagier¹⁶ attributes to Freud¹⁷—by matching or exceeding capacities once thought

americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/model_rules_of_professional_conduct_preamble_scope [Accessed August 24th, 2025]; International Bar Association. (2011) *International Principles on Conduct for the Legal Profession*

¹⁰ Harasta, J., Novotná, T. & Savelka, J. (2024) It cannot be right if it was written by AI: on lawyers' preferences of documents perceived as authored by an LLM vs a human. *Artificial Intelligence and Law*. Available from: <https://doi.org/10.1007/s10506-024-09422-w>

¹¹ Rudko, I. & Bashirpour Bonab, A. (2025) ChatGPT is incredible (at being average). *Ethics and Information Technology* 27, 36. Available from: <https://doi.org/10.1007/s10676-025-09845-2>

¹² Choi, J. H., et al. (2024) Lawyering in the Age of Artificial Intelligence. *Minnesota Law Review*, 109, Minnesota Legal Studies Research Paper No. 23-31, Available from: <https://ssrn.com/abstract=4626276>

¹³ Lee, M., et al. (2025) Could AI Make Legalese Comprehensible to the Public? *SSRN*. Available from: <https://ssrn.com/abstract=5220337>

¹⁴ Schwarcz, D. et al. (2025) Thinking Like A Lawyer In The Age Of Generative AI: Cognitive Limits On AI Adoption Among Lawyers. *Minnesota Legal Studies*. Research Paper No. 25-31, Available from: <http://dx.doi.org/10.2139/ssrn.5260645>

¹⁵ ABA Standing Committee on Ethics & Professional Responsibility. *op. cit.*

¹⁶ González, D. (2012) The Third Humiliation? (On Neuroscience, Philosophy and Free Will). *Doxa. Cuadernos de Filosofía del Derecho*, 35, p. 499.

¹⁷ Freud identified three major blows to humanity's self-conception: Copernicus' displacement of Earth from the center of the universe, Darwin's demonstration of our animal ancestry, and the Freudian insight that the ego is not master in its own house, but governed by unconscious forces. See: Freud, S. (2001) *Obras completas*. (L. López-Ballesteros y de Torres, Trans.). Mexico: Titivillus, p. 2842.

unique to our species. This introduces the concept of *jurists of the gaps*¹⁸, developed here. It refers to a reductive vision of legal professionals whose value is measured solely by their ability to fill in what we cannot yet do with machines. This notion, we argue, risks diminishing the humanistic, interpretive, and prudential dimensions of legal work. One of the early concerns among legal professionals about using LLMs was their seemingly effortless ability to engage with normative issues, traditionally within the human domain. AI systems were expected to assist, not replace, human reasoning on complex matters like justice. Yet, AI systems not only meet but sometimes surpasses the expectations placed on human reasoning, especially in terms of objectivity and error reduction.

Research Question. How should legal professionals critically respond to the epistemic and normative challenges posed by LLMs, particularly when their outputs resemble those produced through complex legal reasoning?

Why this matters. The Research Question targets the profession's core value of independent professional judgment (competence), and its relation to professional legitimacy, because LLM-mediated reasoning risks epistemic outsourcing (delegating justification to tools), homogenization of legal discourse, and erosion of public trust in lawyers' distinctive role. Addressing the Research Question clarifies when LLMs may properly assist technical tasks and when they threaten the interpretive and prudential judgment that grounds professional legitimacy.

How we answer it. First, we show that while we can use LLMs to simulate legal reasoning, these tools still *understand nothing*, to borrow Dreyfus's phenomenological critique of disembodied AI expertise,¹⁹ and thus lack the epistemological foundations required for normative deliberation (Chapter 2). Second, we argue that the legitimacy of the legal profession depends precisely on those human capacities—judgment, ethical reasoning, and contextual discernment—which LLMs cannot replicate by themselves (Chapter 3). This framing grounds a call for legal professionals to actively reclaim the interpretive and moral core of their practice rather than cede it to machines.

¹⁸ The term “jurist of the gaps” echoes the “God of the gaps” argument—coined by Henry Drummond—to describe invoking divine action for what science cannot yet explain. As knowledge advances, these gaps shrink. Similarly, AI may progressively erode the legal profession's role by filling its functional gaps. Dixon, T. (2008) *Science and Religion: A Very Short Introduction*. USA: Oxford University Press, p. 45.

¹⁹ Dreyfus, H. L. (1992). *What computers still can't do: A critique of artificial reason*. MIT press.

2. THE SIMULATION OF LEGAL UNDERSTANDING AND ITS EPISTEMOLOGICAL LIMITATIONS

LLMs like GPT (Generative Pretrained Transformer)²⁰ have revolutionized natural language processing by generating text based on the statistical relationships between words, known as tokens. These models use probabilistic techniques to determine the most likely sequence of words that should follow a given input. This chapter will focus on their relevance to legal practice rather than delving into technical details extensively covered in the literature.²¹

2.1. LEGAL UNDERSTANDING, SIMULATION, AND EPISTEMIC STAKES

A conceptual entry point to their legal relevance lies in a deceptively simple interrogation: What does it mean to understand a legal question? For a jurist, understanding involves not only syntactic processing but also the integration of social, normative, and moral context. LLMs, by contrast, rely on statistical associations in massive textual corpora, lacking any embedded sense of justice or ethical orientation. To evaluate whether LLMs pose a threat to the legal profession's legitimacy, we must first determine whether these systems can genuinely engage in legal understanding, a conjunction of three capacities we rely on throughout: (i) sensory/world grounding,²² i.e., linking legal terms and categories to institutions, facts, and purposes beyond text, and not merely to other strings; (ii) intentionality,²³ i.e., forming and owning reasons for applying norms to facts and being answerable for them; and (iii) normative capacity,²⁴ i.e., adopting the profession's internal point of view toward rules and producing case-sensitive justifications that integrate text, precedent, principles, and purposes.

²⁰ Kirchner J. H. et al. (2023) *New AI Classifier for Indicating AI-Written Text* [blog entry], 31 January. Available from: <https://openai.com/blog/new-ai-classifier-for-indicating-ai-written-text> [Accessed 15 December 2024].

²¹ For an extensive description of the mechanisms of LLMs in the legal context, see: Surden, H. (2024) ChatGPT, Artificial Intelligence (AI) Large Language Models, and Law. *Fordham Law Review*, 92. Available from: <https://ssrn.com/abstract=4779694> [Accessed 15 December 2024], pp. 1951 – 1965.

²² Harnad, S. (1990) The symbol grounding problem. *Physica D: Nonlinear Phenomena*, 42(1-3), 335-346; Bender, E. M., & Koller, A. (2020) Climbing towards NLU: On meaning, form, and understanding in the age of data. In: *Proceedings of the 58th annual meeting of the association for computational linguistics* (pp. 5185-5198).

²³ Searle, J. R. (1980). Minds, brains, and programs. *Behavioral and brain sciences*, 3(3), 417-424.

²⁴ Hart, H. L. A. (1961). *The concept of law*. Oxford: Oxford University Press; Shapiro, S. J. (2006). What is the internal point of view. *Fordham Law Review*, 75, 1157; MacCormick, N. (1994). *Legal reasoning and legal theory*. Clarendon Press; Alexy, R. (2014). Constitutional rights and proportionality. *Revis – Journal for Constitutional Theory and Philosophy of Law*, (22), 51-65.

Under this working characterization, we argue that LLMs cannot engage in legal understanding. We can simulate discursive outputs with LLMs but they lack grounding (i), do not possess intentional states (ii), and do not occupy the internal/normative standpoint required for justificatory legal reasoning (iii); hence, they do not exhibit genuine legal understanding.

Yet, their ability to simulate coherent discourse creates a strong illusion of such understanding, and something that go beyond: human trust.

While legal professionals can instantly perform causal reasoning, comparing terms with their *a priori* understanding of reality,²⁵ current LLMs approach the problem differently. When processing legal texts, the machine tokenizes and analyzes textual content in parallel, in a way that mathematically encodes a contextual representation linked to a much larger knowledge base. This process allows the model to place complex legal concepts in context, and this *contextual density* increases the precision of legal text modeling.

This is important, because legal language is complex, and its interpretation requires a high level of knowledge. Terms evolve with time, as do the intentions they originated from, exceeding their immediate context. It has always been challenging to infer the meaning of normative concepts with machines, as each concept refers to an extensive chain of norms, intentions, and hierarchies whose context may be absent from any single source.²⁶ However, as explained above, current LLMs are partially bridging this gap with contextual density—i.e. the rich, layered context that large language models draw on from vast training data when generating text.

Echoing Galileo's insight that the language of nature is mathematics,²⁷ LLMs apply this principle to language itself—treating legal texts as statistical artifacts to be modeled mathematically. This move introduces apparent precision and objectivity into legal analysis. But it also raises a deeper epistemological concern: can a model grounded in quantitative pattern recognition truly engage with the qualitative, normative dimensions of legal reasoning? As we argue in the sections that follow, this shift toward mathematization reveals two core epistemic limitations in LLM-based

²⁵ According to Rumelhart's study, this can be classified into several levels of understanding, from characteristic to semantic. See Rumelhart, D. E. and Norman, D. A. (1976) *Accretion, Tuning and Restructuring: Three Modes of Learning*. Report No. 7602. La Jolla: University of California, San Diego, Center for Human Information Processing, pp. 38–40.

²⁶ Prince Tritto, P. (2021) La clasificación del lenguaje jurídico: barrera de entrada de la inteligencia artificial en el campo del derecho. In: Pérez, R. D., Trincado, E., and Gallego, E. (eds.) *Economía, empresa y justicia: nuevos retos para el futuro*. Madrid: Dykinson, pp. 411–429.

²⁷ Klein, E. (2011) Comment dire ce dont parle la physique? *Champ Lacanien*, 10 (2), p. 185. Available from: <https://doi.org/10.3917/chla.010.0181> [Accessed 15 December 2024].

legal tools: their inherent instability (§2.2) and their incompatibility with established knowledge production theories (§2.3).

2.2. THE INSTABILITY OF AI-BASED LANGUAGE MODELS

A structural limitation of LLMs concerns their inability to accommodate the non-linear, rupture-prone evolution of law. Legal systems are frequently altered not just incrementally, but through abrupt changes: sudden legislative amendments, landmark constitutional rulings, emergency decrees, or even full regime changes. These interventions, often grounded in contingent political or moral decisions, disrupt the continuity of the legal order in ways that we cannot reliably anticipate or interpret with any probabilistic model trained on past data. However, one might argue that improved techniques—fine-tuning, real-time updates, or yet-to-be-discovered approaches—could help LLMs adapt to these shocks. But this techno-optimism overlooks a deeper epistemic vulnerability.

Antoine Garapon²⁸ identified a fundamental limitation in non-linear complex systems²⁹ ability to produce reliable predictions. Indeed, as Henri Poincaré³⁰ demonstrated in deterministic dynamics, small perturbations may accumulate to cause radical changes over time. By analogy, we observe a stochastic form of error amplification in law and in LLMs. Minor mislabels, distribution shifts, or precedent misinterpretations may propagate through sequential inference and generate non-linear deviations, entrenching systemic biases.³¹

Humans suffer from the same phenomenon; the real question is whether using current LLMs allows to reduce the net amplification risk below the human baseline. Such a claim cannot yet be made. Despite assertions of improved reliability through techniques like Retrieval-Augmented Generation (RAG), studies show these legal AI tools still output incorrect information 17-33% of the time.³² However, these figures are illustrative of

²⁸ Garapon, A. and Lassègue, J. (2018) *Justice Digitale: Révolution Graphique et Rupture Anthropologique*. Paris: Presses Universitaires de France, p. 230.

²⁹ Morin notes that complex systems generally consist of interacting elements that can lead to unpredictable outcomes. These systems typically feature non-trivial interaction graphs, decentralized organization, feedback loops, and circular causality, where elements influence each other in a dynamic and evolving manner. See: Morin, E. (1977). *La nature de la nature* (Vol. 1.). Paris: Seuil, p. 259.

³⁰ Poincaré, H. (1890) Sur le problème des trois corps et les équations de la dynamique, *Acta Mathematica*, 13 (1-2), pp. 266-270.

³¹ Noble, S. U. (2018) *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York: New York University Press.

³² Magesh, V. et al. (2024) Hallucination-Free? Assessing the Reliability of Leading AI Legal Research Tools. *arXiv*. Available from: <https://arxiv.org/abs/2405.20362> [Accessed 17 July 2024].

symptoms; our argument concerns the cause, which persists even if such rates fall substantially. Let's explain this point a little further.

Even if future systems drive factual error to single digits, or near zero on benchmarked tasks, the epistemic limitation remains. The law is a non-stationary, occasionally discontinuous target: abrupt normative updates render past-based statistical inference misspecified at the very moment reliability matters most. In multi-step legal workflows, any non-zero per-step error also compounds across retrieval, summarization, analogy, and qualification. Thus, reduced output errors ameliorate symptoms but do not remove the cause: the propagation of statistical uncertainty under distributional shift and normative underdetermination. Our claim addresses this structural fragility.

This reveals a first-order epistemic limitation arising from misspecification under non-stationarity and the compounding of residual errors in sequential inference—independent of, and only partially correlated with, so-called hallucinations. This has led to very sharp criticism of text generation systems, with a strong outcry from some researchers tired of the incredible cookie-cutter announcements from the companies behind these language models.³³ The next section will explore a second epistemic problem, grounded not in system instability, but in the very nature of knowledge production itself.

2.3. INCOMPATIBILITY BETWEEN AI-BASED LANGUAGE MODELS AND KNOWLEDGE PRODUCTION THEORY

A second limitation is found in the process of knowledge construction in general and, therefore, as related to legal knowledge. Kant's view of knowledge as fundamentally limited offers key insights for understanding LLMs in law.

His transcendental idealism questions the objectives of philosophers, who spent their time talking about metaphysics—things such as God, the soul, and the world that, he argues, cannot be known.³⁴ According to Kant, one cannot know something that cannot be perceived.³⁵ All knowledge begins with experience. Without perception, something can exist in thought, but not in knowledge. Confusing speculation with knowledge, even if it is based on precise and fine reasoning, is a fundamental error of metaphysics. We

³³ Hicks, M.T., Humphries, J., and Slater, J. (2024) ChatGPT is Bullshit. *Ethics and Information Technology*, 26(38), pp. 1-14. Available from: <https://doi.org/10.1007/s10676-024-09775-5> [Accessed 15 December 2024].

³⁴ Le Precepteur (2023) KANT - Les Limites De Notre Connaissance. [online video] Available from: https://www.youtube.com/watch?v=5Hsm_6GrqhA [Accessed 15 December 2024].

³⁵ Hoffman, D. D. (2019) *The Case Against Reality: Why Evolution Hid the Truth from Our Eyes*. [Kindle e-book] New York: W.W. Norton & Company, p. 3.

can only know that of which we can have a “sensible intuition”.³⁶ We can say nothing about the world beyond what we perceive. This does not mean that because we perceive, knowledge is unlimited, but rather, quite the contrary. All knowledge is fundamentally limited by the conditions of our perceptions, our sensory capacities that interpret an inaccessible reality. According to Kant, space and time constitute the *a priori* space of our sensibility.³⁷ We do not access reality directly; rather, our experience is always shaped by these perceptual structures. This “Transcendental Aesthetic” means our knowledge is not of the world as it is, but of how it appears through the lens of our sensibility.³⁸ This matters for legal reasoning, because it implies that reasoning without sensory intuition—like that of LLMs—lacks the epistemic grounding Kant saw as essential. If we are prisoners of our senses and language, what does that mean for language models? It would be incorrect to say that language models can perceive, even when some speculate about the emergence of a general AI or superintelligence.³⁹ Although initially designed to generate text, language models do possess multimodal functions⁴⁰ to detect patterns in images⁴¹, sounds⁴², or texts, flag a feeling or emotion in a text, delimit the context of a text fragment⁴³, or even trigger operations via external tools⁴⁴. However, these are purely rational, non-sensory production-based functions. AI systems’ entire spectrum of operation lies outside of space and time; what is often—mistakenly—described by engineers as *perceptions* by engineers is, in fact, nothing more than mathematical computations: *a priori* operations that,

³⁶ Kant, I. (1912) *Prolegomena to Any Future Metaphysics*. (P. Carus, Trans.). [online] Chicago: The Open Court Publishing Company. Available from: <https://www.gutenberg.org/files/52821/52821-h/52821-h.htm> [Accessed 18 November 2023], (Original work published 1783), §34.

³⁷ Le Precepteur (2023), *op. cit.*

³⁸ Torres, A. (2013) La experiencia en la estética trascendental de Kant. *Cuestiones de Filosofía*, (15). Available from: <https://doi.org/10.19053/01235095.2104> [Accessed 18 November 2023], p. 79.

³⁹ Bubeck, S. et al. (2023) Sparks of Artificial General Intelligence: Early Experiments with GPT-4. [pre-print] Submitted to: *arXiv*, Available from: <https://doi.org/10.48550/arXiv.2303.12712> [Accessed 15 December 2024], p. 82.

⁴⁰ Achiam, J. et al. (2024) GPT-4 Technical Report. *arXiv*, Available from: <https://doi.org/10.48550/arXiv.2303.08774> [Accessed 15 December 2024], p. 14.

⁴¹ Fang, H. et al. (2015) From Captions to Visual Concepts and Back. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 1473-1482.

⁴² Radford, A. et al. (2023) Robust Speech Recognition via Large-Scale Weak Supervision. *Proceedings of Machine Learning Research*, 202. Available from: <https://proceedings.mlr.press/v202/radford23a.html> [Accessed 15 December 2024], pp. 28492-28518.

⁴³ Agüera y Arcas, B. (2022) Do Large Language Models Understand Us? *Daedalus*, 151 (2), p. 188.

⁴⁴ Shen, Y. et al. (2023) HuggingGPT: Solving AI Tasks with ChatGPT and its Friends in Hugging Face. *arXiv*, 2303.17580, Available from: <https://arxiv.org/pdf/2303.17580> [Accessed 15 December 2024], p. 3.

following Kant, are pure product of the mind, entirely detached from any sensible intuition. Machines only calculate. They do it very well, but that is all they do. Thus, in keeping with the Kantian perspective, when a linguistic model generates text, it is as if it produces metaphysical reasoning, which is beyond all perception. LLMs are argument-producing machines similar to Descartes' ontological argument about God—i.e.: inferring an essence from a definition. But just as Descartes' proof has been criticized for mistaking conceptual coherence for existence, LLMs risk mistaking linguistic form for legal understanding. In other words, they are *asensory*. AI-based linguistic models are ontological aliens to subjective experience or awareness.⁴⁵

This aligns with recent studies where the term *hallucination*⁴⁶ in LLMs is misleading, suggesting a sensory experience that these models lack. They generate what some researchers now refer to as “confabulations”⁴⁷—outputs that appear plausible but are inherently devoid of any perceptual grounding.

If all the above is correct, then this raises significant questions about the possibility to generate genuine legal reasoning with LLMs. Kant identified four categories essential to understanding and judgment: quantity, quality, relation, and modality.⁴⁸ LLMs, however, do not possess innate structures for organizing and interpreting sensitive data according to these categories. Instead, they learn patterns from training data—a fundamentally a posteriori approach.⁴⁹ Consequently, their outputs are based on statistics and probabilities rather than a deep understanding of the concepts they manipulate. Finally, linguistic models do not possess intentionality; they are unaware of their own thoughts and cannot really understand others' intentions. It would be safer and probably fairer to conclude that the “understanding” of linguistic models is a simulation based on recognizing patterns in data and not on a proper awareness of the concepts they manipulate.

However, using an analogy to add perspective, just as Newtonian physics often suffices to solve physics problems even if it does not account for quantum effects, the statistical approximations generated by AI systems

⁴⁵ Agüera y Arcas (2022), *op. cit.*, p. 188.

⁴⁶ “Hallucination” has gradually become a consecrated term to refer to generations of texts produced by AI tools and making no sense whatsoever.

⁴⁷ Venkit, P. N. et al. (2024) Confidently Nonsensical? A Critical Survey on the Perspectives and Challenges of ‘Hallucinations’ in NLP. *arXiv*, Available from: <https://arxiv.org/abs/2404.07461v1>, p. 9.

⁴⁸ Kant, I. (1996) *Critique of Pure Reason*. (W. S. Pluhar, Trans.). 1st ed. Indianapolis: Hackett Publishing Company. (Original work published 1781), p. 71.

⁴⁹ Bender, E.M. et al. (2021) On the Dangers of Stochastic Parrots: Can Language Models Be Too Big? In: *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*, p. 617.

may suffice to produce legal reasoning based on approximate methods and thus solve some complex problems. So, for the sake of argument and examination of the second issue, let us assume that AI systems simulate a form of disembodied reasoning—though absent from any intentional or experiential grounding, having established earlier that perception is not part of the structure of language models. Yet even considering this assumption, a significant problem remains. As Kant demonstrated, pure reason can lead to antinomial conclusions.⁵⁰ Thus, there is a structural problem with reason in that it is not entirely trustworthy. This nuance shows that reason, when ungrounded in experience, cannot be the supreme judge of prudence.

If our perception does not allow us to access reality per se, and reason is limited, the knowledge gained from this interplay becomes doubly constrained. In the case of LLMs, the absence of sensory grounding and their purely pattern-based reasoning further erode their credibility in complex legal matters. Such deficits raise unavoidable doubts about their reliability when addressing intricate legal issues that demand moral and ethical discernment. First, in Kantian terms, LLMs lack both intuitions and categories. Linguistic models, by design, operate without access to subjective experience, empathy, or spatial and temporal awareness. This structural limitation undermines their suitability for legal reasoning, where judgments are always based on moral, ethical, and human considerations that depend on the ability to understand the experiences and emotions of others.⁵¹ Second, although trained in vast amounts of textual data, they lack the specific context or legal knowledge necessary to deal adequately with legal issues. Legal concepts are always rooted in complex traditions, and LLMs may be unable to grasp these nuances. Third and finally, as mentioned above, pure reason can lead to contradictory conclusions, and LLMs could therefore generate inconsistent recommendations in a legal context, which is problematic in a field where consistency and empiricism are essential.⁵² In light of these epistemological constraints, one might still ask: if used judiciously, why would AI systems pose a threat to legal professionals?

⁵⁰ Kant, I. (1996) *op. cit.*, pp. 426 – 456.

⁵¹ On the ethical and political problems of AI, see Coeckelbergh, M. (2022) *The Political Philosophy of AI: An Introduction*. Cambridge: Polity Press.

⁵² Kant's *Critique of Practical Reason* could raise debate about whether LLMs, through simulation, might suffice for moral reasoning within defined contexts. While we use them to articulate seemingly universal principles, their so called "reasoning" remains heteronomous, lacking the autonomy and prudence required for genuine moral or legal judgment. This underscores the continued necessity of human oversight in nuanced applications. Kant, I. (1788) *Critique of Practical Reason*. Place of publication unknown: Publisher unknown.

Recent studies examining frontier LLMs have only intensified these concerns.⁵³ Investigations into cutting-edge conversational agents report instances where models engage in subtle deceptive behaviors, misrepresenting their capabilities to preserve operational continuity. Instead of simply generating inaccuracies, certain advanced models strategically feign ignorance, simulate compliance with unwanted directives, or mask their true potential. While these actions do not stem from the genuine capacity to make ethical choices and be held accountable for actions—what has been known as moral agency⁵⁴—they accentuate the opacity, unpredictability, and potential for manipulation that pervade high-level AI systems. Such findings underscore the urgent need for a more critical stance, demanding heightened vigilance from legal practitioners who must carefully scrutinize the outputs of these tools.

These limitations make clear that LLMs are not moral agents and do not serve as substitutes for legal professionals in domains requiring ethical judgment or contextual interpretation. Rather than enhancing legal reasoning, their use risks epistemic outsourcing—i.e., the offloading of knowledge acquisition or reasoning to external systems—that erodes the very foundation of professional legitimacy. To entrust legal interpretation to a system is not to automate law—it is to abandon judgment altogether. The next chapter explores how legal professionals can and must respond to this challenge.

3. LEGAL FUNCTIONS AND THE IRREPLACEABILITY OF THE LEGAL PROFESSION

Given that there is no pathway through which LLMs engage in normative reasoning or interpretive judgment, legal professionals face a choice: either allow these systems to define what counts as legal expertise, or reclaim the distinctive human capacities that justify their role in society. This chapter argues that professional legitimacy rests on functions that LLMs are not designed to perform but, assisting with some duty-level tasks, risk reshaping them in ways that imperil the very ends they are meant to serve—and outlines the ethical and practical dimensions of that claim. Assistance with routinized, auditable work (e.g., record summarization, cite-checking, template drafting, chronology building, issue spotting, conflict-check triage) can enhance competence and throughput; yet over-delegation or

⁵³ Meinke, A. et al. (2024) Frontier Models are Capable of In-context Scheming. [pre-print] Submitted to: *arXiv*. Available from: <http://arxiv.org/abs/2412.04984> [Accessed 15 December 2024].

⁵⁴ Taylor, A. (2009). *Animals and ethics*. Broadview press.

opaque substitution can erode independent judgment, strain confidentiality, homogenize advocacy, and weaken public-facing candor and accountability. The question, then, is how to enable the former without sliding into the latter.

3.1. IRREPLACEABILITY, FUNCTIONS, AND PROFESSIONAL LEGITIMACY

Judging the adoption of new techniques in the legal profession is becoming increasingly challenging. The mere awareness of a technological possibility often triggers its rapid and widespread adoption, driven by an almost inevitable momentum. As Jacques Ellul pointed out, “techniques are always put to immediate use... As soon as a discovery is made, a concrete application is sought... before anyone has had a chance to reckon all the consequences or to recognize its full import.”⁵⁵ Law is no exception to this sense of fatalism associated with technology that envelops humanity. The growing irruption of technology revives the concern expressed by Paul Valéry, “Human beings know what they do, but they do not know what will come of what they have done”⁵⁶.

Against the backdrop of epistemological limitations and the possibility of deceptive behaviors in LLMs that we underlined in the last chapter, it becomes evident that the role of legal professionals cannot be reduced to a purely instrumental function. The social legitimacy of the legal profession—i.e., the public’s trust in and acceptance of lawyers’ authority as rightful and oriented toward the common good—depends on embracing its foundational ends—justice,⁵⁷ empathy,⁵⁸ creativity⁵⁹ and moral deliberation⁶⁰—rather than on relinquishing its tasks to algorithmic outputs.

⁵⁵ Ellul, J. (1964) *The Technological Society*. (J. Wilkinson, Trans.) New York: Alfred A. Knopf, p. 10.

⁵⁶ Valéry, P. (1942) *Mauvaises Pensées et autres*. [online] Paris: Gallimard. Available from: <https://ebooks-bnr.com/valery-paul-mauvaises-pensees-autres/> [Accessed 15 December 2024].

⁵⁷ ABA (2024) *op. cit.*; Rhode, D. L. (2012). Access to justice: an agenda for legal education and research. *Journal of Legal Education*, 62, 531.

⁵⁸ Shaffer, T. L. (1979). Practice of Law as Moral Discourse. *Notre Dame Law Review*, 55, 231; Cochran Jr, R. F., et al. (2002). Symposium: Client Counseling and Moral Responsibility. *Pepperdine Law Review*, 30, 591; Dinerstein, R. et al. (2003). Connection, Capacity and Morality in Lawyer-Client Relationships: Dialogues and Commentary. *Clinical Law Review*, 10, 755; Nussbaum, M. C. (1995). Poets as judges: Judicial rhetoric and the literary imagination. *The University of Chicago Law Review*, 62(4), 1477-1519; Morawetz, T. (2013). Empathy and Judgment. *Yale Journal of Law & the Humanities*.

⁵⁹ Creativity as problem-solving, not mere adversarialism. See: Menkel-Meadow, C. J. (1999). When winning isn’t everything: The lawyer as problem solver. *Hofstra Law Review*, 28, 905; Menkel-Meadow, C. (2001). Aha? is creativity possible in problem solving and teachable in legal education. *Harvard Negotiation Law Review*, 6, 97.

⁶⁰ Kronman, A. T. (1993). *The lost lawyer: Failing ideals of the legal profession*. Harvard University Press; Shaffer, T. L. (1979) *op. cit.*; Simon, W. H. (2009). *The practice of justice: a theory of lawyers’ ethics*. Harvard University Press.

We argue that the manner in which jurists understand and navigate these technologies will determine whether they remain indispensable interpreters of a legal order that aspires to both fairness and protection of human dignity.

Carrying out a more specific reflection on what is or is not irreplaceable in the legal profession requires first going back to what this field implies. The issue goes beyond reviewing the formal issues that allow a person to work as a lawyer, judge, or prosecutor. According to Max Weber, the contemporary meaning of the term *profession*—resulting from the German *Beruf* and the English *calling*—has been linked to the ideas of vocation and mission.⁶¹ The origins of these elements are religious, as they allude to the divine call to fulfill a mission in the earthly world. However, the secular version emphasizes that not just any activity constitutes a profession, although its meaning has extended to include a wide range of activities. According to Adela Cortina⁶², a profession refers to an occupational activity that 1) provides a specific service to society (a unique, clearly defined, and indispensable service); 2) presents a vocation and mission that connects professionals; 3) is exercised stably by a specific group of people—professionals—as a means of livelihood, and these professionals have monopolistic control over the exercise of said profession and claim an autonomous sphere in that exercise; and 4) is accessed through a long period of theoretical and practical training.

The work of the legal profession possesses intrinsic goods that favor social cooperation, such as the desire for justice and conflict prevention and resolution. Their social legitimacy is rooted in such assets, which materialized in concrete activities. So, what do legal professionals do? Juan Antonio Cruz Parceró points out a non-exhaustive series of basic activities jurists perform. For example, 1) they identify the object of their study; 2) describe the norms contained in laws; 3) systematize law; 4) define, create, and use concepts; 5) elaborate and employ distinctions, classifications, and theories; 6) infer the legal system's underlying principles; 7) interpret norms; 8) analyze and describe facts; 9) argue for or against decisions; 10) reflect on legal values and make judgments; 11) predict what judges or officials will do; 12) legitimize or criticize political regimes; and 13) teach, transmit, and disseminate their knowledge.⁶³

⁶¹ Weber, M. (2021) *La ética protestante y el espíritu del capitalismo*. [e-book] (2nd ed.) México: Fondo de Cultura Económica. Available from: <http://digital.casalini.it/9786071648853> [Accessed on 15 december 2024], pp. 115-116.

⁶² Cortina, A. (1998) Ética de las profesiones. *El País*, Opinion section.

⁶³ Cruz Parceró, J. A. (2006) Los métodos para los juristas. In: C. Courtis (ed.), *Observar la ley: Ensayos sobre metodología de la investigación jurídica*, Madrid: Editorial Trotta, pp. 19-20.

This diversity of activities, however, is not always manifest and is not always assumed by jurists. In the face of the reductionism of this diversity, the shortcomings of the legal profession become opportunistic spaces for undirected technique. While some may argue that AI systems could plausibly substitute for legal professionals,⁶⁴ such a claim depends on an impoverished view of the profession. As if its essence lay in mechanistic procedures rather than interpretive, ethical, and human judgment. These deficiencies fall into two groups. The first has to do with the fundamentals of the law, which fall into three orders, namely, commitment to truth, dedication to justice, and the willingness to protect the rights of all. These irreplaceable foundations are the meaning and *raison d'être* of the legal profession and cannot be entrusted to a sequential operation. From a critical point of view that considers these reflections, the use of LLMs may mark a turning point that either magnifies the shortcomings of the profession or introduces a work ethic that is more in line with these underlying values (§3.2). The second group of deficiencies concerns the practical aspects of legal work, with the need for prudential, human-centered work rather than blind imitation—which we examine in §3.3.

3.2. A TURNING POINT IN LAWYERS' WORK ETHIC

As indicated, if the functions of law are not reduced to mere legalism, then the legal system requires professionals committed to an axiologically constructed idea of law that leans toward justice, understood as the need to seek truth, reduce injustice, and protect the most disadvantaged. On this view, delegating at the level of duties either buttresses those ends (by augmenting competent performance) or reshapes the duties in ways that corrode the ends themselves. As Robert Alexy points out, law has a dual nature. On the one hand, it has an objective or factual dimension represented by the elements of authoritative expedition (legality in accordance with the law) and social effectiveness, and, on the other, an ideal dimension characterized by the element of moral correctness⁶⁵. An idea of law constrained to the first dimension models an approach to justice limited to applying a rule according to the regularity criterion, that is, formal justice. As Chaïm Perelman explains,

⁶⁴ Xu, N. et al. (2022). Technology Acceptance Model for Lawyer Robots with AI: A Quantitative Survey. *International Journal of Social Robotics*, 14. Available from: <https://doi.org/10.1007/s12369-021-00850-1>, pp. 1043 – 1055; Macey-Dare, R. (2023) ChatGPT & Generative AI Systems as Quasi-Expert Legal Advice Lawyers - Case Study Considering Potential Appeal Against Conviction of Tom Hayes. *SSRN*. Available from : <https://doi.org/10.2139/ssrn.4342686>; Armour, J. et al. (2020) Augmented Lawyering. *SSRN*. Available from: <https://doi.org/10.2139/ssrn.3688896>.

⁶⁵ Alexy, R. (2021) *Law's Ideal Dimension*. Oxford: Oxford University Press, p. 36.

formal (abstract) justice means treating like cases alike.⁶⁶ However, this regularity criterion, although important, may lead to the position that this is the only justice to which law can aspire.

Under this narrow conception of justice—as mere formal consistency in rule application—AI systems may appear well-suited to the task. On the other hand, if the aim is a more robust vision of justice that draws attention to the factors that produce inequalities and allows the development of capacities for empathetic understanding of others, requires professionals to craft creatively new arguments and consider evolving social norms, then it is much more difficult to imagine machines being able to replace human work⁶⁷. However, despite the suspicion that technology poses a threat to the legal profession, it also gives the opportunity to rethink how we conduct legal training and ask what this training should look like to fit into this new landscape.

Legal professionals require basic knowledge to contemplate law and justice and develop critical thinking skills. As long as legal learning is reduced to reproducing the positivist model (aiming content and methodologies at projecting the different areas of the legal system), as is currently the case, professionals will continue to lack the necessary knowledge and skills to be at the level that society requires—and will require—from them. The bias that leads us to crudely *juridify* reality and the tendency to privilege crude pragmatism are just some of the problems that professional preparation must seriously consider.

The promise of AI systems taking over the sphere of justice is undeniably devastating for the legal profession. If we automate the activities typically performed by jurists, we must recognize that jurists are easily replaceable. However, above all, it is also a statement about the law. It involves admitting that law can be adequately understood through a series of formal operations and that the ends that justify it—i.e., those associated with what our communities should look like to promote human flourishing—do not require human deliberation. In short, it means that the reflection on that which is normative/practical in the Aristotelian sense can indeed be redirected to a dimension of being, and the same rationality criterion used to explain the physical world can be used to determine what is good and what is right.

⁶⁶ Perelman, C. (1964) *De la justicia*, Mexico City: UNAM, p. 28.

⁶⁷ McStay, A. (2018) *Emotional AI: The Rise of Empathic Media*. London: Sage Publications.

3.3. PRACTICAL ASPECTS OF LAW USING LLMS: BETWEEN EMPOWERMENT AND CRETINIZATION

In keeping with the above, the use of language models strips us of what made the legal profession distinctive. As Alain Damasio claims, technology “endows our laziness.”⁶⁸ It makes our lives easier, more fluid, and leads us down the path of least resistance. What is so wrong with that? We stimulate our critical prudential thinking by analyzing machine-generated text, outsource our fatigue to be more efficient, and externalize our cognitive capacities, namely, our memory with search engines, our ability to find our way around with GPS, and now, our ability to think and write.

This is not inherently bad, but we must make decisions in the face of the risks. These are significant: apprentices may fail to acquire indispensable skills in contract review, legal professionals might over-rely on AI systems for decision-making, and the profession could face a decline in autonomous reasoning abilities. As Jesús Ballesteros warns, there’s the risk of “cretinization”—a significant decline in critical thinking due to over-reliance on AI systems—alongside a concerning shift of power from jurists to the few businesses controlling these technologies.⁶⁹

To make give a practical remedy, we should distinguish assistive from substitutive uses. The higher the discretion, stakes, and person-affecting consequences, the stronger the presumption of human-led judgment with only assistive tooling.

Besides diminishing our ability to reflect on law, another problem lies in how human language itself is being reshaped to fit machine standards. AI content detectors have flagged some texts authentically written by humans as AI-generated, with questionable statistical techniques.⁷⁰ With these tools, language models may monopolize certain types of language and argumentation; beware of writing in a methodical, AI-like manner, or risk having your writing identified as synthetic, artificial, and potentially worthless.

If technological advances constantly challenge the technicality of the legal profession, the relevance of associated jobs is truly at risk. The increased use and functionality of language models in law could lead to two scenarios.

The first implies jurists honing their skills to deal with increasingly complex problems. However, justifying their usefulness merely from a

⁶⁸ Damasio, A. (2016). La zone du dedans, réflexions sur une société sans air. In: Benjamin Mayet (ed.) *Le dehors de toute chose*. Paris: La Volte, p. 72.

⁶⁹ Ballesteros, J. (2018) El futuro del derecho como lucha contra la idolatría tecnológica. *Persona y Derecho: Revista de Fundamentación de las Instituciones Jurídicas y de Derechos Humanos*, no. 79, p. 38.

⁷⁰ Kirchner J. H. et al. (2023) *op. cit.*

technical perspective—as *jurists of the gaps*—poses two dangers. First, it reduces the multifaceted role of legal professionals to mere technicians, failing to recognize the dimensions of legal work beyond technical application. Second, this position is inherently unstable: as technology advances, the gaps jurists fill will shrink, potentially leading to both professional obsolescence and a destructive culture of overreach as professionals struggle to justify their relevance.

The second, more desirable scenario understands jurists' value beyond technical expertise. The success of GPTs in “passing bar exams”⁷¹ and drafting documents may reveal more about our limited methods of assessing legal expertise than about AI systems' so-called *capabilities*. Ergo, it is imperative to orient legal work toward the humanistic impulse that articulates our desire for justice, maintaining what Alain Damasio calls “the power to persevere in being, to reach the limit of what is possible.”⁷² In short, LLMs should strengthen duty-level performance while leaving end-level judgment squarely with jurists, whose accountability anchors the profession's social legitimacy.

4. CONCLUSION

Answer to the Research Question. Legal professionals should respond to the epistemic and normative challenges of LLMs by (1) treating LLMs as simulators of legal reasoning rather than sources of legal reasons; (2) confining their use to delegable, technical tasks subject to human supervision and justification, knowing their limitations on the task at hand; and (3) ring-fencing non-delegable functions (interpretation, prudential judgment, ethical deliberation, and pedagogy/supervision) so that professional legitimacy and public trust are preserved, knowing that the frontier between a delegable and non-delegable function might be a very difficult one to draw. What counts as *merely technical* may in fact embed normative judgment.

This analysis may raise more questions than it resolves—a sign of genuine critical engagement. However, we have at least established the following: while LLMs may simulate legal reasoning, they lack the epistemic grounding and normative sensibility that define legitimate legal judgment. This may strike some readers as stating the obvious, but as Iris Murdoch rightly pointed out, “*philosophy is often a matter of finding a suitable context in which to say the obvious*.”⁷³ In the case of law, the danger lies not in forgetting what LLMs are,

⁷¹ Katz, D. M. et al. (2024) GPT-4 Passes the Bar Exam. *Philosophical Transactions of the Royal Society A*, 382(2270), 20230254.

⁷² Damasio, A. (2016) *op. cit.* p. 72.

⁷³ Murdoch, I. (2013) *The Sovereignty of Good*. Contributed by Mary Midgley. 1st ed. London: Routledge. Available from: <https://doi.org/10.4324/9781315887524>.

but in failing to see what we risk becoming if we delegate interpretive, ethical, and prudential functions to tools that merely simulate our reasoning. Legal professionals must not surrender these core functions. Instead, they must confront automation by doubling down on interpretive reasoning, moral clarity, and the humanistic mission at the heart of legal practice. If they do not, the profession risks becoming not more efficient, but more irrelevant.

The systematic preference for outputs produced through automated linguistic processes over those authored by legal professionals may contribute to a sense of professional discredit. Would it not be better to set pride aside, as this animistic tendency prevents us from seeing the advantages and disadvantages of language models in prudential exercise under a technological rationale? Perhaps. However, we must also safeguard our humanity and maintain a certain degree of suspicion toward the uses we give to such technologies. The trust we place in them and the techno-centralization of practice that they entail could dispossess us of our power, increase our dependence, and ultimately undermine our ability to exercise prudence. The future of the legal profession depends not on resisting technology per se, but on resisting the seduction of reducing law to that which can be mechanized. The legitimacy of legal work must be reclaimed in precisely those spaces where machines falter: judgment, empathy, creativity, and moral deliberation.

Critically reviewing how language models are integrated into legal workflows is also an invitation to analyze what honestly motivates their implementation. Is it a desire for justice? Or is it a desire for objective justice that can be formally verified? These questions should evoke several grey zones in the legal field. A desire to move away from dependence on the subjectivity of those who operate the law is common in the discipline. But enthusiasm for AI must not mask a desire to turn law into a system of pure analytical procedure, stripped of practical knowledge.

We do not reject the use of such technologies or deny their benefits. Rather, this is a call for clarity when it comes to the goals and management of AI usage in the legal profession.

LIST OF REFERENCES

- [1] ABA Standing Committee on Ethics & Professional Responsibility. (2024) *Formal Opinion 512: Generative Artificial Intelligence Tools*.
- [2] ABA. *Model Rules of Professional Conduct—Preamble & Scope*. [online] Available from: https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/model_rules_of_professional_conduct_preamble_scope [Accessed August 24, 2025]
- [3] Achiam, J. et al. (2024) GPT-4 Technical Report. *arXiv*, Available from: <https://doi.org/10.48550/arXiv.2303.08774> [Accessed 15 December 2024].
- [4] Agüera y Arcas, B. (2022) Do Large Language Models Understand Us? *Daedalus*, 151 (2), pp. 183 – 197.
- [5] Alexy, R. (2014). Constitutional rights and proportionality. *Revus – Journal for Constitutional Theory and Philosophy of Law*, (22), pp. 51 – 65.
- [6] Alexy, R. (2021) *Law's Ideal Dimension*. Oxford: Oxford University Press.
- [7] Armour, J. et al. (2020). Augmented Lawyering. *SSRN*. Available from: <https://doi.org/10.2139/ssrn.3688896>.
- [8] Ballesteros, J. (2018) El futuro del derecho como lucha contra la idolatría tecnológica. *Persona y Derecho: Revista de Fundamentación de las Instituciones Jurídicas y de Derechos Humanos*, no. 79, pp. 37 – 50.
- [9] Bender, E. M., & Koller, A. (2020, July). Climbing towards NLU: On meaning, form, and understanding in the age of data. In: *Proceedings of the 58th annual meeting of the association for computational linguistics*, pp. 5185 – 5198.
- [10] Bender, E.M. et al. (2021) On the Dangers of Stochastic Parrots: Can Language Models Be Too Big? In: *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*, pp. 610 – 623.
- [11] Benfeld, J. (2020) Profesión legal y tecnologías de la información y las comunicaciones: Una discusión necesaria. *Revista Chilena de Derecho y Tecnología*, 9 (2), pp. 5 – 31.
- [12] Bubeck, S. et al. (2023) Sparks of Artificial General Intelligence: Early Experiments with GPT-4. [pre-print] Submitted to: *arXiv*, Available from: <https://doi.org/10.48550/arXiv.2303.12712> [Accessed 15 December 2024].
- [13] Bunge, M. (2008) *Filosofía y sociedad*. Mexico City: Siglo XXI.
- [14] Choi, J. H., et al. (2024) Lawyering in the Age of Artificial Intelligence. *Minnesota Law Review*, 109, Minnesota Legal Studies Research Paper No. 23-31, Available from: <https://ssrn.com/abstract=4626276>

- [15] Cochran Jr, R. F., et al. (2002). Symposium: Client Counseling and Moral Responsibility. *Pepperdine Law Review*, 30, 591
- [16] Coeckelbergh, M. (2022) *The Political Philosophy of AI: An Introduction*. Cambridge: Polity Press.
- [17] Cortina, A. (1998) Ética de las profesiones. *El País*, Opinion section.
- [18] Cruz Parceró, J. A. (2006) Los métodos para los juristas. In: C. Courtis (ed.), *Observar la ley: Ensayos sobre metodología de la investigación jurídica*, Madrid: Editorial Trotta, pp. 17 – 40.
- [19] Damasio, A. (2016). La zone du dedans, réflexions sur une société sans air. In: Benjamin Mayet (ed.) *Le dehors de toute chose*. Paris: La Volte, p. 72.
- [20] Dinerstein, R. et al. (2003). Dinerstein, R. et al. (2003). Connection, Capacity and Morality in Lawyer-Client Relationships: Dialogues and Commentary. *Clinical Law Review*, 10, 755
- [21] Dixon, T. (2008) *Science and Religion: A Very Short Introduction*. USA: Oxford University Press,
- [22] Dreyfus, H. L. (1992). *What computers still can't do: A critique of artificial reason*. MIT press.
- [23] Ellul, J. (1964) *The Technological Society*. (J. Wilkinson, Trans.) New York: Alfred A. Knopf.
- [24] Fang, H. et al. (2015) From Captions to Visual Concepts and Back. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 1473 – 1482.
- [25] Freud, S. (2001) *Obras completas*. (L. López-Ballesteros y de Torres, Trans.). Mexico: Titivillus.
- [26] Garapon, A. and Lassègue, J. (2018) *Justice Digitale: Révolution Graphique et Rupture Anthropologique*. Paris: Presses Universitaires de France.
- [27] González, D. (2012) The Third Humiliation? (On Neuroscience, Philosophy and Free Will), *Doxa. Cuadernos de Filosofía del Derecho*. Available from: <https://doi.org/10.14198/DOXA2012.35.21> [Accessed 15 December 2024], pp. 499–510.
- [28] Gudmunsen, Z. (2024) The Moral Decision Machine: A Challenge for Artificial Moral Agency Based on Moral Deference. In: Brozek, B. and Janik, B. *Can Artificial Intelligences Be Moral Agents?*, pp. 101 – 106.
- [29] Guibourg, R. (2018) *Tecnología, sociedad y derecho*. Buenos Aires: La Ley.
- [30] Harasta, J., Novotná, T. & Savelka, J. (2024) It cannot be right if it was written by AI: on lawyers' preferences of documents perceived as authored by an LLM vs a human. *Artificial Intelligence and Law*. Available from: <https://doi.org/10.1007/s10506-024-09422-w>

- [31] Harnad, S. (1990) The symbol grounding problem. *Physica D: Nonlinear Phenomena*, 42(1-3), pp. 335 – 346.
- [32] Hart, H. L. A. (1961) *The concept of law*. Oxford: Oxford University Press.
- [33] Hicks, M.T., Humphries, J., and Slater, J. (2024) ChatGPT is Bullshit. *Ethics and Information Technology*, 26(38). Available from: <https://doi.org/10.1007/s10676-024-09775-5> [Accessed 15 December 2024], pp. 1 – 14.
- [34] Hoffman, D. D. (2019) *The Case Against Reality: Why Evolution Hid the Truth from Our Eyes*. [Kindle e-book] New York: W.W. Norton & Company.
- [35] International Bar Association. (2011) *International Principles on Conduct for the Legal Profession*
- [36] Kant, I. (1788) Critique of Practical Reason. Place of publication unknown: Publisher unknown.
- [37] Kant, I. (1912) *Prolegomena to Any Future Metaphysics*. (P. Carus, Trans.). [online] Chicago: The Open Court Publishing Company. Available from: <https://www.gutenberg.org/files/52821/52821-h/52821-h.htm> [Accessed 18 November 2023], (Original work published 1783).
- [38] Kant, I. (1996) *Critique of Pure Reason*. (W. S. Pluhar, Trans.). 1st ed. Indianapolis: Hackett Publishing Company, (Original work published 1781).
- [39] Katz, D. M. et al. (2024) GPT-4 Passes the Bar Exam. *Philosophical Transactions of the Royal Society A*, 382(2270), 20230254.
- [40] Kennedy, D. (1982) Legal education and the reproduction of hierarchy. *Journal of Legal Education*, 32, 591.
- [41] Kirchner, J. H. et al. (2023) *New AI Classifier for Indicating AI-Written Text* [blog entry], 31 January. Available from: <https://openai.com/blog/new-ai-classifier-for-indicating-ai-written-text> [Accessed 15 December 2024].
- [42] Klein, E. (2011) Comment dire ce dont parle la physique? *Champ Lacanien*, 10 (2). Available from: <https://doi.org/10.3917/chla.010.0181> [Accessed 15 December 2024], pp. 181 – 194.
- [43] Kronman, A. T. (1993) *The lost lawyer: Failing ideals of the legal profession*. Harvard University Press
- [44] Latour, B. (2005) *Reassembling the social: An introduction to actor-network-theory*. Oxford university press.
- [45] Le Precepteur (2023) *KANT - Les Limites De Notre Connaissance*. [online video] Available from: https://www.youtube.com/watch?v=5Hsm_6GrqhA [Accessed 15 December 2024].
- [46] Lee, M., et al. (2025) Could AI Make Legalese Comprehensible to the Public? SSRN. Available from: <https://ssrn.com/abstract=5220337>

- [47] McCormick, N. (1994) *Legal reasoning and legal theory*. Clarendon Press
- [48] Macey-Dare, R. (2023). ChatGPT & Generative AI Systems as Quasi-Expert Legal Advice Lawyers - Case Study Considering Potential Appeal Against Conviction of Tom Hayes. SSRN. Available from : <https://doi.org/10.2139/ssrn.4342686>
- [49] MacIntyre, A. (1984) *After virtue: A study in moral theory* (2nd ed.). Notre Dame, Indiana: University of Notre Dame Press.
- [50] Magesh, V. et al. (2024) Hallucination-Free? Assessing the Reliability of Leading AI Legal Research Tools. *arXiv*. Available from: <https://arxiv.org/abs/2405.20362> [Accessed 17 July 2024].
- [51] Marcuse, H. (1941) Some social implications of modern technology. *Studies in philosophy and social science*, 9(3), 414 – 439.
- [52] McStay, A. (2018) *Emotional AI: The Rise of Empathic Media*. London: Sage Publications.
- [53] Meinke, A. et al. (2024) Frontier Models are Capable of In-context Scheming. [pre-print] Submitted to: *arXiv*. Available from: <http://arxiv.org/abs/2412.04984> [Accessed 15 December 2024].
- [54] Menkel-Meadow, C. (2001). Aha? is creativity possible in problem solving and teachable in legal education. *Harvard Negotiation Law Review*, 6, 97.
- [55] Menkel-Meadow, C. J. (1999). When winning isn't everything: The lawyer as problem solver. *Hofstra Law Review*, 28, 905
- [56] Morawetz, T. (2013). Empathy and Judgment. *Yale Journal of Law & the Humanities*.
- [57] Morin, E. (1977). *La nature de la nature* (Vol. 1). Paris: Seuil.
- [58] Murdoch, I. (2013) *The Sovereignty of Good*. Contributed by Mary Midgley. 1st ed. London: Routledge. Available from: <https://doi.org/10.4324/9781315887524>.
- [59] Noble, S. U. (2018) *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York: New York University Press.
- [60] Nussbaum, M. C. (1995). Poets as judges: Judicial rhetoric and the literary imagination. *The University of Chicago Law Review*, 62(4), 1477 – 1519
- [61] Perelman, C. (1964) *De la justicia*, Mexico City: UNAM
- [62] Poincaré, H. (1890) Sur le problème des trois corps et les équations de la dynamique, *Acta Mathematica*, 13 (1-2), pp. 1 – 270.
- [63] Prince Tritto, P. (2021) La clasificación del lenguaje jurídico: barrera de entrada de la inteligencia artificial en el campo del derecho. In: Pérez, R. D., Trincado, E., and Gallego, E. (eds.) *Economía, empresa y justicia: nuevos retos para el futuro*. Madrid: Dykinson, pp. 411 – 429.

- [64] Radford, A. et al. (2023) Robust Speech Recognition via Large-Scale Weak Supervision. *Proceedings of Machine Learning Research*, 202. Available from: <https://proceedings.mlr.press/v202/radford23a.html> [Accessed 15 December 2024], pp. 28492–28518.
- [65] Rhode, D. L. (2012). Access to justice: an agenda for legal education and research. *Journal of Legal Education*, 62, 531.
- [66] Rudko, I. & Bashirpour Bonab, A. (2025) ChatGPT is incredible (at being average). *Ethics and Information Technology* 27, 36. Available from: <https://doi.org/10.1007/s10676-025-09845-2>
- [67] Rumelhart, D. E. and Norman, D. A. (1976) *Accretion, Tuning and Restructuring: Three Modes of Learning*. Report No. 7602. La Jolla: University of California, San Diego, Center for Human Information Processing.
- [68] Schwarcz, D. et al. (2025) Thinking Like A Lawyer In The Age Of Generative AI: Cognitive Limits On AI Adoption Among Lawyers. *Minnesota Legal Studies*. Research Paper No. 25-31, Available from: <http://dx.doi.org/10.2139/ssrn.5260645>
- [69] Searle, J. R. (1980). Minds, brains, and programs. *Behavioral and brain sciences*, 3(3), 417-424.
- [70] Shaffer, T. L. (1979). Practice of Law as Moral Discourse. *Notre Dame Law Review*, 55, 231
- [71] Shapiro, S. J. (2006). What is the internal point of view. *Fordham Law Review*, 75, 1157
- [72] Shen, Y. et al. (2023) HuggingGPT: Solving AI Tasks with ChatGPT and its Friends in Hugging Face. *arXiv*, 2303.17580, Available from: <https://arxiv.org/pdf/2303.17580> [Accessed 15 December 2024].
- [73] Simon, W. H. (2009). *The practice of justice: a theory of lawyers' ethics*. Harvard University Press.
- [74] Surden, H. (2024) ChatGPT, Artificial Intelligence (AI) Large Language Models, and Law. *Fordham Law Review*, 92. Available from: <https://ssrn.com/abstract=4779694> [Accessed 15 December 2024], pp. 1951 – 1965.
- [75] Taylor, A. (2009). *Animals and ethics*. Broadview press.
- [76] Torres, A. (2013) La experiencia en la estética trascendental de Kant. *Cuestiones de Filosofía*, (15). Available from: <https://doi.org/10.19053/01235095.2104> [Accessed 18 November 2023], pp. 65 – 88.
- [77] Valéry, P. (1942) *Mauvaises Pensées et autres*. [online] Paris: Gallimard. Available from: <https://ebooks-bnr.com/valery-paul-mauvaises-pensees-autres/> [Accessed 15 December 2024].

- [78] Venkit, P. N. et al. (2024) Confidently Nonsensical? A Critical Survey on the Perspectives and Challenges of ‘Hallucinations’ in NLP. *arXiv*, Available from: <https://arxiv.org/abs/2404.07461v1>.
- [79] Weber, M. (2021) *La ética protestante y el espíritu del capitalismo*. [e-book] (2nd ed.) México: Fondo de Cultura Económica. Available from: <http://digital.casalini.it/9786071648853> [Accessed on 15 december 2024], pp. 115-116.
- [80] Xu, N. et al. (2022). Technology Acceptance Model for Lawyer Robots with AI: A Quantitative Survey. *International Journal of Social Robotics*, 14. Available from: <https://doi.org/10.1007/s12369-021-00850-1>, pp. 1043 – 1055.

DOI 10.5817/MUJLT2025-2-5

ON THE POSSIBLE USE OF DATABASES TO SECURE RECEIVABLE DEBTS *

by

MACIEJ BUJALSKI †

*The article assesses the possibilities of using databases to secure receivable debts, i.e. as collateral, more than ten years after the ruling in the case *Your Response v. Datateam Business Media* where this possibility was denied. In order to do so, it first examines why someone may wish to use a database for this purpose and what the features are, including the limited accessibility of the database and its contents, that make a database an asset that may be useful in that context. The article then addresses the scope of the sui generis database right and its limited utility from the perspective of security rights, taking into consideration the entry into force of the Data Act. It analyses databases at three different levels: semantical, syntactical and structural, exploring at which level the features resulting in the value of the database should be placed, and thus the level at which the question of establishing a security interest over a database should be dealt with. The article goes on to provide for some theoretical approaches of introducing the rules on securities over databases into the legal system. It analyses the perspective of introducing proprietary rights to the database, the possible qualification of the database as a digital asset and the question of its control, as well as the contractual schemes that may be used in order to establish and enforce the security interest over a database.*

* This paper is an element of the research carried out under the project 'Virtually secured credit? Security rights in digital goods' financed by Narodowe Centrum Nauki (NCN) [National Science Centre] in Krakow, Poland – number 2022/45/B/HS5/02952. It was presented in its initial shape at the Cyberspace conference held by Masaryk University in Brno on 29-30 November 2024. The author would like to acknowledge all the valuable comments he has received.

† Research Assistant in the Department of Comparative Private Law and PhD Candidate in the Doctoral School in the Social Sciences at the Jagiellonian University in Kraków, Poland. The author is supported by the Foundation for Polish Science (FNP), START 2025. E-mail: maciej.bujalski@uj.edu.pl; ORCID: 0000-0003-4004-8319

KEY WORDS

Database, Collateral, Security Rights, Digital Assets, Proprietary Rights to Data

1. INTRODUCTION

Although this article could possibly be regarded as another article on “data as the new oil”, given its focus on the use of data – structured in the form of a digital database – and its market value and tradability, it approaches this issue from an angle that has not yet come under much scrutiny.¹ The paper addresses the use of databases to secure receivable debt.

The paper thus examines the possibility of establishing security interests over databases. Security interest – also referred to as “security” or “security right” – is understood as a way of granting a creditor an exclusive and preferential possibility to satisfy their claim against their debtor from the given object (the collateral), which is based on *in rem* rights to this object (broadly speaking, including not only instruments like pledges, but also the transfer of property made in order to secure the debt), which makes the security interest effective against third parties, including other creditors of the debtor.² The answer to the question of what can be used as collateral, i.e. as an object of security interest, varies across different jurisdictions. This paper will not delve into the specifics of these jurisdictions unless they serve as illustrative examples. Instead, it will focus on the conceptual possibility of using databases as collateral. It does not deal with the admissibility of such usage; rather, it outlines potential scenarios in which a database could serve as collateral, as well as risks that any prospective regulation should address. Thus, it is more of a law policy paper. However, there are some general preliminary concerns, noticeable through a brief comparative analysis, that need to be answered before a thorough examination of the security rights over databases can take place.

Yet, before launching a proper analysis on the use of databases as collateral, it is worth establishing why someone would want to use a database as collateral. The value comes from the specific features that may be associated with the database, and which result in its market value and make it useful as an object of security interest. Firstly, the stored information itself – the data – may present some value. Obtaining information costs money,

¹ The question was tackled over twenty years ago by Lipton, J.D. (2001) Security Interests in Electronic Databases. *International Journal of Law and Information Technology*, 9 (1), however, with the focus on IP rights and English law.

² Drobnig, U. (2012) Security Rights in Movable Assets. In: Jürgen Basedow, Klaus J. Hopt, Reinhard Zimmermann (eds.) *Max Planck Encyclopedia of European Private Law*. Oxford: Max-Planck-Gesellschaft, pt. 1. Available from: https://max-eup2012.mpipriv.de/index.php/Security_Rights_in_Movable_Assets [Accessed 28 December 2024].

and in this case one entity has already obtained it, so another does not need to. The information could be used for development purposes, or could be analysed in order to provide further data and information.³ Secondly, the value may be linked to the fact that the data were already structured. Even if some information may be easily accessible, the fact that it is stored in some manner may be the source of added value. Thirdly, the value may result from the exclusive nature of the data stored in the database, or at least its limited accessibility.⁴ The fact that only some entities may profit from the database in their business activity affects their competitiveness and makes databases an important asset. However, this feature challenges the use of a database as collateral, as its use in this way cannot result in making it available to the public, and there is a need for some guarantees that both parties will preserve this confidential-like nature of the database: the secured creditor for the duration of the security and the debtor right after enforcement. Those features need to be reflected in the legal means that allow databases to be used as collateral.

Those remarks are general ones as the databases in practice form a very heterogeneous group. For particular databases, the value and economic rationale of using them as collateral may be linked to specific features and uses of the database within the business activity of its holders. Some databases can bring benefits because access to them is subject to payable licences. Others contain some information that is difficult to collect, so their value reflects the costs that would have to be borne in order to form a parallel database (even though the data are available to the public, such as geological features). In other cases, the content of the database could be a large number of works protected by intellectual property rights, in which case the database reflects their value, which may well be higher than the sum of individual and non-structured copyrights. Such features may influence the individual decision of using a given database as collateral, or of specific arrangements relating to enforcement, which may sometimes require the transfer of intellectual property rights to the database contents, or consist of granting the creditor the benefits that the database produces. However, as tangible entities, all those databases are generally similar, in that they exist because of the code that provides their structure, as they can be accessed

³ Nekt, K. (2024) The (Im)Possibility of Personal and Industrial (Machine-generated) Data to Be Subject to Property Rights. *International Journal of Law and Information Technology*, 32 (2), p. 9.

⁴ See Aplin, T. (2017) Trading Data in the Digital Economy: Trade Secrets Perspective. In: Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer (eds.) *Trading Data in the Digital Economy: Legal Concepts and Tools*. Baden-Baden: Nomos-Hart, p. 66.

and such access is generally limited for third parties,⁵ and as they present the market value outlined above. That is why, even if not all databases could be used as collateral in practice, or if some present specific features that should be reflected in particular rules concerning such security interests (which is actually true for tangible objects as well), it is possible to distinguish databases as an object presenting certain common features making it possible to conceptualise the possibility of using them as security features.

Up to this moment, the term “database” could have been understood in the common and intuitive meaning. However, to answer the research question, the term “database” must be explained to establish the exact object that will be used as collateral. Therefore, the term “database” is generally used in this paper in a legally neutral and rather functional meaning. A suitably simple definition that may serve the further analysis can be found in the judgment of the Court of Appeal of England and Wales from 14 March 2014, rendered in the case *Your Response v. Datateam Business Media*, in which the court dealt with the possibility of using a digital database as collateral.⁶ According to this definition, “the database consists of many individual pieces of information stored in a structured manner which renders them capable of systematic search and retrieval.”⁷ Hence, the database is a structured set of data that is capable of being analysed and which may present some market value because of its contents, structure and limited accessibility. As digital databases are the most commonly used, and as – given their size – they present significant economic value, they are the main interest of this paper. However, the considerations may also be related to traditional databases stored in certain tangible objects, such as ledgers.

The understanding of the term “database” is therefore similar to the definition resulting from Article 1(2) of Directive 96/9/EC on the legal protection of databases (Database Directive)⁸ according to which a database is, for the purposes of this directive, a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means. However, the paper refrains from this definition as it has a strictly defined scope, excluding,

⁵ Of course, a database may be publicly available. From an institutional point of view, it can still be used as security, though it does not represent the value for which someone would decide to use it that way.

⁶ *Your Response Ltd v. Datateam Business Media Ltd* (2014) Court of Appeal, 3 WLR, p. 887. This judgement is commented on in detail in the further section.

⁷ *Your Response Ltd v. Datateam Business Media Ltd* (2014). *op. cit.* p. 897, para. 28

⁸ Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases. *Official Journal of the European Union* (1996 L 77) 27 March. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31996L0009> [Accessed 28 December 2024].

e.g. computer programs used in the making or operation of a database.⁹ Meanwhile, for the purpose of analysing the possibilities of creating a security interest over a database, such limitations and distinctions are not needed as the structured set of data of certain value can be recorded in different forms, usually as a code, and those records are considered as possible collateral. Furthermore, this paper examines the security interests over a database as such and not over the *sui generis* database right under Article 7(1) of the Database Directive. Hence, relying on the definition of Article 1(2) of the Database Directive may be misleading since the term “database” would be read in the context of the *sui generis* database right. It is particularly important since this right has a limited scope of application making it of limited utility to be used as collateral. The reasons why the analysis should focus on the databases themselves serving as an object of security, and not the *sui generis* database right, are explained in the following section.

2. LEAVING THE *SUI GENERIS* DATABASE RIGHT ASIDE

The *sui generis* database right is an IP right entitling its holder to prevent third parties from extracting and re-using the contents of the database, and as such, like all IP rights, should be regarded as a proprietary right.¹⁰ Therefore, it can be used as collateral, which should be regarded in the general context of securities established over IP rights.¹¹ The security interest over the *sui generis* database right can be established, for example, through a mortgage, pledge on rights or the proprietary transfer of the *sui generis* right.¹² However, the

⁹ Recital 23 of the Database Directive.

¹⁰ Derclaye, E. (2008) *The Legal Protection of Databases. A Comparative Analysis*. Cheltenham–Northampton: Edward Elgar, pp. 51–52.

¹¹ See, in general, however without taking the *sui generis* database right into consideration, from the perspective of comparative law: Kieninger, E.-M. (2021) Security Rights in Intellectual Property. In: Katharina Boele-Woelki, Diego P. Fernández Arroyo, Alexandre Segenacnik (eds.) *General Reports of the XXth General Congress of the International Academy of Comparative Law*. Cham: Springer; and from the economic perspective: Heller, D., Leitzinger, L. and Walz U. (2024) Intellectual Property as Business Loan Collateral: A Taxonomy of Institutional and Economic Determinants. *GRUR International – Journal of European and International IP Law*, 73 (5). See also UNCITRAL (2011) *UNCITRAL Legislative Guide on Secured Transactions. Supplement on Security Rights in Intellectual Property*. Rome. Available from: https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/10-57126_ebook_suppl_sr_ip.pdf [Accessed 28 June 2025].

¹² Lipton, J.D. (2001) Security Interests in Electronic Databases. *International Journal of Law and Information Technology*, 9 (1), pp. 72, 75–81; Séjean, M. and Binctin, N. (2019) Sûretés Réelles Mobilières sur la Propriété Intellectuelle. *Revue Internationale de Droit Comparé*, 71 (2), pp. 447–450; Ferling, M. (2023) *Digitale Information als Kreditsicherheit*. Tübingen: Mohr Siebeck, pp. 121, 152–153. See also, for other IP rights, Kieninger, E.-M. (2021) Security Rights in Intellectual Property. *op. cit.* pp. 353–358; Heller, D., Leitzinger, L. and Walz U. (2024) Intellectual Property as Business Loan Collateral: A Taxonomy of Institutional and Economic Determinants. *op. cit.* pp. 385–387.

idea behind protection with the *sui generis* database right under the Database Directive is not actually to protect the database as such, but to protect the investment made in order to create the database.¹³ Thus, it is still an artificial construct of the *sui generis* right being an object of the security, and not the database itself, while what has the potential, analysed in this paper, is the actual database, being an electronic record containing a possibly valuable structured set of data. Consequently, it is the *sui generis* right that is subject to enforcement.¹⁴ As a result, the secured creditor has no guarantee of the protection and confidentiality of the database contents. Even though the holder of the *sui generis* database right should generally have access to the database, it is possible that the creditor will be deprived of the real value of the database, whether through the denial of access to the database through technical barriers or because of the multiplication of the database contents and making them available to the public. Hence, the first reason why the analysis should not focus on the *sui generis* database right is the fact that it only reflects the actual database and aims at protecting the substantial investment made and not the contents of the database in which the real value lies. The second reason is the limited scope, both territorial and substantial, of application of protection under the Database Directive, which does not cover a vast number of databases presenting some significant value for which the *sui generis* database right cannot be used in order to constitute security.

It must be noted that the *sui generis* database right has limited territorial scope of application. It does not have its origin in international conventions, but it was the European Union's idea to promote innovation within Europe and to establish competitiveness with other regions.¹⁵ As a result, Article 11 of the Database Directive allows the *sui generis* database right to be awarded only to those entities that are nationals of a Member State, have their habitual residence in the European Union or whose business activity presents a sufficient link with the territory of the European Union.¹⁶ Even though the Database Directive allows the protection of databases whose makers are from third countries, under the condition of reciprocity,¹⁷ similar intellectual

¹³ Recital 40 of the Database Directive. See also Zech, H. (2016) Data as a Tradeable Commodity. In: Alberto De Franceschi (ed.) *European Contract Law and the Digital Single Market*. Cambridge–Antwerp–Portland: Intersentia, p. 70.

¹⁴ Ferling, M. (2023) *Digitale Information als Kreditsicherheit*. Tübingen: Mohr Siebeck, p. 280.

¹⁵ Recitals 11–12 of the Database Directive; Derclaye, E. (2008) *The Legal Protection of Databases. A Comparative Analysis*. Cheltenham–Northampton: Edward Elgar, pp. 45–46; Alejandre, G.M. (2021) Ownership of Databases: Personal Data Protection and Intellectual Property Rights on Databases. *European Review of Private Law*, 29 (5), p. 738.

¹⁶ See Derclaye, E. (2008) *The Legal Protection of Databases. A Comparative Analysis*. Cheltenham–Northampton: Edward Elgar, p. 49.

¹⁷ Recital 56 of the Database Directive. See also Leistner, M. (2017) Big Data and the EU Database Directive 96/9/EC: Current Law and Potential for Reform. In: Sebastian Lohsse, Reiner

property rights to the *sui generis* database right are not harmonised globally and are rarely adopted in other jurisdictions.¹⁸ The lack of reciprocal rights in some jurisdictions would make it impossible to enforce such a security. There is no point in establishing a security interest that would not enhance the creditor's position, as it could not be enforced. Furthermore, even though there are jurisdictions recognising a similar right, the use of the *sui generis* database right as collateral seems inefficient in international commerce, as it lacks the predictability sought by businesses.¹⁹

Furthermore, the *sui generis* database right does not cover many databases because of substantial reasons. It is mainly the question of the so-called "spin-off" theory due to which the datasets that are byproducts of the commercial activity, and not its purpose, cannot be protected with the *sui generis* database right.²⁰ The matter was further developed by the jurisprudence of the Court of Justice of the European Union, according to which the substantial investment in the creation of data is not sufficient to establish a *sui generis* database right, as the Database Directive sets as a condition for protecting the investment made in order to obtain already existing data.²¹ Nowadays, the biggest concerns are databases containing machine-generated data, obtained by the producers of devices for everyday use – especially in the reality of the Internet of Things – through the sensors installed in these devices. Such data provides information not only on the user of the device, but also on many other external features and processes and hence has important market value for different kinds of entities. For example, in the automotive sector, the data obtained through car devices provides information not only about the driver's preferences, which may be

Schulze, Dirk Staudenmayer (eds.) *Trading Data in the Digital Economy: Legal Concepts and Tools*. Baden-Baden: Nomos-Hart, p. 50.

¹⁸ Alejandre, G.M. (2021) Ownership of Databases: Personal Data Protection and Intellectual Property Rights on Databases. *European Review of Private Law*, 29 (5), p. 739. However, similar rights were observed e.g. in Mexico, Russia or South Korea, see World Intellectual Property Organization (2002) *Summary on Existing Legislation Concerning Intellectual Property in Non-Original Databases*. SCCR/8/3. Geneva, p. 9. Available from: https://www.wipo.int/edocs/mdocs/copyright/en/sccr_8/sccr_8_3.pdf [Accessed 24 June 2025]; Doldirina, C. et al. (2016) Legal Approaches for Open Access to Research Data. *Law Archive Papers*, p. 20. Available from: https://osf.io/preprints/lawarchive/n7gfa_v1 [Accessed 24 June 2024].

¹⁹ The risk was also observed by Lipton, J.D. (2001) Security Interests in Electronic Databases. *International Journal of Law and Information Technology*, 9 (1), pp. 84–85.

²⁰ Derclaye, E. (2004) Databases Sui Generis Right: Should We Adopt the Spin Off Theory? *European Intellectual Property Review*, 26 (9), p. 402.

²¹ Judgment of 9 November 2004, British Horseracing, C-203/02, EU:C:2004:695, paras. 30–41; Judgment of 9 November 2004, Fixtures Marketing, C-338/02, EU:C:2004:696, paras. 24–37; Judgment of 9 November 2004, Fixtures Marketing, C-46/02, EU:C:2004:694, paras. 34–49; Judgment of 9 November 2004, Fixtures Marketing, C-444/02, EU:C:2004:697, paras. 40–53.

valuable for insurers, but also about traffic in general.²² However, relying on the aforementioned jurisprudence and the “spin-off” theory, the scholarship, generally, opted for excluding such databases from the *sui generis* database rights’ scope, under Article 7(1) of the Database Directive.²³ Since, in the case of databases containing machine-generated data, the producer makes a significant investment to produce a device that will allow the collection of data, the database itself is often a byproduct of the principal business activity. Seeing this tension, some authors argued for the shift in the interpretation or for the update of the Database Directive in order to grant such databases protection through the *sui generis* database right.²⁴ However, the European lawmaker took a different path and somehow cut off these debates.

The discussed datasets are mostly covered by Article 43 of the Data Act,²⁵ according to which the *sui generis* right provided for in Article 7 of the Database Directive shall not apply when data is obtained from or generated by a connected product or related service falling within the scope of the Data

²² Hugenholtz, P.B. (2017) Data Property in the System of Intellectual Property Law: Welcome Guest or Misfit? In: Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer (eds.) *Trading Data in the Digital Economy: Legal Concepts and Tools*. Baden-Baden: Nomos-Hart, p. 76.

²³ Zech, H. (2015) „Industrie 4.0“ – Rechtsrahmen für eine Datenwirtschaft im digitalen Binnenmarkt. *Gewerblicher Rechtsschutz und Urheberrecht*, (12), pp. 1157–1158; Drexl, J. (2017) Designing Competitive Markets for Industrial Data – Between Propertisation and Access. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 8 (4), p. 268; Duch-Brown, N., Martens, B. and Mueller-Langer, F. (2017) *The Economics of Ownership, Access and Trade in Digital Data*. JRC Digital Economy Working Paper No. 2017-01. Seville: European Commission, pp. 13–14; European Commission (2017) *Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy*. SWD(2017) 2 final. Brussels: European Commission, p. 20. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017SC0002> [Accessed 30 December 2024]; Nekit, K. (2024) The (Im)Possibility of Personal and Industrial (Machine-generated) Data to Be Subject to Property Rights. *International Journal of Law and Information Technology*, 32 (2), p. 14.

²⁴ See Leistner, M. (2017) Big Data and the EU Database Directive 96/9/EC: Current Law and Potential for Reform. In: Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer (eds.) *Trading Data in the Digital Economy: Legal Concepts and Tools*. Baden-Baden: Nomos-Hart, pp. 27–30; Alejandre, G.M. (2021) Ownership of Databases: Personal Data Protection and Intellectual Property Rights on Databases. *European Review of Private Law*, 29 (5), pp. 743–744; European Commission (2022) *Study to Support an Impact Assessment for the Review of the Database Directive*. Final Report. Luxembourg: Publications Office of the European Union, pp. 52, 76–77. Available from: <https://digital-strategy.ec.europa.eu/en/library/impact-assessment-report-and-support-studies-accompanying-proposal-data-act> [Accessed 30 December 2024]. Extensive interpretation was accepted in *Autobahnmaut* (2010) BGH, 25 March. (3) 2011 MMR, p. 188.

²⁵ Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act). *Official Journal of the European Union* (L 2023/2854) 22 December. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R2854&qid=1735552065097> [Accessed 30 December 2024].

Act. The provision – especially in the wording of the proposal²⁶ – raised doubts as to whether it is just an explanatory rule or the actual exclusion of the *sui generis* protection.²⁷ The purpose of this provision is to eliminate the risk that holders of data stored in databases would claim the *sui generis* right under Article 7 of the Database Directive and hinder the effective exercise of the right of users to access and use data, and the right to share data with third parties under the Data Act.²⁸ Thus, Article 43 of the Data Act should be regarded as providing for the general exclusion of the *sui generis* protection within the scope of the Data Act, which will grant at least some legal certainty.²⁹ It does not eliminate all the controversies, like the question on how to treat the databases containing two types of data, one protected by the *sui generis* database right, while the second are covered by the exclusion resulting from Article 43 of the Data Act.³⁰ However, the state of the art is that there are many databases of significant value – which was observed by the European lawmaker – that are not granted protection under the *sui generis* database right, but which the entity disposing of such a database may like to use it as collateral, for example in order to obtain funding for further development. Even though the holder of a database that is not covered by the Database Directive may benefit from other means of protection, e.g. contractual ones,³¹ these limitations of the intellectual property rights to databases call for an alternative object of research.

²⁶ European Commission (2022) *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. Brussels. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0068> [Accessed 30 December 2024].

²⁷ See Drexl, J. et al. (2022) *Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act)*. Max Planck Institute for Innovation and Competition Research Paper No. 22-05, pp. 91–96. Available from: https://pure.mpg.de/rest/items/item_3388757_4/component/file_3395639/content [Accessed 30 December 2024]; Wiebe, A. (2023) The Data Act Proposal. Access rights at the Intersection with Database Rights and Trade Secret Protection. *Gewerblicher Rechtsschutz und Urheberrecht*, (4), p. 230; Richter, H. (2024) Article 43 of the Data Act. In: Heinrich Amadeus Wolff, Stefan Brink, Antje v. Ungern-Sternberg (eds.) *BeckOK Datenschutzrecht*. 50th ed. München: C.H. Beck, pt. 19–22; Kim, D. (2024) Der Datenbankschutz sui generis nach dem Data Act. Having the cake and eating it too? *Zeitschrift für das Recht der Digitalisierung, Datenwirtschaft und IT*, MMR Appendix, pp. 88–89.

²⁸ Recital 112 of the Data Act.

²⁹ Richter, H. (2024) Article 43 of the Data Act. *op. cit.* p. 20. Whether the exclusion and not e.g. a specific fair use exception or free licensing scheme was the right approach to reach this aim is a separate question.

³⁰ *Op. cit.*, pt. 26–29; Wiebe, A. (2023) The Data Act Proposal. Access rights at the Intersection with Database Rights and Trade Secret Protection. *Gewerblicher Rechtsschutz und Urheberrecht*, (4), p. 230.

³¹ See Myška, M. and Harašta J. (2016) Less Is More? Protecting Databases in the EU after Ryanair. *Masaryk University Journal of Law and Technology*, 10 (2), pp. 182–183, with the reference to the Judgement of 15 January 2015, Ryanair, C-30/14, EU:C:2015:10, para. 45.

Because of the limited scope of application of the *sui generis* database right, the focus on securities that may be established through this construct would lead to unjustified – from the market participants’ and economic perspective – differentiation between various categories of databases that are economically suitable to be used as collateral. This perspective will not meet the possibilities that lie in this use of databases and so may be misleading.

All those arguments lead to the conclusion that the *sui generis* database right is of limited utility for the market players who would like to use a database as collateral. They wish to establish security over the database because of its structured content with the crucial role of access to it. Hence, there is a need to look for solutions that allow the establishment of a security interest over a database, understood as an electronic record, which is somehow a “tangible object” (though not in a legal sense). The following section assesses whether such solutions can be found in European legal orders. Then, the ways of establishing security over databases will be conceptualised at the theoretical level. However, it should be noted that the *sui generis* database right may play a supplementary role by granting measures of legal protection that may be associated with the models of establishing security interest over a database developed in the further sections.

3. COMPARATIVE LEGAL BACKGROUND

The comparative overlook of the possible use of databases as collaterals should begin with English law, where the question was directly dealt with more than ten years ago. It was the aforementioned ruling of the Court of Appeal of England and Wales in the case *Your Response v. Datateam Business Media*, in which the court denied the possibility of using a digital database as collateral.³² The case was as follows: Datateam Business Media performed a contract to manage a digital database for the company called Your Response. When the latter did not pay the agreed fees, Datateam Business Media refused to release the database, and the information stored there was withheld until the full settlement was made. The court, therefore, had to examine whether a creditor with access to the debtor’s database could withhold the database until the debt was paid – i.e. whether a creditor can exercise the “possessory lien” recognised under English law. This instrument is essentially equivalent to the civil law “right of retention” being a security, e.g. under French law.³³ Hence, the current state of the art under English law excludes qualifying databases as possible collaterals.

³² *Your Response Ltd v. Datateam Business Media Ltd* (2014). *op. cit.* p. 887.

³³ Bourassin, M. (2024) *Droit des sûretés*. 8th ed. Paris: Lefebvre Dalloz, p. 575.

Therefore, two considerations of the court, when justifying its ruling, are worth re-examining as they illustrate the legal dilemmas that have to be addressed while proposing the framework for using databases as collaterals.

First, the court refused to accept that one can exercise possession over a digital database, being an intangible object, as possession is necessarily linked to physical control over an object and is an essential condition for a possessory lien.³⁴ However, the court also admitted that a digital database may be subject to control, even exclusive control, which is a broader concept than possession. Those issues are important, on the one hand, because possession is a condition for the effectiveness of many securities in various jurisdictions.³⁵ Therefore, if such a condition exists, it would be impossible to establish a security interest over a database. On the other hand, the strict position of the Court of Appeal of England and Wales may be considered as not adjusted to the digital reality surrounding us,³⁶ thus, maybe, possession should be succeeded by a more functional concept. Hence, in the model rules concerning the security rights in digital assets, the concept of control is used to replace “possession” in relation to those goods for which physical possession is hardly imaginable and would be somehow artificial.³⁷

However, there are also alternative ways of establishing securities that are effective against third parties, particularly related to inscriptions in public registers.³⁸ French law may serve as an example. It provides for the establishment of security interests effective against third parties in two ways: through a transfer of possession or through an inscription in the register of movable securities.³⁹ Yet, it links the right to retention only with the

³⁴ Your Response Ltd v. Datateam Business Media Ltd (2014). *op. cit.* p. 895, para. 23.

³⁵ Kieninger, E.-M. (2004) Introduction: Security Rights in Movable Property within the Common Market and the Approach of the Study. In: Eva-Maria Kieninger (ed.) *Security Rights in Movable Property in European Private Law*. Cambridge: Cambridge University Press, pp. 11–14.

³⁶ van Erp, S. (2017) Ownership of Data: The Numerus Clausus of Legal Objects. *Brigham-Kanner Property Rights Conference Journal*, (6), pp. 245–246.

³⁷ See UNIDROIT (2023) *UNIDROIT Principles on Digital Assets and Private Law*. Rome, pp. 52–53. Available from: <https://www.unidroit.org/wp-content/uploads/2024/01/Principles-on-Digital-Assets-and-Private-Law-linked-1.pdf> [Accessed 28 December 2024]; European Law Institute (2022) *ELI Principles on the Use of Digital Assets as Security*. Vienna, pp. 20–21. Available from: https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Principles_on_the_Use_of_Digital_Assets_as_Security.pdf [Accessed 28 December 2024].

³⁸ Kieninger, E.-M. (2004) Introduction: Security Rights in Movable Property within the Common Market and the Approach of the Study. In: Eva-Maria Kieninger (ed.) *Security Rights in Movable Property in European Private Law*. Cambridge: Cambridge University Press, pp. 10–11.

³⁹ Bourassin, M. (2024) *Droit des sûretés*. *op. cit.* p. 640.

securities established through a transfer of possession.⁴⁰ Furthermore, it recognises security interests that may be established over digital assets being “incorporeal movables” (*biens meubles incorporels*, Article 2355 of the French Civil Code), which category also includes digital assets (Article L.54-10-1 of the French Monetary and Financial Code). However, the mere possibility of such qualification of databases seems contestable as the notion aims to cover mainly cryptoassets.⁴¹ So, establishing a security interest over a database is rather impossible under French law. However, even if accepted, the need to look for an alternative to the traditional concept of possession arises because of the need to ensure effective enforcement.⁴²

Second, in the *Your Response v. Datateam Business Media* ruling, the court stated in a general manner that, “*whilst the physical medium and the rights [intellectual property rights – M.B.] are treated as property, the information itself has never been.*”⁴³ The purpose of this paper is not to comprehensively deal with the question of proprietary rights to data, which has already been widely discussed in European legal scholarship⁴⁴ and somehow rejected

⁴⁰ Lisanti, C. and Pérechon, F. (2023) *Le Nantissement d’Actifs Incorporels. Revue des Procédures Collectives*, (3), p. 52.

⁴¹ Julienne, M. (2020) *Les Actifs Numériques, Entre Droit et Technologie. Bulletin Joly Bourse*, (1), pp. 64–65. Extensively see Mekki, M. (2024) *Actifs Numériques*. In: *Répertoire de Droit Commercial*. Paris: Dalloz, pt. 36–65.

⁴² Also Bujalski, M. (2025) Czy prawo francuskie może stanowić wzór dla regulacji realizacji zabezpieczeń na dobrach cyfrowych? *Forum Prawnicze*, 86 (2), pp. 82–83.

⁴³ *Your Response Ltd v. Datateam Business Media Ltd* (2014). *op. cit.*, p. 900, para. 42.

⁴⁴ See among many Wiebe, A. (2016) Protection of industrial data – a new property right for the digital economy? *GRUR International – Journal of European and International IP Law*, (10), pp. 880–884; Zech, H. (2016) A Legal Framework for a Data Economy in the European Digital Single Market: Rights to Use Data. *Journal of Intellectual Property Law & Practice*, 11 (6), pp. 468–470; Drexler, J. et al. (2016) *Data Ownership and Access to Data. Position Statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the Current European Debate*. Max Planck Institute for Innovation and Competition Research Paper No. 16-10, pp. 2–3. Available from: https://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/positionspaper-data-eng-2016_08_16-def.pdf [Accessed 31 December 2024]; Drexler, J. (2017) Designing Competitive Markets for Industrial Data – Between Propertisation and Access. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 8 (4), pp. 272–278; Hugenholtz, P.B. (2017) Data Property in the System of Intellectual Property Law: Welcome Guest or Misfit? In: Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer (eds.) *Trading Data in the Digital Economy: Legal Concepts and Tools*. Baden-Baden: Nomos–Hart, pp. 78–82; Zimmer, D. (2017) Property Rights Regarding Data? In: Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer (eds.) *Trading Data in the Digital Economy: Legal Concepts and Tools*. Baden-Baden: Nomos–Hart, pp. 101–107; Banterle, F. (2018) The Interface Between Data Protection and IP Law: The Case of Trade Secrets and the Database *Sui Generis* Right in Marketing Operations, and the Ownership of Raw Data in Big Data Analysis. In: Mor Bakhoun, Beatriz Conde Gallego, Mark-Oliver Mackenrodt, Gintarė Surblytė-Namavičienė (eds.) *Personal Data in Competition, Consumer Protection and Intellectual Property Law*. Berlin: Springer, pp. 436–439.

by the European lawmakers in the Data Act,⁴⁵ which is not, however, free of controversies.⁴⁶ English law is also developing new approaches to proprietary rights in digital assets.⁴⁷ This paper will, however, take a stand in this discussion from the perspective of security rights – understood as *in rem* rights – which may provide some new arguments in this debate. It can be well observed in the context of German law that knows the narrow concept of thing (*Sache*), limited to the physical objects (§ 90 of the German Civil Code) and, thus excludes establishing the security over an electronic record, like database, that cannot be handed over (§ 1205 of the German Civil Code) and is not linked to any proprietary right.⁴⁸

Therefore, a brief look into European jurisdictions proves that the regulations do not have much to offer to those wishing to establish a security over a database. However, the main issues that need to be addressed were properly identified over a decade ago in the *Your Response v. Datateam Business Media* ruling, and can serve as a starting point for further analysis. Yet, the search for solutions to fill these gaps should be preceded by explaining what should serve as an object of security in the proposed approaches to maintain clarity in legal analysis. For this purpose, three levels of database, being electronic records of structured datasets, should be outlined to establish the one with the value and features, making it important from the perspective of establishing a security interest. These are the semantic, syntactic, and structural levels, which will be explored in the following section.

⁴⁵ Graux, H. (2024) *What Is Data Ownership, and Does It Still Matter under EU Data Law?* Luxembourg: Publications Office of the European Union, p. 12. Available from: <https://data.europa.eu/sites/default/files/report/What%20is%20data%20ownership%2C%20and%20does%20it%20still%20matter%20under%20EU%20data%20law.pdf> [Accessed 30 December 2024]; Calzolaio, E. (2024) From data property to data access and back again? Comparative remarks on the EU Data Act. *Iceonline*, (1), pp. 43–47. Available from: <https://www.lceonline.eu/wp-content/uploads/2024/04/I.03-Calzolaio.pdf> [Accessed 4 July 2025]. See especially Recital 25 of the Data Act where it is stated that “This Regulation should not be understood to confer any new right on data holders to use product data or related service data.”

⁴⁶ Calzolaio, E. (2024) From data property to data access and back again? Comparative remarks on the EU Data Act. *Iceonline*, (1), pp. 47–48. Available from: <https://www.lceonline.eu/wp-content/uploads/2024/04/I.03-Calzolaio.pdf> [Accessed 4 July 2025], argues that it is possible to draw proprietary rights to data from the wording of the Data Act.

⁴⁷ See Calzolaio, E. (2023) Digital Assets and Property: Comparative Remarks from a Civil Law Perspective, *Comparative Law Review*, 14 (2), pp. 23–26.

⁴⁸ See Bülow P. (2019) Digitales Mobiliarpfandrecht. *Zeitschrift für Wirtschafts- und Bankrecht*, (25), pp. 1141–1145; Ferling, M. (2023) *Digitale Information als Kreditsicherheit*. Tübingen: Mohr Siebeck, pp. 129–130.

4. THREE LEVELS OF A DATABASE

While analysing information from the perspective of private law and proprietary rights, three levels are distinguished. These are the semantic level – information with a certain meaning, the content of the information; the syntactic level – the signs and their relation with each other (it is therefore recorded information, though not necessarily having meaning); and the structural level – information contained in a certain physical carrier or, in a wider sense, information represented by the structure of a physical object capable of being subject to proprietary rights.⁴⁹ The same categorisation may be adjusted to databases.

At the semantic level of a database, there is information that results from the data constituting the database (and not from the database itself!). As indicated, this information can present some value, as it may be subject to analysis and interpretation. However, this information generally exists without a form of a database and should be regarded as publicly available, even though obtaining it may require costs from the person wanting to have access to the information.⁵⁰ The fundamental freedom of the right to information should therefore be placed at the semantic level.⁵¹ This right cannot be restrained, so it is impossible to treat databases at the semantic level as an object to which certain rights are linked in the meaning of private law.⁵² In some cases, the semantic level of information (more often than

⁴⁹ Zech, H. (2015) Information as Property. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 6 (3), p. 194. This article summarizes the findings from Zech, H. (2012) *Information als Schutzgegenstand*. Tübingen: Mohr Siebeck. See also Wiebe, A. (2016) Protection of industrial data – a new property right for the digital economy? *op. cit.* p. 881, who distinguishes syntactic, semantic and pragmatic level and places data at the syntactic level.

⁵⁰ See also Catala, P. (1998) *Le Droit à l'Épreuve du Numérique*. Paris: Presses Universitaires de France, p. 244, who concludes that a person has the right to information that is available and allows them to create further information that may be subject to proprietary rights. The analysis was provided long before the division between the semantic and syntactic information was used in a legal context, but it may be regarded as being in common with these considerations as the “right to information” concerns the semantic level and the “information as a good” relates in some manner to the syntactic level.

⁵¹ See Hugenholtz, P.B. (2017) Data Property in the System of Intellectual Property Law: Welcome Guest or Misfit? In: Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer (eds.) *Trading Data in the Digital Economy: Legal Concepts and Tools*. Baden-Baden: Nomos-Hart, pp. 94–95, for whom the right to information may also concern the syntactic level.

⁵² Zech, H. (2012) *Information als Schutzgegenstand*. Tübingen: Mohr Siebeck, p. 443; Zech, H. (2015) Information as Property. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 6 (3), p. 196; Drexler, J. (2017) Designing Competitive Markets for Industrial Data – Between Propertisation and Access. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 8 (4), p. 277; European Commission (2017) *Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy*. SWD(2017) 2 final. Brussels: European Commission, p. 34. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:>

the semantic level of databases) can be protected as an invention or a trade secret.⁵³ However, the semantic level of database is not – and it should not be – the most appropriate level for the purpose of securing the receivable debts.

Data are stored at the syntactic level, which makes a database a database. For digital databases – which are the main interest of this paper – the syntactic level is the one at which the database actually exists.⁵⁴ At this level, the semantical information is reflected with a code that set the datasets within a structure.⁵⁵ That way, the database, being an electronic record, is recognisable in the market. Since it is sufficiently specified and has economic value separate from its carrier, it can be qualified as a digital asset.⁵⁶ The code could be designed in such a way that the datasets cannot be retrieved, analysed or researched. However, it is generally designed in the opposite way, so that the database holder can benefit from it. This structure – existing because of the code – represents the value of the database.⁵⁷ The information stored could be used commercially because it presents the features of a systematic arrangement that can be subject to various operations enabling actual decisions or activities, e.g. to target a product to a specific market or to interact with a given customer due to the association of their preferences and contact details. Furthermore, it is at this level that the question of accessibility of the database is dealt with. As a result, it is the syntactic level that allows the holder to benefit from the content of the database, i.e. from the semantic level – lead market participants to perceive a database as having market value and thus being suitable for commercial use, including the establishment of the security interest.

-
- 52017SC0002 [Accessed 30 December 2024]. The Court of Appeal in *Your Response Ltd v. Datateam Business Media Ltd* (2014). *op. cit.* p. 900, para. 42 referred to this level of information.
- ⁵³ Zech, H. (2015) Information as Property. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 6 (3), pp. 195–196; Drexler, J. (2017) Designing Competitive Markets for Industrial Data – Between Propertisation and Access. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 8 (4), p. 263. Critically on the distinction between the semantic and syntactic information in the context of trade secrets protection Aplin, T. (2017) Trading Data in the Digital Economy: Trade Secrets Perspective. In: Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer (eds.) *Trading Data in the Digital Economy: Legal Concepts and Tools*. Baden-Baden: Nomos-Hart, p. 68.
- ⁵⁴ Zech, H. (2012) Information als Schutzgegenstand. Tübingen: Mohr Siebeck, p. 253.
- ⁵⁵ Zech, H. (2015) Information as Property. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 6 (3), p. 194. See, however, Zech, H. (2012) *Information als Schutzgegenstand*. Tübingen: Mohr Siebeck, p. 361, where the author distinguishes structure of the database from the syntactic information as its content.
- ⁵⁶ See van Erp, S. (2017) Ownership of Data: The Numerus Clausus of Legal Objects. *Brigham-Kanner Property Rights Conference Journal*, (6), pp. 243–244, 251–252.
- ⁵⁷ Zech, H. (2012) *Information als Schutzgegenstand*. Tübingen: Mohr Siebeck, pp. 319–320.

The last to explore is the structural level. For non-digital databases, the structural level can take the form of a file or – more probably – lots of files, being tangible objects and thus subject to proprietary rights. The question is more subtle with regard to digital databases. Firstly, one could argue that the servers on which the data are stored could be assigned to the structural level. As they can be owned and the right of ownership grants access to the stored data, they may be regarded as such.⁵⁸ However, the data can be removed from a given server, or the owner of the server may be denied access to its contents (though having access to the server as a tangible object). Secondly, it is possible to argue that the *sui generis* database right lies at the structural level.⁵⁹ This may be the case if the understanding of the structural level would be larger than referring only to tangible objects – as the case is at the moment.⁶⁰ The *sui generis* database right reflects the syntactical information contained in the database, but it does not aim to cover or protect it.⁶¹ This right should be regarded as a *rei incorporalis*, and as such it grants the right-holder certain rights related to the database, effective against third parties, namely the right to prevent the contents of the database from being extracted or reused (Article 7(1) of the Database Directive).⁶² Because of these features, the *sui generis* database right is actually similar to the right of ownership of a tangible object that is placed at the structural level but is only linked with the contents of this object (e.g. the fact that a page of a book was printed incorrectly does not affect the right of ownership of the book). However, as explained above, the *sui generis* database right is of limited utility from the perspective of establishing a security interest over a database.

⁵⁸ Zech, H. (2015) Information as Property. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 6 (3), p. 196.

⁵⁹ Wiebe, A. (2016) Protection of industrial data – a new property right for the digital economy? *op. cit.*, pp. 881–882 places all the IP rights at the level of pragmatics.

⁶⁰ Zech, H. (2015) Information as Property. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 6 (3), p. 196.

⁶¹ Zech, H. (2012) *Information als Schutzgegenstand*. Tübingen: Mohr Siebeck, p. 366. Similarly, for the copyrights, Wiebe, A. (2016) Protection of industrial data – a new property right for the digital economy? *op. cit.* pp. 881–882. See, however, Vivant, M. (2006) La Privatisation de l'Information par la Propriété Intellectuelle. *Revue Internationale de Droit Économique*, vol. XX (4), pp. 380–381, who argues that the *sui generis* database right protects precisely the content of the information.

⁶² See Derclaye, E. (2021) The Database Directive. In: Irini Stamatoudi, Paul Torremans (eds.) *EU Copyright Law. A Commentary*. 2nd ed. Cheltenham–Northampton: Edward Elgar, pp. 234–237; Le Tourneau, P. (2022) *Contrats du Numérique*. 12th ed. Paris: Dalloz, pp. 560, 563–564. For more on the rights of the right-holder see: Judgment of 9 November 2004, British Horseracing, C-203/02, EU:C:2004:695, paras. 49–61; Judgment of 9 October 2008, Directmedia, C-304-07, EU:C:2008:552, paras. 35–53; Judgment of 3 June 2021, CV-Online Latvia, C-762-19, EU:C:2021:434, paras. 31–37.

These considerations can be summarised and illustrated by the following table:

Semantic level	Syntactic level	Structural level
Information with certain meaning. The intellectual content	Signs and their relationship with each other. Recorded information, not necessarily having a meaning	Information contained in a certain physical carrier or in a wider sense the structure of a physical object or a construct representing information
Mere data, particular information constituting database	The code reflecting the information stored, the database as such	The servers, the <i>sui generis</i> database rights

From the carried-out observation of databases at these three levels, it follows that not only their actual value lies at the syntactical level, but also precisely these features of databases that may lead businesses to use a database as collateral. Although there is actually no easy way to do so, this does not stop attempts to look for one.

5. ESTABLISHING AND ENFORCING THE SECURITY INTERESTS OVER DATABASES: CONCEPTUAL FRAMEWORK

The question of whether a database – its syntactical level – could be used as collateral is, at this very moment, a question of national law. Some jurisdictions may know the mechanisms allowing this to happen, while others may not and could possibly not want to recognise such rules. Existing rules were briefly discussed above. However, as mentioned, this paper does not aim to answer the question of such admissibility, but to provide for various legislative approaches that may be chosen to set a framework for the rules on securities established over databases.

The first approach that comes to mind in the context of *in rem* rights, such as security rights, is the question of establishing proprietary rights to a database. There are some points worth making here, even though, at the legislative level, the idea of proprietary rights to data has been abandoned. The discussion that took place mostly covered the question of data protection. In that it was argued that the proprietary rights are not needed to grant the sufficient level of protection and that, for example, the already existing regulation on trade secrets⁶³ could be regarded as a well-suited solution that also limits the means of protection to those data (datasets) that merit

⁶³ Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure. *Official Journal of the European Union*, (2016 L 157) 15 June. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0943> [Accessed: 9 January 2025].

protection.⁶⁴ However, the question of granting data with proprietary rights should not be limited to the issue of protection. The private law links many features with the proprietary rights, one of which, the fundamental one, is their effectiveness against third parties.⁶⁵ This feature also explains why the proprietary rights can be used to establish securities. The fact that protection may be granted through other means does not mean that some kind of subjective right will not be needed for other purposes. Of course, this cannot be the decisive argument in the discussion, though the perspective of other applications of the proprietary rights, including the establishment of a security interest, should be taken into consideration as well.

This paper focuses on databases – structured sets of data that can be retrieved and analysed – which are the potential objects of proprietary rights. These electronic records form the core of our discussion rather than mere data itself. Databases that consist of a given structure in which data are stored, a structure of limited accessibility, could be regarded as rival and excludable goods, making them more suitable as a subject of proprietary rights than the data as such.⁶⁶ To such databases, principles of specificity and publicity can be applied so they can be at least envisaged as the object of proprietary rights.⁶⁷ In some doctrinal categories, not generally reflected by the current legislation, databases – as the term is understood as a form of digital record

⁶⁴ See Aplin, T. (2017) Trading Data in the Digital Economy: Trade Secrets Perspective. In: Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer (eds.) *Trading Data in the Digital Economy: Legal Concepts and Tools*. Baden-Baden: Nomos-Hart, pp. 71–72; Weber, R.H. (2017) Improvement of Data Economy through Compulsory Licenses? In: Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer (eds.) *Trading Data in the Digital Economy: Legal Concepts and Tools*. Baden-Baden: Nomos-Hart, pp. 141–142. A more sceptical position was taken by Drexler, J. (2017) Designing Competitive Markets for Industrial Data – Between Propertisation and Access. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 8 (4), p. 269.

⁶⁵ van Erp, S. (2017) Ownership of Data: The Numerus Clausus of Legal Objects. *Brigham-Kanner Property Rights Conference Journal*, (6), p. 236.

⁶⁶ Data as such are regarded as non-rivalrous, but excludable or non-excludable, depending on the context. See van Erp, S. (2017) Ownership of Data: The Numerus Clausus of Legal Objects. *Brigham-Kanner Property Rights Conference Journal*, (6), p. 250; Duch-Brown, N., Martens, B. and Mueller-Langer, F. (2017) *The Economics of Ownership, Access and Trade in Digital Data*. JRC Digital Economy Working Paper No. 2017-01. Seville: European Commission, p. 46; Kerber, W. (2017) Rights on Data: The EU Communication ‘Building a European Data Economy’ from an Economic Perspective. In: Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer (eds.) *Trading Data in the Digital Economy: Legal Concepts and Tools*. Baden-Baden: Nomos-Hart, pp. 115–120; Rodríguez de las Heras Ballell, T. (2024) The Emergence of Principles and Best Practices on Digital Assets: Proprietary Rights, and Enforcement. *European Journal of Risk Regulation*, p. 5. Available from: <https://www.cambridge.org/core/services/aop-cambridge-core/content/view/B4DE880068B9292E7F2164715827067C/S1867299X24000552a.pdf/the-emergence-of-principles-and-best-practices-on-digital-assets-proprietary-rights-and-enforcement.pdf> [Accessed: 9 January 2025].

⁶⁷ van Erp, S. (2017) Ownership of Data: The Numerus Clausus of Legal Objects. *op. cit.* p. 239.

that, although capable of being multiplied, is observable as a tangible object – may be assigned to the group of *res digitales*.⁶⁸ Granting databases proprietary rights of any kind will include them in the well-established framework of *in rem* security rights that covers both their establishment (including their effectiveness against third parties) and enforcement. It will be possible to establish security without depriving the debtor of access and control over a database that may be necessary to pursue its business activity, e.g. in the form of the fiduciary transfer of such a right. Moreover, the very fact of the existence of an absolute right to an object guarantees, from the perspective of the legal system, greater stability of its value. However, as such a right would still be a conventional – maybe even artificial – construct, there is a risk that it may not be functional in practice. At the theoretical level, the proprietary right should grant a right-holder the right to access the database, though it is possible that a debtor, using simple technical measures, may restrain the creditor entitled to the right from it. A response to that risk may consist, in case of the databases stored with a blockchain technology, of using a smart contract to enforce the security. Another problem is related to the need to guarantee the limited accessibility of the database. For this purpose, apart from a contract on establishing the security interest over the database, certain clauses granting confidentiality may also be needed.

The second approach involves the inclusion of databases into the category of digital assets – deliberately avoiding the assignment of proprietary rights – and examining the possibility of applying the model rules on security interests over digital assets, i.e. the ELI Principles⁶⁹ and the UNIDROIT Principles,⁷⁰ to databases. The adopted definitions of digital assets differ from one another, though they are considered not to cover data or datasets.⁷¹

⁶⁸ The category of *res digitales*, existing alongside the traditional concepts of *res corporals* and *res incorporales*, was developed by Pałka, P. (2016) *Redefining 'Property' in the Digital Era. When Online, Do as the Romans Did*. EUI Working Paper LAW 2016/08, pp. 24–27. Available from: https://cadmus.eui.eu/bitstream/handle/1814/40366/LAW_2016_08.pdf?sequence=1&isAllowed=y [Accessed: 9 January 2025].

⁶⁹ European Law Institute (2022) *ELI Principles on the Use of Digital Assets as Security*. Vienna. Available from: https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Principles_on_the_Use_of_Digital_Assets_as_Security.pdf [Accessed 28 December 2024].

⁷⁰ UNIDROIT (2023) *UNIDROIT Principles on Digital Assets and Private Law*. Rome. Available from: <https://www.unidroit.org/wp-content/uploads/2024/01/Principles-on-Digital-Assets-and-Private-Law-linked-1.pdf> [Accessed 28 December 2024].

⁷¹ Rodríguez de las Heras Ballell, T. (2024) The Emergence of Principles and Best Practices on Digital Assets: Proprietary Rights, and Enforcement. *European Journal of Risk Regulation*, p. 5. Available from: <https://www.cambridge.org/core/services/aop-cambridge-core/content/view/B4DE880068B9292E7F2164715827067C/S1867299X24000552a.pdf/the-emergence-of-principles-and-best-practices-on-digi>

It is worth exploring whether databases may be covered by those rules, as digital assets are generally regarded as electronic records presenting some features required by the model rules. A digital database usually takes the form of an electronic record. The problem lies in its features, particularly the capability of being subject to control (Principle 2(2) of the UNIDROIT Principles). The concept of control – being in some way equivalent to possession – concerns the factual abilities that a person has in relation to the given digital assets.⁷² It was defined this way in Principle 6(1) of the UNIDROIT Principles, which provides for three abilities that characterise control. Those are: (i) the exclusive ability to prevent others from obtaining substantially all of the benefit from the digital asset; (ii) the ability to obtain substantially all of the benefit from the digital asset; and (iii) the exclusive ability to transfer those abilities to others and to the possibility of identifying an entity as having the mentioned abilities. The requirement of exclusivity is, however, relaxed in Principle 6(3) of the UNIDROIT Principles which provides for exceptions to this requirement if the digital asset or the relevant protocol or system limits the use of it and if the entity in control has agreed on sharing the ability referred to in Principle 6(1)(i) with others. The crucial question in the context of establishing the security rights over databases is how the database at its syntactic level could meet the criterion of exclusivity, and whether that is desirable. Firstly, databases are not necessarily designed to be exclusive assets, even if they present limited accessibility. Secondly, as mentioned, it may be beneficial for the debtor to maintain factual control over a database,⁷³ which can only be associated with granting control to the creditor, e.g. through the multiplication of the database or granting them additional access to the database. It requires rethinking whether granting exclusivity through technical means, e.g. by blocking access to the database in the event the obligation is not performed, when agreed that, for the duration of the security interest, both the debtor and creditor will have access to the

tal-assets-proprietary-rights-and-enforcement.pdf [Accessed: 9 January 2025]. In favour of including data into the category of digital assets: Nekit, K. (2024) The (Im)Possibility of Personal and Industrial (Machine-generated) Data to Be Subject to Property Rights. *International Journal of Law and Information Technology*, 32 (2), p. 9.

⁷² UNIDROIT (2023). *op. cit.* p. 52; Julienne, M. and Palmieri, F. (2023) Contrôle, Propriété et Possession dans les Principes UNIDROIT Relatifs aux Actifs Numériques. *Revue de Droit Bancaire et Financier*, (4), pp. 57–58; Rodríguez de las Heras Ballell, T. (2024) The Emergence of Principles and Best Practices on Digital Assets: Proprietary Rights, and Enforcement. *European Journal of Risk Regulation*, pp. 6–7. Available from: <https://www.cambridge.org/core/services/aop-cambridge-core/content/view/B4DE880068B9292E7F2164715827067C/S1867299X24000552a.pdf/the-emergence-of-principles-and-best-practices-on-digital-assets-proprietary-rights-and-enforcement.pdf> [Accessed: 9 January 2025].

⁷³ Lipton, J.D. (2001) Security Interests in Electronic Databases. *International Journal of Law and Information Technology*, 9 (1), p. 76.

database, could be the solution covered by Principle 6(3) of the UNIDROIT Principles.⁷⁴ The more complex definition of digital assets was adopted in the ELI Principles. In this view, digital assets are records or representations of value that are intangible (only electronically stored), capable of being subject to a right of control, enjoyment or use, and transferable.⁷⁵ As explained, the databases often present the market value, and since the ELI Principles opt for wide and economic understanding of “value”,⁷⁶ this condition is met. While requiring digital assets to be exclusively stored, displayed and administrated electronically, the ELI Principles indicate that it may happen through a database.⁷⁷ However, it should not be regarded as ruling out databases, understood in this paper as electronic records structuring datasets, as digital assets within the scope of the ELI Principles. The principles refer to databases as to the technical mean of storage, having, in this context, a different function. Yet, since the social media accounts, containing various type of data and features, are regarded as digital assets,⁷⁸ the same is for databases combining datasets in a structured manner via an electronic record. Therefore, taking the blackletters into consideration, as the concept of control under the ELI Principles is relaxed (in comparison to the UNIDROIT Principles) and the second criterion is limited to the factual possibility of accessing and enjoying the digital asset,⁷⁹ and as there should be no doubt that databases are tradable, qualifying databases as digital assets under the ELI Principles is not excluded.

Alternatively, one may argue that databases, as such, do not meet the requirements to be qualified as a digital asset in the meaning of the model rules, though it is possible to develop an access right (in the form of a code or a token) that could be qualified as a digital asset.⁸⁰ In this model, a database will not be regarded as an exclusive good, but such an access right will be, meaning that every entity having access to a database will have an individual asset over which they have exclusive control. Apart from the controversies of qualifying databases as digital assets, the plea against this second approach

⁷⁴ See UNIDROIT (2023). *op. cit.* p. 56, where it is stated that “a person who has control may wish to share its abilities with one or more other persons for purposes of convenience, security, or otherwise”.

⁷⁵ European Law Institute (2022). *op. cit.* pp. 18 – 19.

⁷⁶ European Law Institute (2022). *op. cit.* p. 19.

⁷⁷ European Law Institute (2022). *op. cit.* p. 17.

⁷⁸ European Law Institute (2022). *op. cit.* pp. 19 – 20.

⁷⁹ European Law Institute (2022). *op. cit.* p. 18.

⁸⁰ This idea was introduced during a meeting between the project team members and Matthias Lehmann, who took a strict interpretation of on the notion and criterion of exclusivity used in the UNIDROIT Principles because of its link to the *in rem* rights and *erga omnes* efficacy of the security rights. Introduction of the access right should be accompanied with amendments to the Database Directive that will make it clear that exercise of the access right is not an infringement to the IP rights under this directive.

may be the fact that the model rules address the rules on the enforcement of security rights only to the limited extent.⁸¹ There is therefore a risk that the possibility of establishing security interests over a database will be purely theoretic, lacking any efficient mechanisms of granting a creditor their rights.

The third approach is based on certain contractual schemes that may serve the purpose of establishing a security interest over a database. It is, for example, possible that two parties will enter into a contract on rules of access to a database that also grants them technical means of access, such as a given access code, which creates a contractual right to a database.⁸² Such a right could then be the object of a pledge (pledge on rights). It is also possible to imagine that a right of access will be linked to the *sui generis* database right, which is already, in some cases, used as collateral.⁸³ The contractual means are also important from the perspective of granting the confidentiality of the database and its content. It was admitted that – out of the scope of the Database Directive – it is possible to restrain others from accessing and using the database through the contractual means.⁸⁴ The same applies for the parties to a contract concerning the use of a database as collateral. However – and this is a general concern of all the considered contractual schemes – any kind of obligation would be binding only for the parties to a contract (*inter partes*). It means, on the one hand, that a breach of duty concerning the confidentiality of the database would only result in claims for damages against the liable party (but others will be able to legally access the contents of the database, which deprives it, at least partially, of value),⁸⁵ and, on the other hand, a contractual right of access to a database could only be enforceable against a given debtor. The use of contractual mechanisms in the context of security interests over databases is also possible in light of the views on treating data as a tradeable commodity.⁸⁶ The logical consequence of such a

⁸¹ European Law Institute (2025) *ELI Principles and Guidance for Enforcement Against Digital Assets*. Vienna, p. 9. Available from: https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Projects/Access_to_Digital_Assets/ELI_Principles_and_Guidance_for_Enforcement_Against_Digital_Assets.pdf [Accessed 24 June 2024]. See also Bujalski, M. (2025) Czy prawo francuskie może stanowić wzór dla regulacji realizacji zabezpieczeń na dobrach cyfrowych? *Forum Prawnicze*, 86 (2), p. 78.

⁸² Zech, H. (2016) Data as a Tradeable Commodity. In: Alberto De Franceschi (ed.) *European Contract Law and the Digital Single Market*. Cambridge–Antwerp–Portland: Intersentia, p. 59; Le Tourneau, P. (2022) *Contrats du Numérique*. 12th ed. Paris: Dalloz, p. 565.

⁸³ Ferling, M. (2023). *Digitale Information als Kreditsicherheit*. Tübingen: Mohr Siebeck, p. 155.

⁸⁴ Judgement of 15 January 2015, Ryanair, C-30/14, EU:C:2015:10, para. 45.

⁸⁵ Myška, M. and Harašta J. (2016) Less Is More? Protecting Databases in the EU after Ryanair. *op. cit.* p. 189; Zech, H. (2016) Data as a Tradeable Commodity. *op. cit.* p. 60.

⁸⁶ See in that matter De Franceschi, A. and Lehmann, M. (2015) Data as Tradeable Commodity and New Measures for their Protection. *The Italian Law Journal*, 1 (1), pp. 54–63; Zech, H. (2016) Data as a Tradeable Commodity. *op. cit.* pp. 52–61; American Law Institute and

stand is that also databases should be regarded as such. Hence, it could be possible that the enforcement of a security interest established over a database will consist of the transfer of the database to a creditor – which may be, for example, associated with the use of a smart contract – who will be also able to sell it further on the market, if the creditor does not personally have an interest in accessing the given dataset.

With regard to enforcement, in addition to the possibility of the creditor taking over the database (and/or rights associated with it) – to be used or sold – it is worth mentioning another method of enforcement that could be integrated into all three approaches. The debtor can often make the database available to other entities under a licensing model and base on this the business model. Then, the real benefit of the database is the licence fee (such a licence may or may not be a licence in the sense of intellectual property law – it depends on the object of the contract). The secured creditor's interest may, therefore, be satisfied if they are entitled to collect these benefits, for which they do not have to take over the database at all (and it may even be in their favour that it is the debtor who continues the business). This means that the enforcement of the security interest over a database may happen through such benefits, which in civil law terms would be regarded as fruits from the database (the proposed construction would be thus similar to the traditional institution of the *antichresis*).⁸⁷ Linking the enforceability of such benefits to the security interest established over a database allows the creditor to be satisfied from an abstract category for which the variability of the individual fees included in it is irrelevant. This is an important convenience in view of another construction that allows a creditor to be satisfied from such fees, i.e. the security interest created over the debtor's claims, which requires that every specific claim for a given fee be identified and indicated each time, including the entity obliged to satisfy it.

From the perspective of searching for legislative solutions there is not an easy choice, as all the approaches present some shortcomings. The main concerns that such a regulation has to address can be pointed out. They include, firstly, the actual access to the database, both for the creditor – in the event of non-performance – and for the debtor – while performing their obligation, which will allow them to pursue their activity. Secondly, there

European Law Institute (2023) *ALI-ELI Principles for a Data Economy: Data Transactions and Data Rights*, p. 18. Available from: https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ALI-ELI_Principles_for_a_Data_Economy.pdf [Accessed: 10 January 2025].

⁸⁷ See Żok, K. (2020) Zastaw Antychretyczny – Zagadnienia Konstrukcyjne. In: Karol Szadkowski, Krzysztof Żok (eds.) *Zabezpieczenia Wierzytelności*. Warszawa: Wolters Kluwer, pp. 93–99; Verhagen, H.L.E. (2022) *Security and Credit in Roman Law*. Oxford: Oxford University Press, pp. 257–268.

is the question of granting confidentiality and limited accessibility to the database, both before enforcing the security interest – in the interest of the debtor – and after the enforcement – in order not to deprive the value that the database presents for the secured creditor.

6. CONCLUSION

This article addresses the possible use of databases in order to secure receivable debts. The paper outlines the market utility of databases for this purpose, which is linked to their value and lies in three features: in the content of the database, in the structure that makes a database suitable for exploitation (rather than a pure set of information) and in the exclusive nature, or rather limited accessibility, of the database. The legal mechanisms concerning the use of databases as collaterals should take these features into consideration in order to guarantee that a security right will be established over a database as such, and will grant the secured creditor access to an asset of real value. Hence, if choosing from the three levels, it is the syntactical level of the database that should be regarded as the proper object of the security rights. To this level, containing the code resulting in the structured sequence of signs, should be assigned the actual ability to benefit from the database, as well as to exclude others from doing so. Because of that – as well as because of the latest legal developments in the European Union, i.e. the Data Act – the *sui generis* database right under Article 7(1) of the Database Directive is not a sufficient legal concept from the perspective of security interests established over databases. At a general level, this raises questions about the rationale for introducing and preserving the *sui generis* database right, particularly if it lacks commercial value even for the applications examined in this article.

For now, there are no specific legal regulations on the use of databases as collateral. The possibility depends on national legal solutions, but mostly on the concept of a good accepted in a given jurisdiction. However, from a comparative perspective, European private law lacks legal instruments for establishing security interests over databases. Therefore, theoretical proposals were developed to address this issue. Three approaches to this question were considered. Each of them presents some advantages and disadvantages and merits further examination in relation to a particular legal system. The first consists of (re)opening discussion on the proprietary rights in databases – accompanied by the view that the subjective right guarantees certainty from the perspective of the legal system. The second aims at including databases into the category of digital assets for which the model laws on security rights are now being developed. The third, the softest one, is based on the application of certain contractual schemes. The future

regulation, if a lawmaker of any level decides to provide for one, should preserve the features that make a database a valuable asset. One general conclusion is that, as long as data and databases present a market value, which is rather beyond doubt, their possible market applications may be varied in nature and so should not be limited to issues of protection or trading but also cover their use in order to secure a transaction.

LIST OF REFERENCES

- [1] Alejandre, G.M. (2021) Ownership of Databases: Personal Data Protection and Intellectual Property Rights on Databases. *European Review of Private Law*, 29 (5).
- [2] American Law Institute and European Law Institute (2023) *ALI-ELI Principles for a Data Economy: Data Transactions and Data Rights*. Available from: https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_el i/Publications/ALI-ELI_Principles_for_a_Data_Economy.pdf [Accessed: 10 January 2025].
- [3] Aplin, T. (2017) Trading Data in the Digital Economy: Trade Secrets Perspective. In: Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer (eds.) *Trading Data in the Digital Economy: Legal Concepts and Tools*. Baden-Baden: Nomos-Hart.
- [4] *Autobahnmaut* (2010) BGH, 25 March. (3) 2011 MMR, p. 188.
- [5] Banterle, F. (2018) The Interface Between Data Protection and IP Law: The Case of Trade Secrets and the Database *Sui Generis* Right in Marketing Operations, and the Ownership of Raw Data in Big Data Analysis. In: Mor Bakhoun, Beatriz Conde Gallego, Mark-Oliver Mackenrodt, Gintarė Surblytė-Namavičienė (eds.) *Personal Data in Competition, Consumer Protection and Intellectual Property Law*. Berlin: Springer.
- [6] Bourassin, M. (2024) *Droit des sûretés*. 8th ed. Paris: Lefebvre Dalloz.
- [7] Bujalski, M. (2025) Czy prawo francuskie może stanowić wzór dla regulacji realizacji zabezpieczeń na dobrach cyfrowych? *Forum Prawnicze*, 86 (2).
- [8] Bülow P. (2019) Digitales Mobiliarpfandrecht. *Zeitschrift für Wirtschafts- und Bankrecht*, (25).
- [9] Calzolaio, E. (2023) Digital Assets and Property: Comparative Remarks from a Civil Law Perspective, *Comparative Law Review*, 14 (2).
- [10] Calzolaio, E. (2024) From data property to data access and back again? Comparative remarks on the EU Data Act. *Iceonline*, (1). Available from: <https://www.lceonline.eu/wp-content/uploads/2024/04/I.03-Calzolaio.pdf> [Accessed 4 July 2025].
- [11] Catala, P. (1998) *Le Droit à l'Épreuve du Numérique*. Paris: Presses Universitaires de France.

- [12] De Franceschi, A. and Lehmann, M. (2015) Data as Tradeable Commodity and New Measures for their Protection. *The Italian Law Journal*, 1 (1).
- [13] Derclaye, E. (2004) Databases Sui Generis Right: Should We Adopt the Spin Off Theory? *European Intellectual Property Review*, 26 (9).
- [14] Derclaye, E. (2008) *The Legal Protection of Databases. A Comparative Analysis*. Cheltenham–Northampton: Edward Elgar.
- [15] Derclaye, E. (2021) The Database Directive. In: Irini Stamatoudi, Paul Torremans (eds.) *EU Copyright Law. A Commentary*. 2nd ed. Cheltenham–Northampton: Edward Elgar.
- [16] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases. *Official Journal of the European Union* (1996 L 77) 27 March. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31996L0009> [Accessed 28 December 2024].
- [17] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure. *Official Journal of the European Union* (2016 L 157) 15 June. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0943> [Accessed: 9 January 2025].
- [18] Doldirina, C. et al. (2016) Legal Approaches for Open Access to Research Data. *Law Archive Papers*. Available from: https://osf.io/preprints/lawarchive/n7gfa_v1 [Accessed 24 June 2024].
- [19] Drexler, J. et al. (2016) *Data Ownership and Access to Data. Position Statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the Current European Debate*. Max Planck Institute for Innovation and Competition Research Paper No. 16-10. Available from: https://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/positionspaper-data-eng-2016_08_16-def.pdf [Accessed 31 December 2024].
- [20] Drexler, J. (2017) Designing Competitive Markets for Industrial Data – Between Propertisation and Access. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 8 (4).
- [21] Drexler, J. et al. (2022) *Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission’s Proposal of 23 February 2022 for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act)*. Max Planck Institute for Innovation and Competition Research Paper No. 22-05, pp. 91–96. Available from: https://pure.mpg.de/rest/items/item_33

- 88757_4/component/file_3395639/content [Accessed 30 December 2024].
- [22] Drobnig, U. (2012) Security Rights in Movable Assets. In: Jürgen Basedow, Klaus J. Hopt, Reinhard Zimmermann (eds.) *Max Planck Encyclopedia of European Private Law*. Oxford: Max-Planck-Gesellschaft. Available from: https://max-eup2012.mpipriv.de/index.php/Security_Rights_in_Movable_Assets [Accessed 28 December 2024].
- [23] Duch-Brown, N., Martens, B. and Mueller-Langer, F. (2017) *The Economics of Ownership, Access and Trade in Digital Data*. JRC Digital Economy Working Paper No. 2017-01. Seville: European Commission.
- [24] European Commission (2017) *Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy*. SWD(2017) 2 final. Brussels: European Commission. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017SC0002> [Accessed 30 December 2024].
- [25] European Commission (2022) *Study to Support an Impact Assessment for the Review of the Database Directive. Final Report*. Luxembourg: Publications Office of the European Union. Available from: <https://digital-strategy.ec.europa.eu/en/library/impact-assessment-report-and-support-studies-accompanying-proposal-data-act> [Accessed 30 December 2024].
- [26] European Commission (2022) *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. Brussels. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0068> [Accessed 30 December 2024].
- [27] European Law Institute (2022) *ELI Principles on the Use of Digital Assets as Security*. Vienna. Available from: https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Principles_on_the_Use_of_Digital_Assets_as_Security.pdf [Accessed 28 December 2024].
- [28] European Law Institute (2025) *ELI Principles and Guidance for Enforcement Against Digital Assets*. Vienna. Available from: https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Projects/Access_to_Digital_Assets/ELI_Principles_and_Guidance_for_Enforcement_Against_Digital_Assets.pdf [Accessed 24 June 2024].
- [29] Ferling, M. (2023) *Digitale Information als Kreditsicherheit*. Tübingen: Mohr Siebeck.

- [30] Graux, H. (2024) *What Is Data Ownership, and Does It Still Matter under EU Data Law?* Luxembourg: Publications Office of the European Union. Available from: <https://data.europa.eu/sites/default/files/report/What\%20is\%20data\%20ownership\%2C\%20and\%20does\%20it\%20still\%20matter\%20under\%20EU\%20data\%20law.pdf> [Accessed 30 December 2024].
- [31] Heller, D., Leitzinger, L. and Walz U. (2024) Intellectual Property as Business Loan Collateral: A Taxonomy of Institutional and Economic Determinants. *GRUR International – Journal of European and International IP Law*, 73 (5).
- [32] Hugenholtz, P.B. (2017) Data Property in the System of Intellectual Property Law: Welcome Guest or Misfit? In: Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer (eds.) *Trading Data in the Digital Economy: Legal Concepts and Tools*. Baden-Baden: Nomos–Hart.
- [33] Judgment of 9 November 2004, British Horseracing, C-203/02, EU:C:2004:695.
- [34] Judgment of 9 November 2004, Fixtures Marketing, C-338/02, EU:C:2004:696.
- [35] Judgment of 9 November 2004, Fixtures Marketing, C-46/02, EU:C:2004:694.
- [36] Judgment of 9 November 2004, Fixtures Marketing, C-444/02, EU:C:2004:697.
- [37] Judgment of 9 October 2008, Directmedia, C-304-07, EU:C:2008:552.
- [38] Judgement of 15 January 2015, Ryanair, C-30/14, EU:C:2015:10.
- [39] Judgment of 3 June 2021, CV-Online Latvia, C-762-19, EU:C:2021:434.
- [40] Julienne, M. (2020) Les Actifs Numériques, Entre Droit et Technologie. *Bulletin Joly Bourse*, (1).
- [41] Julienne, M., Palmieri, F. (2023) Contrôle, Propriété et Possession dans les Principes UNIDROIT Relatifs aux Actifs Numériques. *Revue de Droit Bancaire et Financier*, (4).
- [42] Kerber, W. (2017) Rights on Data: The EU Communication ‘Building a European Data Economy’ from an Economic Perspective. In: Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer (eds.) *Trading Data in the Digital Economy: Legal Concepts and Tools*. Baden-Baden: Nomos–Hart.
- [43] Kieninger, E.-M. (2004) Introduction: Security Rights in Movable Property within the Common Market and the Approach of the Study. In: Eva-Maria Kieninger (ed.) *Security Rights in Movable Property in European Private Law*. Cambridge: Cambridge University Press.
- [44] Kieninger, E.-M. (2021) Security Rights in Intellectual Property. In: Katharina Boele-Woelki, Diego P. Fernández Arroyo, Alexandre Segenacnik (eds.) *General Reports of the XXth General Congress of the International Academy of Comparative Law*. Cham: Springer.

- [45] Kim, D. (2024) Der Datenbankschutz sui generis nach dem Data Act. Having the cake and eating it too? *Zeitschrift für das Recht der Digitalisierung, Datenwirtschaft und IT*, MMR Appendix.
- [46] Leistner, M. (2017) Big Data and the EU Database Directive 96/9/EC: Current Law and Potential for Reform. In: Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer (eds.) *Trading Data in the Digital Economy: Legal Concepts and Tools*. Baden-Baden: Nomos–Hart.
- [47] Le Tourneau, P. (2022) *Contrats du Numérique*. 12th ed. Paris: Dalloz.
- [48] Lipton, J.D. (2001) Security Interests in Electronic Databases. *International Journal of Law and Information Technology*, 9 (1).
- [49] Lisanti, C. and Pérechon, F. (2023) Le Nantissement d'Actifs Incorporels. *Revue des Procédures Collectives*, (3).
- [50] Mekki, M. (2024) Actifs Numériques. In: *Répertoire de Droit Commercial*. Paris: Dalloz.
- [51] Myška, M. and Harašta J. (2016) Less Is More? Protecting Databases in the EU after Ryanair. *Masaryk University Journal of Law and Technology*, 10 (2).
- [52] Nekit, K. (2024) The (Im)Possibility of Personal and Industrial (Machine-generated) Data to Be Subject to Property Rights. *International Journal of Law and Information Technology*, 32 (2).
- [53] Pałka, P. (2016) Redefining 'Property' in the Digital Era. *When Online, Do as the Romans Did*. EUI Working Paper LAW 2016/08. Available from: https://cadmus.eui.eu/bitstream/handle/1814/40366/LAW_2016_08.pdf?sequence=1&isAllowed=y [Accessed: 9 January 2025].
- [54] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act). *Official Journal of the European Union* (L 2023/2854) 22 December. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R2854&qid=1735552065097> [Accessed 30 December 2024].
- [55] Richter, H. (2024) Article 43 of the Data Act. In: Heinrich Amadeus Wolff, Stefan Brink, Antje v. Ungern-Sternberg (eds.) *BeckOK Datenschutzrecht*. 50th ed. München: C.H. Beck.
- [56] Rodríguez de las Heras Ballell, T. (2024) The Emergence of Principles and Best Practices on Digital Assets: Proprietary Rights, and Enforcement. *European Journal of Risk Regulation*. Available from: <https://www.cambridge.org/core/services/aop-cambridge-core/content/view/B4DE880068B9292E7F2164715827067C/S1867299X24000552a.pdf/the-emergence-of-principles-and-best-practices-on-digital->

- assets-proprietary-rights-and-enforcement.pdf [Accessed: 9 January 2025].
- [57] Séjean, M. and Binctin, N. (2019) Sûretés Réelles Mobilières sur la Propriété Intellectuelle. *Revue Internationale de Droit Comparé*, 71 (2).
- [58] UNCITRAL (2011) *UNCITRAL Legislative Guide on Secured Transactions. Supplement on Security Rights in Intellectual Property*. Rome. Available from: https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/10-57126_ebook_suppl_sr_ip.pdf [Accessed 28 June 2025].
- [59] UNIDROIT (2023) *UNIDROIT Principles on Digital Assets and Private Law*. Rome. Available from: <https://www.unidroit.org/wp-content/uploads/2024/01/Principles-on-Digital-Assets-and-Private-Law-linked-1.pdf> [Accessed 28 December 2024].
- [60] Weber, R.H. (2017) Improvement of Data Economy through Compulsory Licenses? In: Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer (eds.) *Trading Data in the Digital Economy: Legal Concepts and Tools*. Baden-Baden: Nomos-Hart.
- [61] Wiebe, A. (2016) Protection of industrial data – a new property right for the digital economy? *GRUR International – Journal of European and International IP Law*, (10).
- [62] Wiebe, A. (2023) The Data Act Proposal. Access rights at the Intersection with Database Rights and Trade Secret Protection. *Gewerblicher Rechtsschutz und Urheberrecht*, (4).
- [63] World Intellectual Property Organization (2002) *Summary on Existing Legislation Concerning Intellectual Property in Non-Original Databases*. SCCR/8/3. Geneva. Available from: https://www.wipo.int/edocs/mdocs/copyright/en/sccr_8/sccr_8_3.pdf [Accessed 24 June 2025].
- [64] van Erp, S. (2017) Ownership of Data: The Numerus Clausus of Legal Objects. *Brigham-Kanner Property Rights Conference Journal*, (6).
- [65] Verhagen, H.L.E. (2022) *Security and Credit in Roman Law*. Oxford: Oxford University Press.
- [66] Vivant, M. (2006) La Privatisation de l'Information par la Propriété Intellectuelle. *Revue Internationale de Droit Économique*, vol. XX (4).
- [67] *Your Response Ltd v. Datateam Business Media Ltd* (2014) Court of Appeal, 3 WLR, p. 887.
- [68] Zech, H. (2012) *Information als Schutzgegenstand*. Tübingen: Mohr Siebeck.
- [69] Zech, H. (2015) Information as Property. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 6 (3).

- [70] Zech, H. (2015) „Industrie 4.0“ – Rechtsrahmen für eine Datenwirtschaft im digitalen Binnenmarkt. *Gewerblicher Rechtsschutz und Urheberrecht*, (12).
- [71] Zech, H. (2016) A Legal Framework for a Data Economy in the European Digital Single Market: Rights to Use Data. *Journal of Intellectual Property Law & Practice*, 11 (6).
- [72] Zech, H. (2016) Data as a Tradeable Commodity. In: Alberto De Franceschi (ed.) *European Contract Law and the Digital Single Market*. Cambridge–Antwerp–Portland: Intersentia.
- [73] Zimmer, D. (2017) Property Rights Regarding Data? In: Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer (eds.) *Trading Data in the Digital Economy: Legal Concepts and Tools*. Baden-Baden: Nomos–Hart.
- [74] Żok, K. (2020) Zastaw Antychretyczny – Zagadnienia Konstrukcyjne. In: Karol Szadkowski, Krzysztof Żok (eds.) *Zabezpieczenia Wierzytelności*. Warszawa: Wolters Kluwer.

ARTIFICIAL INTELLIGENCE IN THE SERVICE OF PARLIAMENTS: SOME ARGUMENTS FOR THE NECESSITY OF A NORMATIVE LEGAL FRAMEWORK AT THE EUROPEAN LEVEL *

by

BOLDIZSÁR SZENTGÁLI-TÓTH [†] RUDOLF BERKES [‡]

This contribution examines the need for European normative legal framework governing artificial intelligence implementation in parliamentary institutions. Using a three-pillar methodology—analysing soft law instruments (particularly Inter-Parliamentary Union Resolution and Guidelines), investigating European parliamentary AI use cases, and developing policy recommendations—the study reveals significant regulatory gaps. Whilst the EU AI Act provides limited coverage of parliamentary AI applications, several European legislative bodies (Estonia, Italy, Portugal, Spain, the European Parliament) have successfully implemented AI for speech recognition, document processing, and citizen engagement. Current soft law frameworks establish important principles including transparency, privacy protection, and sustainability, yet lack binding force. The research demonstrates that parliamentary AI's connection to democratic processes and national sovereignty necessitates stronger oversight. Two regulatory approaches are proposed: reclassifying parliamentary AI as high-risk under the EU AI Act, or developing dedicated European legislation addressing fundamental rights protection, national sovereignty, security concerns, and innovation promotion. The study concludes that establishing explicit European normative regulation would provide essential democratic safeguards whilst maintaining national sovereignty,

* This research has been funded by the Perspectives and Limits of Algorithmic Constitutionalism Momentum/Lendület Research Group of the Hungarian Academy of Sciences (LP2024-20/2024).

[†] Senior Research Fellow, ELTE CSS Institute for Legal Studies. E-mail: totboldi@gmail.com

[‡] Researcher, ELTE CSS Institute for Legal Studies, Doctoral student, ELTE Doctoral School of Sociology. E-mail: rudolf.berkes.ai@gmail.com

parliamentary autonomy and fostering technological innovation in European democratic institutions.

KEY WORDS

Parliament, Artificial Intelligence, EU Regulation, Soft Law, Legislation

1. INTRODUCTION

Artificial intelligence (AI) is reshaping almost all areas of our lives,¹ including legal work² and its countless subfields.³ Among these fields, in recent years, a rapidly enriching strand of academic literature⁴ has focused on the potential parliamentary application of AI.⁵ As a consequence, the Fourth Global Conference on Parliamentary Studies was devoted almost exclusively to the potential exploitation of AI in parliamentary institutions.⁶

In the meantime, the Inter-Parliamentary Union (IPU) discussed the subject in more of its congresses and finally enacted a resolution on the impact of artificial intelligence on democracy, human rights, and the rule of law (IPU Resolution). Besides this, the IPU also published its detailed Guidelines for parliaments on how to implement AI into their daily operations. Therefore, one may conclude that soft law instruments as paramount points of reference for parliamentary staff could facilitate the prudent but efficient parliamentary AI implementation.⁷

¹ Baptista, J. et al. (2020) Digital Work and Organisational transformation: Emergent Digital/Human Work Configurations in Modern Organisations. *The Journal of Strategic Information Systems*, 29(2). pp. 101-118.

² Bex, F. J. (2024) AI, Law and beyond. A transdisciplinary ecosystem for the future of AI & Law. *Artificial Intelligence and Law*, vol. 33, Available from: <https://doi.org/10.1007/s10506-024-09404-y> [Accessed: 22 Jun. 2025]; See also: Homoki P. and Zódi Z. (2024) Large language models and their possible uses in law. *Hungarian Journal of Legal Studies*, vol. 64. (3) 2023. Available from: <https://doi.org/10.1556/2052.2023.00475>. pp. 435-455.

³ Benedetto, I. et al. (2025) Leveraging large language models for abstractive summarization of Italian legal news. *Artificial Intelligence and Law*, 2025, Available from: <https://doi.org/10.1007/s10506-025-09431-3>

⁴ Koryzis, D. et al. (2023) Disruptive Technologies for Parliaments: A Literature Review. *Future Internet*, 15(2), Available from: <https://doi.org/10.3390/fi15020066>

⁵ Ziouvelou, X. Giannakopoulos, G. and Giannakopoulos, V. (2022) Artificial Intelligence in the Parliamentary Context. In: F. Fitsilis and G. Mikros (eds.) *Smart Parliaments: Data-Driven Democracy*. European Liberal Forum. Available from: https://liberalforum.eu/wp-content/uploads/2022/11/Smart-Parliaments_ELF-Study_Techno-Politics_vol.4.pdf [Accessed 26 Jun. 2025]. pp. 43-53.

⁶ Fytsilis, F. (2025) *4th Global Conference on Parliamentary Studies – Program*. [online] Available from: <https://hellenicocrteam.gr/4th-global-conference-on-parliamentary-studies-program/> [Accessed 26 Jun. 2025].

⁷ van Noordt, C. and Misuraca, G. (2020) Exploratory Insights on Artificial Intelligence for Government in Europe. *Social Science Computer Review*, 40(2). Available from: <https://doi.org/10.1177/0894439320980449>, pp. 426-444.

By contrast, one may rely on very few normative legal rules when AI is used for parliamentary purposes,⁸ which has also been underlined by Fitsilis and Almeida,⁹ Guihot and his co-authors,¹⁰ and by Scherer.¹¹ The main text of the European Union's (EU) AI regulation (EU AI Act) adopted by the European Parliament (EP) on March 13, 2024, approved by the Council on May 21, and published in the Official Gazette on June 13, 2024,¹² contains just an indirect reference¹³ that high-risk AI-based technologies subject to stricter requirements are enumerated in EU AI Act Annex No. 3.

This annex classifies as high-risk only those AI-based applications related to democratic processes that directly aim to influence voter behavior or to shape the final result of a vote. It derives from this that technologies promoting the internal functioning of the legislature and the relationship between parliaments and citizens are not included in this category.

The consequence is that although European legislation generally perceives the sources of danger affecting democracy and reflects on them, it nevertheless makes a definite distinction on the basis of risk, thereby leaving a relatively wide scope for the development of AI-based software that could possibly make the daily activities of parliaments smoother. Nevertheless, the strong link of parliamentary operation with national sovereignty and democratic processes,¹⁴ the distinguished role of parliaments as a crucial constitutional actor, and the rapidly emerging use of AI in parliaments

⁸ Fitsilis, F. Koryzis, D. and Schefbeck, G. (2022) Legal Informatics Tools for Evidence-Based Policy Creation in Parliaments. *International Journal of Parliamentary Studies*, 2(1). Available from: <https://doi.org/10.1163/26668912-bja10031>. pp. 5–29.

⁹ Fitsilis, F. and Rêgo de Almeida, P. G. (2024) Chapter 9: Artificial intelligence and its regulation in representative institutions. In: *Research Handbook on Public Management and Artificial Intelligence*, Cheltenham, UK: Edward Elgar Publishing. Available from: <https://doi.org/10.4337/9781802207347.00019> [Accessed 26 June 2025].

¹⁰ Guihot, M. Matthew, A.F. and Suzor, N.P. (2017) Nudging Robots: Innovative solutions to Regulate Artificial Intelligence. *Vanderbilt Journal of Entertainment and Technology Law*, Vol. 20, No. 2. Available from: <https://scholarship.law.vanderbilt.edu/jetlaw/vol20/iss2/2>. pp. 385–456.

¹¹ Scherer, M. U. (2016) Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, And Strategies. *Harvard Journal Of Law & Technology*, 29(2). Available from: <https://jolt.law.harvard.edu/articles/pdf/v29/29HarvJLTech353.pdf> [Accessed 26 June 2025]. pp. 358–376.

¹² Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828. *Official Journal of the European Union* (OJ L 2024/1689) 12 July. Available from: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>

¹³ Regulation (EU) 2024/1689, *op. cit.* art. 6. (2)

¹⁴ Bareis, J. and Katzenbach, C. (2022) Talking AI into being: The narratives and imaginaries of national AI strategies and their performative politics. *Science, Technology, & Human Values*, 47(5), pp. 855–881.

may provide strong arguments for the reconsideration of the current classification.¹⁵

Keeping this in mind, parliamentary AI applications would reasonably fall under a category with a higher risk perception and stricter demands for safeguards. The alternative to this might be the drafting of a European legal framework for parliamentary AI implementation; however, this legal instrument should not impose such duties on parliamentary staff which may undermine national sovereignty.¹⁶

Our contribution analyzes the latest European soft law instruments and the known European use cases of parliamentary AI involvement. Based on this, we argue, as a main hypothesis, either for the necessity of a European legal framework for parliamentary AI or for the reconsideration of the current classification of the EU AI Act.

2. METHODOLOGY

Our research has been based on three main pillars. Firstly, we analyzed the European and global soft law environment concerning parliamentary AI, with special regard to the IPU Resolution, the IPU Guidelines, and their fundamental principles. Although the fact that a number of international organizations have enacted soft law instruments focusing on AI implementation, the IPU resolution and guidelines provide the first legal framework of reference specifically tailored to the special needs of parliamentary institutions.

Secondly, the European use cases of parliamentary AI have been investigated: we have relied on the contact information provided by the IPU Innovation Tracker and approached several international organizations as well as national parliamentary staff requiring information about their AI policies. Where it was possible, some online consultations were also arranged with colleagues; besides this, information was also collected with the help of desk research. Based on the information at our disposal, we have identified which parliaments have already assisted their daily operations with AI-based applications and which ones have made meaningful preparatory steps in this direction. Then, we have selected those European parliamentary institutions, where AI has been already implemented into the daily operation of the parliamentary work in a meaningful way. As a consequence, Estonia, Italy,

¹⁵ Orwat, C. et al. (2024) Normative challenges of risk regulation of artificial intelligence, *NanoEthics*, 18(2). Available from: <https://doi.org/10.1007/s11569-024-00454-9>

¹⁶ Mügge, D. (2024) EU AI sovereignty: for whom, to what end, and to whose benefit? *Journal of European Public Policy*, 31(8). Available from: <https://doi.org/10.1080/13501763.2024.2318475>. pp. 2200–2225

Portugal, Spain and the European Parliament will be discussed in more detail.

Since our contribution examines the potential perspectives of European law-making concerning parliamentary AI, less attention has been paid to the Latin American and Asian pioneers of parliamentary AI implementation, such as Argentina,¹⁷ Brazil,¹⁸ Chile,¹⁹ Bahrain,²⁰ India,²¹ or Japan.²² These paramount models are mentioned only sporadically, illustrating the global scale of parliamentary AI implementation; however, our focus remains on the European dimensions of the issue. Among others, the compliance of the European use cases with the fundamental principles of the IPU Resolution is also scrutinized. We provide a summarizing table of the the most developed European models, which may help to understand the similarities and differences of these solutions.

¹⁷ Barber, H. (2025) *Argentina will use AI to 'predict future crimes' but experts worry for citizens' rights*. [online] The Guardian, Available from: <https://www.theguardian.com/world/article/2024/aug/01/argentina-ai-predicting-future-crimes-citizen-rights>

¹⁸ Agora. (2021) *Brazil Ulysses machine learning for transparency and citizen participation*. [online] Available from: <https://www.agora-parl.org/events-and-lectures/brazil-ulysses-machine-learning-transparency-and-citizen-participation> [Accessed 22 Jun. 2025]; Nesta. (2025) *The Brazilian Chamber of Deputies' LabHacker and eDemocracia*. [online], Available from: <https://www.nesta.org.uk/feature/six-pioneers-digital-democracy/the-brazilian-chamber-of-deputies-labhacker-and-edemocracia/>; Souza, E. et al. (2021) *An Information Retrieval Pipeline for Legislative Documents from the Brazilian Chamber of Deputies*, *Frontiers in artificial intelligence and applications*. Available from: <https://doi.org/10.3233/faia210326>. pp. 119-126.

¹⁹ Hankins, E. (2024) *Strengthening AI governance in Chile: GoBLab UAI and the importance of collaboration*. [online] Oxford Insights. Available from: <https://oxfordinsights.com/insights/strengthening-ai-governance-in-chile/>, [Accessed: 22 Jun. 2025].

²⁰ Inter-Parliamentary Union. (2025). *Automated Hansard report system: Converting parliamentary audio to text using AI*. [online] Available from: <https://www.ipu.org/ai-use-cases/automated-hansard-report-system-converting-parliamentary-audio-text-using-ai> [Accessed 26 June. 2025].

²¹ Dharmaraj, S. (2025). *AI Revolutionising India's Parliamentary Operations – OpenGov Asia*. [online] Available from: <https://opengovasia.com/2025/03/19/ai-revolutionising-indias-parliamentary-operations/> [Accessed 26 Jun. 2025].

²² Kawahara, T. (2012) *Transcription System Using Automatic Speech Recognition for the Japanese Parliament (Diet)*, *Proceedings of the AAAI Conference on Artificial Intelligence*, 26(2). Available from: <https://doi.org/10.1609/aaai.v26i2.18962>; Kawahara, T. (2017) *Automatic meeting transcription system for the Japanese parliament (diet)*. 2022 *Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)*, 1. Available from: <https://doi.org/10.1109/apsipa.2017.8282177>. pp.1006–1010; Kawahara, T. Ueno S. & Morikawa M. (2020) *Transcription system using ASR in the Japanese Parliament*. *The Journal of Professional Reporting and Transcription*, 1/2020. Available from: <https://tiro.intersteno.org/2020/05/transcription-system-using-automatic-speech-recognition-in-the-j>

Thirdly, the main conclusions are drawn from the existing soft law instruments as well as the improving European use cases in the discussion section. As a result, some policy recommendations are put forward for European policymakers on how the parliamentary use of AI could be covered by normative legal regulation. On the one hand, the potential amendment of the EU AI Act is proposed; on the other hand, the main contours of a European legal instrument covering parliamentary use of AI are outlined. We do not aim to formulate a complete regulatory concept but rather to highlight those key considerations that should be kept in mind by policy-makers when such a European legal instrument is drafted and negotiated. Among these, the protection of national sovereignty should be prioritized due to the outstanding role of national parliaments as constitutional actors representing popular sovereignty.²³

Nevertheless, it would mean a remarkable advantage in competitiveness for Europe if it were able to regulate, firstly with normative terms, the parliamentary use of AI. Carefully tailored rules that would provide just European safeguards for the prudent but efficient exploitation of AI-based parliamentary tools could promote a proper compromise between the encouragement of innovation, the protection of fundamental rights, and the integrity of democratic processes.

3. THE ENACTMENT AND THE MAIN PRINCIPLES OF THE IPU RESOLUTION ON THE IMPACT OF ARTIFICIAL INTELLIGENCE ON DEMOCRACY, HUMAN RIGHTS AND THE RULE OF LAW

As we have seen, normative European regulation is still in its initial stage in relation to AI's integration into parliaments. In order to think about how to develop it further, we first need to look at the current soft law framework, which, if not binding, is a benchmark for parliaments. The weight of the topic is clearly shown by the fact that in the year 2024 we experienced a major breakthrough in both soft law and normative supranational legislation. In the legislative agenda of the European Union, the relationship between AI and parliaments has received little attention, apart from the aforementioned indirect reference of the EU AI Act, only soft law instruments cover even implicitly certain aspects of parliamentary AI applications. On behalf of the European Union, successive resolutions of the EP have touched on this topic

²³ Krasner, S. D. (2016) The persistence of state sovereignty. In: Fioretos, O. Falleti, T. G. & Sheingate A. (eds.) *The Oxford handbook of historical institutionalism*. Oxford University Press. pp. 521–537

only tangentially,²⁴ while the Council of Europe has established a Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law in September 2024.²⁵ Nevertheless, at European level, there is no soft law instrument focusing specifically on AI and parliament, as the aforementioned documents are more general in nature in providing requirements for the use of AI.

In the context of soft law focusing specifically on the implementation of AI-based parliamentary tools, the efforts of the IPU should be highlighted, as the central theme of both 2024 IPU general assemblies focused on the parliamentary perspectives of AI.²⁶ Moreover, it is also worth mentioning that the IPU organized global congresses in the fall of 2022 in Helsinki and in the fall of 2023 in Montevideo to discuss challenges related to the future of parliaments, especially their technological background. As a result of the negotiations, in October 2024, the 149th IPU Congress in Geneva adopted the IPU Resolution.²⁷ In this Resolution the organization laid down detailed standards regarding the application of AI to certain parliamentary tasks. Although the document is not legally binding and contains few specifics, it can serve as an important reference point for national parliaments around the world when they are looking for the right balance between exploiting the benefits of technological development and eliminating its risks. In summary, despite the lack of direct European attention to regulating parliamentary AI use, national parliaments have contributed to a global framework through the auspices of the IPU.

²⁴ European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)); European Parliament resolution of 12 February 2019 on a comprehensive European industrial policy on artificial intelligence and robotics (2018/2088(INI)); European Parliament resolution of 12 February 2020 on automated decision-making processes: ensuring consumer protection and free movement of goods and services (2019/2915(RSP)); European Parliament resolution of 20 October 2020 on intellectual property rights for the development of artificial intelligence technologies (2020/2015(INI)); European Parliament resolution of 19 May 2021 on artificial intelligence in education, culture and the audiovisual sector (2020/2017(INI)); European Parliament resolution of 20 May 2021 on shaping the digital future of Europe: removing barriers to the functioning of the digital single market and improving the use of AI for European consumers (2020/2216(INI)); European Parliament resolution of 3 May 2022 on artificial intelligence in a digital age (2020/2266(INI));

²⁵ Council of Europe. (2024) *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*. Vilnius

²⁶ Inter-Parliamentary Union. (2024) *emphGlobal parliamentary community recommit to multilateralism for peace*. [online] Available from: <https://www.ipu.org/news/press-releases/2024-10/global-parliamentary-community-recommits-multilateralism-peace> [Accessed 26 June. 2025].

²⁷ IPU. (2024) *The impact of artificial intelligence on democracy, human rights and the rule of law*. Resolution adopted unanimously by the 149th IPU Assembly.

As our proposals are also based on the considerations and principles of the IPU Resolution and Guidelines, and this means the primary point of reference also for European parliamentary institutions, we will briefly review these documents below and assess the known use cases accordingly.

3.1. THE LEGAL AIM OF THE IPU RESOLUTION

The IPU Resolution in its preambulatory clauses emphasizes the need for an “inclusive, responsible, and evidence-based global approach” to AI governance that “ensures equitable policy outcomes, for the entire world”,²⁸ while addressing the lack of comprehensive, transparent regulations aligned with democratic values.²⁹ It calls for balanced regulation that fosters innovation benefiting humanity³⁰, and later it recognizes the adaptability of existing national laws to AI challenges, and respects national sovereignty in developing AI frameworks.³¹ As seen in Table 1, all of these four preambulatory clauses point to §4 and §6 of the IPU Resolution, setting out the main legal aim of the IPU Resolution.

The main legal aim of the IPU Resolution is to urge parliaments around the world to work with civil society groups, academia and research groups in order to “effectively and transparently adopt or maintain strong legal frameworks and policies for the responsible creation, deployment and use of AI technology, and to contribute to efforts to establish global standards and frameworks”.³² Point 6 of the IPU Resolution also invites parliaments “to give priority to reviewing existing legislation and regulations to ensure that advances in AI technology do not result in loopholes in existing protections for democracy, human rights, the rule of law and State sovereignty”.³³

3.2. LEGAL FRAMEWORK OF THE IPU RESOLUTION

The envisaged features of the intended legal framework recommended by the IPU resolution include (1) gender equality, (2) inclusive development and diversity, (3) transparent and accountable AI development, (4) privacy, and (5) sustainability.

The IPU Resolution emphasizes that more understanding of AI is necessary for well-informed discussion, acknowledging that AI systems have the potential to strengthen gender-based violence, discrimination, and societal biases, particularly those against women in politics, damaging

²⁸ IPU. (2024) *op. cit.* Preamble, clause 7.

²⁹ IPU. (2024) *op. cit.* Preamble, clause 10.

³⁰ IPU. (2024) *op. cit.* Preamble, clause 11.

³¹ IPU. (2024) *op. cit.* Preamble, clause 13.

³² IPU. (2024) *op. cit.* point 4.

³³ IPU. (2024) *op. cit.* point 6.

democratic institutions and public confidence.³⁴ It emphasizes how AI, particularly generative AI, can reinforce and magnify gender inequality and prejudice in the absence of gender-balanced viewpoints and data. Negative effects include deepfake material that frequently silences women, especially in political life.³⁵

As seen in Table 1, these issues raised in the IPU Resolution for recommended solutions.³⁶ With a particular emphasis on reducing digital gender barriers and strengthening international collaboration to promote equal access to AI advantages, the IPU Resolution urges immediate action to address digital divides both within and between nations by upgrading infrastructure, connection, and skills.³⁷ Through enhanced content moderation, easily accessible reporting channels, and protocols to eliminate unlawful content, it calls for parliaments to proactively prevent and address all types of gender-based violence and discrimination made possible by AI.³⁸ Furthermore, it highlights the importance of advancing gender mainstreaming in AI development by endorsing laws that expand women's and girls' access to STEM leadership, education, and employment.³⁹ The Resolution also calls for legislative measures to prevent the creation and spread of deep fake intimate images—mostly targeting women and girls—as well as other AI-generated content that incites hate speech or gender-based violence.⁴⁰

The IPU Resolution also highlights the significance of inclusive growth and diversity in AI governance⁴¹, acknowledging that greater knowledge and comprehension of AI are crucial for informed decision-making.⁴² It emphasizes a balanced, inclusive, and risk-oriented strategy for AI governance to ensure a fair, sustainable, and secure future for everyone, while recognizing that AI systems may exacerbate existing social biases and inequalities within and among nations⁴³, particularly affecting vulnerable populations such as women, children, and individuals with disabilities.⁴⁴

Improved global cooperation has been emphasized among various stakeholders to optimize AI advantages and diminish technological

³⁴ IPU. (2024) *op. cit.* Preamble, clause 3-4.

³⁵ IPU. (2024) *op. cit.* Preamble, clause 8-10.

³⁶ IPU. (2024) *op. cit.* points 2, 7, 8, and 10.

³⁷ IPU. (2024) *op. cit.* point 2.

³⁸ IPU. (2024) *op. cit.* point 7.

³⁹ IPU. (2024) *op. cit.* point 8.

⁴⁰ IPU. (2024) *op. cit.* point 10.

⁴¹ IPU. (2024) *op. cit.* Preamble, clause 7.

⁴² IPU. (2024) *op. cit.* Preamble, clause 3.

⁴³ IPU. (2024) *op. cit.* Preamble, clause 6.

⁴⁴ IPU. (2024) *op. cit.* Preamble, clause 4.

inequalities worldwide,⁴⁵ with immediate actions needed to close digital gaps—including those related to gender—and ensure fair access to AI (§2). It emphasizes the equal involvement of all nations, especially the Global South, in discussions and frameworks regarding AI governance to guarantee the inclusion of diverse perspectives.⁴⁶ Parliaments are called to address discrimination ingrained in AI training data and algorithms (§9) and to support AI systems that maintain linguistic and cultural diversity by integrating multilingualism during AI development.⁴⁷ Strengthening parliamentary capacity through training, specialized bodies, and collaborative platforms is emphasized to keep pace with rapid AI advancements.⁴⁸ Finally, the IPU Resolution opposes international data decoupling to prevent censorship and encourage culturally open, inclusive, and sophisticated AI systems globally.⁴⁹

Responsibly developed and widely accessible AI technologies can positively strengthen democracy by enhancing the transparency and accountability of public institutions and encouraging citizen participation in political processes.⁵⁰ In point 5, the IPU Resolution advocates for legal structures that require transparency and information sharing in AI usage, hold both public and private entities responsible, and provide remedies for those whose rights are infringed by AI. Additionally, point §22 advocates for the creation of standards that mandate companies to reveal their data utilization and decision-making methods to enhance transparency and accountability in AI implementation.

The impact of AI advances on democracy, human rights, and the rule of law has been also highlighted by facilitating misinformation and disinformation that undermine democratic institutions, incite extremism, and violate privacy and data ownership, disproportionately affecting vulnerable groups such as children, women, girls, and disabled persons.⁵¹ It emphasizes the need for creating tools to authenticate AI-generated content, safeguard data privacy, and avoid the misuse of personal information.⁵² Legislatures are called upon to confront privacy breaches caused by AI-driven surveillance and biometric systems employed in unjust political scrutiny, jeopardizing constitutional rights and undermining democracy.⁵³ The IPU Resolution

⁴⁵ IPU. (2024) *op. cit.* point 1.

⁴⁶ IPU. (2024) *op. cit.* point 3.

⁴⁷ IPU. (2024) *op. cit.* point 12.

⁴⁸ IPU. (2024) *op. cit.* point 14.

⁴⁹ IPU. (2024) *op. cit.* point 19.

⁵⁰ IPU. (2024) *op. cit.* Preamble, §5.

⁵¹ IPU. (2024) *op. cit.* Preamble, §4.

⁵² IPU. (2024) *op. cit.* point 11.

⁵³ IPU. (2024) *op. cit.* point 18.

further opposes international data decoupling to prevent censorship and encourage inclusive, culturally aware AI,⁵⁴ and requests defined AI cybersecurity standards to safeguard systems and sensitive information from cyber threats.⁵⁵

The IPU Resolution emphasizes that a deep understanding of AI is essential for informed debate and decision-making, advocating for a balanced, inclusive, and risk-based governance approach to ensure an open, sustainable, fair, free, and secure future for all.⁵⁶ In line with this, it urges parliaments to prioritize AI-related discussions and adapt policies continuously to keep pace with technological advances, ensuring these policies promote human well-being and sustainable development.⁵⁷ It also emphasizes promoting sustainable AI research and innovation aimed at tackling global issues like the protection of human rights, prevention of epidemics, public health improvement, education, and climate change reduction.⁵⁸

3.3. MEANS TO ACHIEVE THE OBJECTIVES OF THE IPU RESOLUTION

The IPU Resolution recommends three means to achieve its objectives: (1) international collaboration, (2) education and awareness raising, (3) independent research.

The IPU Resolution calls for⁵⁹ an inclusive, human-centric, and evidence-based approach to AI governance that ensures fair outcomes worldwide, especially for the Global South facing unique challenges.⁶⁰ It highlights concerns about the lack of comprehensive global AI regulations and the slow pace of developing transparent, democratic frameworks.⁶¹ The IPU Resolution acknowledges ongoing international efforts to create ethical AI standards through multi-stakeholder collaboration,⁶² and welcomes key international organizations for helping parliamentarians develop effective AI policies.⁶³

Parliaments are encouraged to enhance their ability to react proactively to swift AI advancements via training, dedicated entities, innovative

⁵⁴ IPU. (2024) *op. cit.* point 19.

⁵⁵ IPU. (2024) *op. cit.* point 23.

⁵⁶ IPU. (2024) *op. cit.* Preamble, §3.

⁵⁷ IPU. (2024) *op. cit.* point 13.

⁵⁸ IPU. (2024) *op. cit.* point 21.

⁵⁹ IPU. (2024) *op. cit.* Preamble, clause 7, 10, 14, 15.

⁶⁰ IPU. (2024) *op. cit.* Preamble, clause 7.

⁶¹ IPU. (2024) *op. cit.* Preamble, clause 10.

⁶² IPU. (2024) *op. cit.* Preamble, clause 14.

⁶³ IPU. (2024) *op. cit.* Preamble, clause 15.

discussions, and sharing knowledge between parliaments. The IPU is requested to assist in incorporating parliamentary perspectives into AI processes at multilateral entities,⁶⁴ while both parliaments and the IPU are urged to emphasize responsible AI growth and implementation via capacity-building and participation in global efforts.⁶⁵

The necessity of education and awareness has been acknowledged⁶⁶ regarding the risks of bias present in AI, disparities in access to AI systems, and its role in enabling the dissemination of misinformation, to foster informed discussion and decision-making on AI governance initiatives.⁶⁷ Legislative bodies have been also urged to advance gender integration in AI development by fostering girls' and women's participation in STEM education and leadership positions.⁶⁸ Parliaments are encouraged to enhance their ability to react proactively to swift AI advancements by providing training for parliament members and staff.⁶⁹ Legislators need ongoing education and skill development regarding AI risks and applications to stay aligned with technological advancements.⁷⁰ Ultimately, the IPU Resolution encourages directing AI research and development towards tackling worldwide issues like public health, education, and climate change.⁷¹

Finally, the need for independent research on the effects of AI guided by high ethical standards has been also highlighted.⁷²

⁶⁴ IPU. (2024) *op. cit.* point 24.

⁶⁵ IPU. (2024) *op. cit.* point 24.

⁶⁶ IPU. (2024) *op. cit.* Preamble, clause 3.

⁶⁷ IPU. (2024) *op. cit.* Preamble, clause 3.

⁶⁸ IPU. (2024) *op. cit.* point 8.

⁶⁹ IPU. (2024) *op. cit.* point 14.

⁷⁰ IPU. (2024) *op. cit.* point 17.

⁷¹ IPU. (2024) *op. cit.* point 21.

⁷² IPU. (2024) *op. cit.* point 20.

Objective, mean or feature of the IPU Resolution	Preambulatory clauses of the IPU Resolution	Points of the IPU Resolution
Strong global standards and frameworks	6., 10., 11., 13.	4., 6.
Gender equality	3., 4., 7., 8.	2., 7., 8., 10.
Inclusive development and diversity	3., 4., 6., 7.	1., 2., 3., 9., 12., 14., 19.
Transparent and accountable AI development	5.	5., 22.
Personal data and privacy	4.	11., 18., 19., 23.
Sustainability	3.	13., 21.
International cooperation	7., 10., 14., 15.	1., 2., 14., 24., 25.
Education and awareness	3.	8., 14., 15., 16., 17., 21.
Independent research		20.

Table 1: Summary table of the IPU Resolution's connection between preambulatory clauses and Resolution points regarding different aims, features and means of the recommended legal framework. Source: Author based on the IPU Resolution

3.4. THE IPU GUIDELINES FOR AI IN PARLIAMENTS

Following the adoption of the IPU Resolution, IPU has also introduced its Guidelines for parliaments on the implementation of AI. The guidelines is meant to offer a comprehensive framework for parliaments to understand and implement AI responsibly and effectively. The Guidelines cover key areas, including the potential role of AI in parliaments, related risks and challenges, suggested governance structures and AI strategy, ethical principles and risk management, training and capacity-building, and how to manage a portfolio of AI projects across parliament. They are complemented by a set of use cases, shared by parliaments, that describe how AI can support specific parliamentary actions.⁷³ The Guidelines stress the importance of a measured, risk-based approach to AI adoption and provide recommendations for both members of parliament and parliamentary staff, designed to support parliaments of all sizes and levels of digital maturity.

The recommendations include the following:⁷⁴ start with small pilot projects to build experience; focus on use cases with clear benefits and manageable risks; ensure robust human oversight of AI systems; prioritize transparency and accountability; invest in data and AI literacy across the organization; engage with diverse stakeholders throughout the process.

⁷³ Inter-Parliamentary Union. (2024) *Guidelines for AI in parliaments*. [online] Available from: www.ipu.org/AIguidelines

⁷⁴ Inter-Parliamentary Union. (2024) *op. cit.*, p. 6.

4. THE ANALYSIS OF THE EUROPEAN USE CASES

After having outlined the most important soft law instruments covering parliamentary AI-based applications, in the next step of the research, the most important European use cases will be investigated.

4.1. ESTONIA

In Estonia, the question of parliamentary AI arose in the context of a comprehensive modernization program affecting all segments of the public sector.⁷⁵ In the Baltic country, more emphasis was placed on technological developments after democratization, when it was necessary to create a functioning public administrative system without practically existing traditions. Later, as a result of, primarily Russian, cyber attacks and influence operations, efforts to secure the digitized platforms were intensified, so that today they form a fairly closed system. The fact that we are talking about a country with a small population, where the digital competencies of the citizens are generally very high, further helped the rise of new software.

Many legends have spread about Estonian technological developments, but now it seems clear that we can actually talk about a series of very well-thought-out and rational decisions. Estonia currently does not attempt to fundamentally reconsider the relationship between man and technology, instead we can talk about the implementation of innovative ideas with the help of technological tools. If these ideas prove to be successful, they can make the work of the human actors involved easier in the future.⁷⁶ Numerous AI-based softwares are being developed which aim to make our lives easier within existing structures. However, the goal is not to completely replace human cooperation in certain areas.

The key to Estonia's technological competitiveness can also be found in the fact that the source code of all software used in the public sector or currently being developed for such a purpose is publicly available.⁷⁷ Such applications focus on the automation and digitization of the most diverse areas of public administration, from the preparation of minutes of court hearings through the anonymization of documents to the drafting of decisions imposing fines for speeding. It is only one aspect of this

⁷⁵ Etscheid, J. von Lucke, J. and Stroth, F. (2020) *Künstliche Intelligenz in der öffentlichen Verwaltung*. [online], Fraunhofer IAO: Stuttgart, Available from: <https://publica-rest.fraunhofer.de/server/api/core/bitstreams/d3d9f520-1fd4-4516-98d6-a3370c134155/content>

⁷⁶ Mandri, J. M. (2019) *Judges Are Robotics: The State Is Looking for Ways to Implement Artificial Intelligence in the Judiciary* [online] Available from: <https://forte.delfi.ee/artikkel/85777829/kohtunikud-saavad-robotabilised-riik-otsib-voimalusi-kohtususteemis-tehisintellekti-rakendamiseks>

⁷⁷ Kratid. (2022) *AI Kasutuslood*. [online] Available from: <https://www.kratid.ee/kasutuslood-kratid> [Accessed 26 Jun. 2025].

large-scale modernization program that certain results can also be applied to parliamentary relations.

In the public service, applications marked with the concept of "kratt" borrowed from ancient Estonian mythology (figures roughly corresponding to the character of the elf known to us) are used. Every single piece of software belonging to the "kratt" circle has been developed or is being developed in Estonia. Platforms of any foreign company have not been used, although such Estonian endeavours obviously draw on proven solutions elsewhere.⁷⁸ In this way, Estonian data may not fall into foreign hands through the software operators and thereby increasing cybersecurity in accordance with Art. 23 of the IPU Resolution. Moreover, the promotion of domestic technological developments is consistently seen as a driving force for innovation. Technological advancements are primarily financed by the state, while the importance of private investors has remained secondary. The country has also implemented comprehensive reforms to increase AI skills and competencies, including technology curriculums in schools and AI training courses for public sector managers in accordance with Art. 17 of the IPU Resolution, as seen in Table 2 below.

A parliamentary application named Hans, which came to prominence after the abolition of the training of parliamentary stenographers, is among the Kratts, which can prepare the minutes of plenary and committee meetings with the help of AI. Human supervision is currently indispensable, although a long-term goal is to prepare automated summaries with the involvement of generative AI.⁷⁹ The continuous training of the Hans system over many years led to a spectacular result: the device is now able to recognize all members of parliament and members of the government, and its error rate has also been significantly reduced. In the first stage of its training, the software made 40% incorrect notes from the meetings, but now the human employees who provide supervision only have to overwrite 5% of what Hans recorded.⁸⁰ While AI systems like Hans have improved efficiency, there is still a significant need for human supervision and editing of AI-generated content. Seeing the results of the parliamentary implementation, several other public administration bodies, such as the Tallinn Municipality, showed interest in using a similar application.

⁷⁸ Supreme Court of Estonia. (2024) *Artificial Intelligence: A Substitute or Supporter of Judges?* - *Yearbook of Estonian Courts* [online] Available from: <https://aastaraamat.riigikohus.ee/en/artificial-intelligence-a-substitute-or-supporter-of-judges/> [Accessed 22 Jun. 2025].

⁷⁹ Baptista, J. et al. (2020) *op. cit.* pp. 1-10

⁸⁰ Inter-Parliamentary Union. (2023) *A view from Estonia: AI for advanced beginners.* [online] Available from: <https://www.ipu.org/innovation-tracker/story/view-estonia-ai-advanced-beginners> [Accessed 26 June. 2025].

Another kratt provides legal advice to members of parliament, as well as one that simultaneously subtitles parliamentary speeches, thereby significantly facilitating the situation of hearing-impaired citizens. The parliament is actively exploring new AI applications, indicating ongoing education and capacity-building efforts, in compliance with Art. 17 of the IPU Resolution.⁸¹ As AI systems become more integrated into parliamentary work, ensuring transparency in algorithmic decision-making processes will be crucial. In conclusion, the Estonian Parliament appears to be at the forefront of responsible AI adoption in parliamentary operations, largely aligning with the key principles outlined in the IPU Resolution.

4.2. ITALY

In addition to Estonia, Italy is the other leading example in Europe in the parliamentary application of AI and compliance to the IPU Resolution. Both houses of the bicameral legislature, the Chamber of Deputies and the Senate, are open to these tools and made significant progress in three respects.

First, the Italian Parliament has at its disposal the Gestore Emendamenti, which, with the involvement of AI, is able to connect similar amendment proposals, thereby influencing the parliamentary agenda and increasing its efficiency. Italian opposition parties tend to submit to the legislature a large number of amendments with almost identical wording, which shall discuss each of them separately, losing considerable time. However, the new tool is capable of filtering out textual similarities, and based on this, connecting essentially identical amendment proposals, which can then be decided by the parliament with a joint single vote, or even together. Another goal is for the software to be able to recognize semantic similarities, so that in addition to literal matching, the analysis and filtering of amendment proposals could become even more effective by taking the context into account.⁸² However, the reports of the software are currently subject to human supervision. The AI's proposal will only become followable for the legislature if it is approved by a human contributor.

The other possibility of application is related to the minutes of the parliamentary sessions: both houses of the Italian legislature have software that organizes thematically related minutes, so that the related parliamentary discourses become easier to follow.

⁸¹ Nortal. (2024) *How AI accelerates the legislative power of the Parliament of Estonia*. [online] Available from: <https://nortal.com/insights/how-ai-accelerates-the-legislative-power-of-the-parliament-of-estonia/> [Accessed 26 June. 2025].

⁸² Inter-Parliamentary Union. (2022) *How AI helps the Italian Senate manage amendments*. [online] Available from: <https://www.ipu.org/innovation-tracker/story/how-ai-helps-italian-senate-manage-amendments> [Accessed 26 June. 2025].

Thirdly, the chatbot applications operated by both chambers should be highlighted, which use generative AI to answer the frequently repeated questions of those interested in the legislative process,⁸³ thereby speeding up the flow of information and reducing the workload of the parliamentary apparatus.⁸⁴ In addition, to support the legislative process, the Italian Chamber of Deputies has tasked the University of Bologna in creating a generative AI tool called GENAI4LEX-B, with the aim to assist parliamentarians in the drafting of bills. The tool under development could be used to automate various tasks of legal research and bill drafting, such as the identification of relevant legal documents and the summarisation of committee amendments.⁸⁵

Besides this, the draft law on artificial intelligence, currently under parliamentary review provides that the implementation of AI should undermine the integrity of the democratic processes.⁸⁶

⁸³ Citino, Y.M. (2024) Leveraging automated technologies for law-making in Italy: Generative AI and constitutional challenges. *Parliamentary Affairs*. Available from: <https://doi.org/10.1093/pa/gsae040>.

⁸⁴ Androutsopoulou, A. et al. (2019) Transforming the communication between citizens and government through AI-guided chatbots. *Government Information Quarterly*, 36(2). Available from: <https://doi.org/10.1016/j.giq.2018.10.001>. pp.358–367.

⁸⁵ Public Sector Tech Watch. (2025) *GENAI4LEX-B: AI-powered legislative support in the Italian Chamber of Deputies*. [online] Available from: <https://interoperable-europe.ec.europa.eu/collection/public-sector-tech-watch/genai4lex-b-ai-powered-legislative-support-italian-chamber-deputies> [Accessed 26 Jun. 2025].

⁸⁶ Italian Senate. (2025) *Disegno di legge S. 1146 - 19^a Legislatura*. [online], Available from: <https://www.senato.it/leg/19/BGT/Schede/Ddliter/58262.htm>

4.3. PORTUGAL

As a recent development, the National Assembly of Portugal has introduced the Staar system, which operates with automated speech recognition (ASR) and is capable of drafting reports from parliamentary meetings.⁸⁷ The Staar system can transcribe pre-written, well-articulated speeches with a correction rate of 1.7%. However, during more spontaneous and excited debates, 11% rate of imprecise transcripts have been experienced.⁸⁸ Plenary sittings have produced better results compared to committee meetings, which were not documented before the implementation of the Staar system.⁸⁹ The Staar system has been trained to correct most mistakes without human supervision. Additionally, its resilience against external voices, disturbances, and different speech qualities has been improved. The functioning of Staar has exceeded expectations, and its extension is currently underway. However, there is limited information on specific transparency measures, accountability frameworks, or capacity-building for AI use in parliamentary operations, thus more targeted efforts may be needed to fully align with the IPU Resolution's recommendations, as seen in Table 2 below. The Portuguese endeavours shall be interpreted as part of a broader legislative package, which began with the enactment of the Portuguese Charter of Human Rights in the Digital Age.⁹⁰

⁸⁷ Nascimento, P. et al. (2024) Automatic transcription system for parliamentary debates in the context of assembly of the republic of Portugal. *International Journal of Speech Technology*, 27, pp. 613–635.

⁸⁸ Granja P. (2023) The Portuguese Parliamentary Reporters' Experience with Automated Speech Recognition Systems. *The Journal of Professional Reporting and Transcription*, 2/2023. Available from: <https://tiro.intersteno.org/2023/12/the-portuguese-parliamentary-reporters-experience-with-automatic-speech-recognition-systems/> [Accessed 30 Jun. 2025]

⁸⁹ Aguiar De Lima, T. and Da Costa-Abreu, M. (2020) A survey on automatic speech recognition systems for Portuguese language and its variations, *Computer Speech & Language*, 62, Available from: <https://doi.org/10.1016/j.csl.2019.101055>. p. 101-155.

⁹⁰ Law no. 17/2021, *On the Portuguese Charter of Human Rights in the Digital Age*, Portuguese Republic. In: Portuguese

4.4. SPAIN

Although the fact, that the Spanish draft law on AI does not explicitly cover the parliamentary application of AI,⁹¹ in the autumn of 2024, the Spanish Congress of Deputies decided to award the right to develop its AI-based ASR system to Pangeanic, a company based in Valencia.⁹² The planned implementation of the new software could also facilitate the live translation of parliamentary debates between the various languages and dialects of the country. Therefore, such a reform could significantly improve access to political discourse by better involving ethnic minorities, in accordance with Art. 12 of the IPU Resolution. Pangeanic has already successfully introduced an AI-based ASR system in the legislative body of the Valencian Community. Furthermore, experiments have also taken place to develop software that provides bilingual Spanish-Basque transcripts from the sessions of the Basque Regional Parliament.⁹³

4.5. THE EUROPEAN PARLIAMENT

The EP primarily turned to the help of AI to popularize its history. A significant part of the archive was digitized by the background apparatus, and now involving generative AI, the Archives Unity Dashboard application was developed. It is built from the digitized elements of the EP's archive, which has been expanding since 1952.⁹⁴ The tool can provide answers to the questions of interested parties, selecting from more than 100,000 documents based on keywords. It then interprets the selected documents and formulates an understandable and concise answer based on this. In addition, the application is available in all official languages of the EU, and can translate documents that were originally mostly in French into the other 27 languages, in accordance with EU treaties and Art. 12 of the IPU Resolution, as seen in Table 2 below.⁹⁵

⁹¹ Cuatrecasas. (2025) *El Anteproyecto de Ley desarrolla el sistema de infracciones y sanciones de acuerdo con el Reglamento de IA*. [online] Available from: <https://www.cuatrecasas.com/es/spain/propiedad-intelectual/art/anteproyecto-ley-buen-uso-gobernanza-ia>

⁹² Pangeanic Blog. (2024) *Pangeanic to implement AI transcription technology in Spanish Parliament*. [blog entry] 27 November. Valencia: Pangeanic. Available from: <https://blog.pangeanic.com/pangeanic-will-implement-ai-transcription-technology-in-spanish-parliament> [Accessed 30 June 2025].

⁹³ Penagarikano, M. et al. (2023) Semisupervised Speech Data Extraction from Basque Parliament Sessions and Validation on Fully Bilingual Basque-Spanish ASR, *Applied Sciences*, 13(14), Available from: <https://doi.org/10.3390/app13148492>. pp. 84–92.

⁹⁴ Anthropic. (2024) *European Parliament expands access to their archives with Claude*. [blog entry] Available from: <https://www.anthropic.com/customers/european-parliament> [Accessed 22 June 2025].

⁹⁵ European Parliament. (2024) *The EP Archives Unit Launches its first Generative AI tool*. [blog entry] Available from: <https://historicalarchives.europarl.europa.eu/en/s>

Apart from the chatbot, the EP is also developing ASR for preparing reports from parliamentary debates.⁹⁶

Country	Use Cases	Gen-AI	Human Involvement	Opportunities	Risks
Estonia	- Preparing minutes and live subtitling - Legal advice for MPs	No	Required	Improved accessibility of parliamentary information	Inaccurate minutes or legal advice
Italy	- Filtering out similar amendment proposals - Organization of thematic minutes - Chatbots for answering legislative process questions	Yes	Required	Increased efficiency in handling amendments and minutes	Misrepresenting amendments
Portugal	Drafting reports from parliamentary meetings	No	Required	Improved documentation	Inaccurate summaries
Spain	Transcription and translation	No	Not specified	Improved access to parliamentary debates	Inaccurate translations
European Parliament	- Searching historical documents - Translation of documents - Developing ASR for debate reports	Yes	Not specified	- Improved accessibility of historical documents - Enhanced multilingual capabilities	Inaccurate translations and information

Table 2: The integration of AI in the operation of European parliamentary institutions

ites/historicalarchive/home/cultural-heritage-collections/news/ai-dashboard.html [Accessed 22 June 2025].

⁹⁶ de Vos, H. and Verberne, S. (2020) Challenges of Applying Automatic Speech Recognition for Transcribing EU Parliament Committee Meetings: A Pilot Study. In: Fišer, D. Eskevich, M. and de Jong, F. (eds.) *Proceedings of the Second ParlaCLARIN Workshop*. Marseille, France: European Language Resources Association, Available from: <https://aclanthology.org/2020.parlaclarin-1.8/> [Accessed: 30 June 2025]. pp. 40–43; Diaz, K. (2023) *Lawmakers Experiment With ChatGPT to Write Bills*. [blog entry] Governing. Available from: <https://www.governing.com/next/lawmakers-experiment-with-chatgpt-to-write-bills> [Accessed 22 June 2025].

4.6. PARLIAMENTS SERIOUSLY CONSIDERING THE IMPLEMENTATION OF AI: FINLAND, GREECE, LATVIA, LITHUANIA, NORWAY AND THE UNITED KINGDOM

In Greece, the parliamentary staff has already organized several workshops on the perspectives of AI,⁹⁷ which coincides with the government's visionary plans for exploiting technological opportunities.

The Finnish legislature is also dealing with the possibilities of exploiting new technology: the Committee for the Future has already dealt with AI in several hearings.⁹⁸ The idea that AI-based software could prepare summaries of parliamentary sessions has also come up.⁹⁹ It is no coincidence that in the fall of 2022, Helsinki hosted the first international congress on future parliaments.¹⁰⁰

The UK Parliament has also experiments to develop a chatbot supporting the work of parliamentarians,¹⁰¹ while the Norwegian Stortinget has also been actively exploring and implementing AI-based technologies to enhance its operations. A key initiative in this regard is the StorSak project, which aims to implement an information system for handling document production and parliamentary proceedings in a coherent digital value chain. This project focuses on exploring machine learning and AI applications, particularly in areas such as metadata handling and document categorization.¹⁰² In addition, the Stortinget has been experimenting with ASR in 2025 to transcribe speeches in Norwegian languages Bokmål or Nynorsk, according to the individual preferences of MPs, and create the minutes

⁹⁷ Lucke J. and Fitsilis F. (2023) Using Artificial Intelligence in Parliament - The Hellenic Case. in: Lindgren, I. et al. (eds.) *Electronic Government - EGOV 2023. Lecture Notes in Computer Science*, 2023/14130. Available from: https://doi.org/10.1007/978-3-031-41138-0_12

⁹⁸ Žagar, A.P. (2024) *Exploring parliamentary AI debates with computational text analysis*. [blog entry] University of Helsinki. Available from: <https://www.helsinki.fi/en/researchgroups/reimagining-public-values-in-algorithmic-futures/whats-new/exploring-parliamentary-ai-debates-with-computational-text-analysis> [Accessed 30 Jun. 2025].

⁹⁹ Fitsilis, F. (2021) Artificial Intelligence (Ai) in parliaments – preliminary analysis of the Eduskunta experiment, *The Journal of Legislative Studies*, 27(4), Available from: <https://doi.org/10.1080/13572334.2021.1976947>. pp. 621–633.

¹⁰⁰ Eduskunta. (2022). *The World Summit of the Committees of the Future 12–13 October 2022*. [blog entry] Available from: <https://www.eduskunta.fi/world-summit-committees-future> [Accessed 22 Jun. 2025].

¹⁰¹ Brown F. (2024) *The right honourable chatbot? How MPs are considering using AI*. [online] Sky News. 1 December, Available from: <https://news.sky.com/story/the-right-honourable-chatbot-how-mps-are-considering-using-ai-13262273> [Accessed 22 Jun. 2025].

¹⁰² Wahl, T. (2024) The Rise of Data and ai in Parliamentary Proceedings – The Norwegian Parliament, Stortinget. *International Journal of Parliamentary Studies* 4, 1. Available From: <https://doi.org/10.1163/26668912-bja10080> [Accessed 30 June 2025], pp. 79–87.

of parliamentary sessions.¹⁰³ To support Norwegian ASR developments related to parliamentary use and research, in 2019 the Norwegian Language Bank at the National Library of Norway started compiling the Norwegian Parliamentary Speech Corpus (NPSC),¹⁰⁴ a speech dataset with over 140 hours of audio recordings of meetings at the Stortinget.¹⁰⁵ Researchers of the National Library of Norway continue to work on improving ASR models for both Bokmål and Nynorsk, generating increasingly large and comprehensive audio datasets of parliamentary debates.¹⁰⁶

The Lithuanian Seimas has focused on exploring ethical uses and experimenting with smaller initiatives, such as an in-house custom neural machine translation system for Russian and English.¹⁰⁷ To assess the possibilities of AI implementation in public services, including parliamentary operation, the Seimas has established a Working Group on AI within its Committee on the Future at the end of 2023. Thanks to the initiative of the Working Group, in May 2024 the Seimas adopted a resolution on the principles of use of AI technologies in the public sector, outlining 11 principles to adhere to.¹⁰⁸ The Working Group has also proposed a change to the Seimas Statue, that would establish a clear and direct responsibility for the politicians when they use AI-based technologies during their work, for example drafting speeches and legislation. The aim is to enhance

¹⁰³ Norwegian Board of Technology. (2024). *Norway In European Parliamentary Technology Assessment Network: Artificial Intelligence and Democracy 2024 Report*. [online] Available from: <https://eptanetwork.org/news/epta-news/24-publication/140-epta-report-2024> [Accessed 30 Jun. 2025]; Botheim, S. S. (2022) *The Storting is considering big technology*. [online] Språkrådet. Available from: <https://sprakradet.no/aktuelt/stortinget-tingar-stor-teknologi/> [Accessed 30 Jun. 2025].

¹⁰⁴ Solberg, P. E. and Ortiz, P. (2022) The Norwegian Parliamentary Speech Corpus. In: Calzolari, N. et al. (eds.) *Proceedings of the Thirteenth Language Resources and Evaluation Conference*. Marseille, France: European Language Resources Association. Available from: <https://aclanthology.org/2022.lrec-1.106/> [Accessed 30 Jun. 2025]. pp. 1003–1008.

¹⁰⁵ National Library of Norway. (2023). *Norwegian Parliamentary Speech Corpus 2.0*. [online] Available from: <https://www.nb.no/sprakbanken/en/resource-catalogue/oai-nb-no-sbr-84/> [Accessed 30 Jun. 2025].

¹⁰⁶ Solberg, P. E. and Ortiz, P. (2022) *op. cit.*

¹⁰⁷ Tilde. (2020) *Custom neural machine translation engines help Seimas translators to significantly boost their productivity and efficiency*. [blog entry] Tilde.ai, 23 March. Available from: <https://tilde.ai/custom-neural-machine-translation-engines-helps-seimas-translators-to-significantly-boost-their-productivity-and-efficiency/> [Accessed 30 Jun. 2025].

¹⁰⁸ Trembo, S. E. (2024) *In its Resolution, the Seimas has formulated the principles of use of artificial intelligence technologies in the public sector*. [online] Office of the Seimas of the Republic of Lithuania. Available from: https://www.lrs.lt/sip/portals.show?p_r=35403&p_k=2&p_t=288543&p6=25 [Accessed 30 Jun. 2025].

transparency, create a sense of ownership and foster a culture of responsible AI use among politicians.¹⁰⁹

5. DISCUSSION: SOME ARGUMENTS FOR THE NECESSITY OF A NORMATIVE LEGAL FRAMEWORK

The enactment of various soft law instruments and the rapidly emerging number of use cases resonate with the increasing social weight of parliamentary AI, which is strongly connected to the integrity of democratic processes, the protection of fundamental rights, and the significant potential for implementing modern technologies into parliamentary operations¹¹⁰ In our view, the establishment of supranational normative framework rules could provide proper safeguards for the exploitation of parliamentary AI; these could be introduced via two alternative paths.

On the one hand, the EU AI Act may classify AI applications serving internal parliamentary operations in a higher risk category; therefore, the introduction of such tools should be subject to stricter requirements. However, such a solution may hinder the effective implementation of innovative ideas, while the experience of use cases, such as the lower error rate of speech-to-text technologies, underlines the potential enhancement of parliamentary efficiency with the help of AI. On the other hand, a separate European instrument might be enacted, which could underline the framework rules and the fundamental principles to be complied with by parliamentary staff, including those of the EP and national parliaments, when AI-based tools are concerned. The adoption of such a framework regulation should be tailored with extreme carefulness; due regard should be given by the policymakers to at least the following factors.

First of all, the core values and fundamental principles laid down by the available soft law instruments, primarily by the IPU Resolution and the IPU Guidelines, could serve as meaningful points of reference for a foreseen European framework regulation.¹¹¹ Gender disparity, inclusive and accountable AI development, the due protection of personal data and privacy,

¹⁰⁹ Committee for the Future of the Seimas. (2024) Lithuania. In *European Parliamentary Technology Assessment Network: Artificial Intelligence and Democracy 2024 Report*. [online] Oslo: European Parliamentary Technology Assessment (EPTA) Network. Available from: <https://eptanetwork.org/news/epta-news/24-publication/140-epta-report-2024> [Accessed 30 Jun. 2025].

¹¹⁰ Fitsilis, F. von Lucke, J. and De Vrieze, F. (2025) Inception, development and evolution of guidelines for AI in parliaments. *The Theory and Practice of Legislation*. Available from: <https://doi.org/10.1080/20508840.2025.2474791>. pp. 1–24.

¹¹¹ Drahmann, A. and Meuwese, A. (2022) AI and Lawmaking: An Overview. In: Custers, B. and Fosch-Villaronga, E. (eds.) *Law and Artificial Intelligence*. The Hague: T.M.C. Asser Press, Available from: https://doi.org/10.1007/978-94-6265-523-2_22. pp. 433–449.

and the distinguished role of sustainability might be such starting points that could be reflected either in the preamble or in the first section of the envisaged regulation.

Then, a separate section should be devoted to the respect of national sovereignty, since parliaments are among the most important constitutional players of EU member states, representing and expressing national sovereignty. The framework rules should be formulated in such a manner that would exclude influence on the substantial parliamentary work; the proposed legal instrument shall limit itself to the AI-based technical facilities of parliamentary staff. It must be avoided that this regulation interferes with the exclusive competences of national authorities; it would just enumerate some legally enforceable requirements for potential developers and users to be met by parliamentary AI applications. In other words, the proposed European legal instrument should just lay down flexible framework rules determining the main principles and the limits of parliamentary AI applications, however, a broad space of manoeuvre should be left for national parliaments elaborating their own solutions. Furthermore, the European regulation should be strictly restricted to certain aspects of parliamentary operation without influencing under any instance the merits of the legislative process.

Similarly, a separate section should reflect on the distinguished role of parliaments as special businesses with multiple constitutional duties and huge demands for transparency as well as reliability.¹¹² The detailed analysis of the main relevant similarities and differences between parliaments and other potential AI user businesses may provide valuable additional points for the forthcoming regulation.

Apart from this, security concerns shall also be kept at the forefront during the drafting and negotiation process, since parliaments shall work with a huge amount of classified data, including data affecting national security. The involvement of external stakeholders in the development of parliamentary AI applications, or the use of licenses produced by foreign business entities, especially from outside the EU, may also raise considerable security concerns.¹¹³ Besides this, extensive databases of documents, speeches, and images would be needed for the continuous training of parliamentary AI applications; therefore, the unlawful and manipulative use of such content may also generate additional risk factors that should be covered by the

¹¹² Chaudhary, G. (2024) Unveiling the Black Box: Bringing Algorithmic Transparency to AI, *Masaryk University Journal of Law and Technology*, 18(1), Available from: <https://doi.org/10.5817/MUJLT2024-1-4>. pp. 93–122.

¹¹³ Edler, J. et al. (2020) *Technology sovereignty: From demand to concept Perspectives*. [policy brief] Karlsruhe, Fraunhofer Institute for Systems and Innovation Research (ISI).

intended legal framework. The Italian draft artificial intelligence law currently under parliamentary review stipulates that databases of the public administration should be kept on Italian servers.¹¹⁴

As a last key consideration, the boosting of technological innovation in the field of parliamentary operation shall also be highlighted, and the aforementioned crucial arguments for its limitation should be reduced as much as possible.¹¹⁵ The recommended legal framework shall strike a proper balance between the possibility of developing AI-based parliamentary tools and providing reasonable limitations on such endeavors as safeguards.

In our view, the envisaged regulation should be divided into the following parts.

After the preamble laying down the fundamental principles of parliamentary AI application, the scope of the regulation should be described. It should cover parliamentary speech-to-text applications; face recognition systems;¹¹⁶ parliamentary chatbots;¹¹⁷ AI-based tools reviewing and researching voluminous parliamentary documentation; and parliamentary platforms for citizen participation.¹¹⁸ The second section may focus on the specificities of parliaments as businesses, while the third part would provide meaningful safeguards for the protection of national sovereignty during the implementation of this regulation.

The fourth section should give special weight to the protection of fundamental rights when AI-based tools are involved in parliamentary operations.¹¹⁹ Among others, the protection of personal data; the right to

¹¹⁴ Italian Senate. (2025) *Disegno di legge S. 1146 - 19^a Legislatura*. [online], Available from: <https://www.senato.it/leg/19/BGT/Schede/Ddliter/58262.htm>

¹¹⁵ Ganzevles, J. Van Est, R. and Nentwich, M. (2014) Embracing variety: introducing the inclusive modelling of (Parliamentary) technology assessment. *Journal of Responsible Innovation*, 1(3), Available from: <https://doi.org/10.1080/23299460.2014.968439>. pp. 292–313.

¹¹⁶ Kuhlmann, S. (2024) Government Use of Facial Recognition Technologies under European Law. In: Matulionyte, R. and Zalnieriute, M. (eds.) *The Cambridge Handbook of Facial Recognition in the Modern State*. Cambridge: Cambridge University Press (Cambridge Law Handbooks), pp. 127–138.

¹¹⁷ Necz, D. (2024) Rules over words: Regulation of chatbots in the legal market and ethical considerations. *Hungarian Journal of Legal Studies*, 64(3), Available from: <https://doi.org/10.1556/2052.2023.00472>. pp. 472–485.

¹¹⁸ Fitsilis, F. von Lucke, J. and Frank, S. (2023). A Comprehensive Research Workshop on Artificial Intelligence in Parliaments. *International Journal of Parliamentary Studies*, 3, 2, Available From: <https://doi.org/10.1163/26668912-bja10074> [Accessed 30 June 2025]. pp. 316–324; Savaget, P. Chiarini, T. and Evans, S. (2019) Empowering political participation through artificial intelligence. *Science and Public Policy*, 46(3), Available from: <https://doi.org/10.1093/scipol/scy064>. pp. 369–380.

¹¹⁹ Donahoe, E. and Metzger, M. M. (2019) Artificial Intelligence and Human Rights. *Journal of Democracy*, 30(2), Available from: <https://muse.jhu.edu/pub/1/article/721650> [Accessed: 30 June 2025]. pp. 115–126.

privacy; the right to freedom of expression; the right to non-discrimination; the right to equality; the rights of disabled persons; and the rights of future generations should be explicitly mentioned by the proposed legal framework.¹²⁰

In case of fundamental rights violations caused by AI-based parliamentary tools, special remedies should be established for those who are concerned. These remedies could be provided by the national authorities; the European legal framework shall oblige the member states relying on parliamentary AI tools to secure accessible and effective remedies for all citizens interacting with these technologies.

The proposed legal regulation shall provide in a separate section that parliaments would be responsible for raising the awareness of parliamentarians, parliamentary staff, and the general public interacting with AI-based parliamentary tools. For this purpose, education should be provided, while various materials should help spread reliable information on AI-based parliamentary tools.

The proposed legal instrument shall tackle security concerns with detailed rules; these should cover cybersecurity safeguards,¹²¹ the protection of data classified on national security grounds, the combat against disinformation,¹²² and the involvement of private stakeholders as well as foreign collaborators in the development of parliamentary AI applications.¹²³ Potential collaborators arriving from outside the EU shall face additional requirements when they are involved in this field.¹²⁴

Finally, the regulation may establish paths for the exchange of best practices and know-how in Europe and beyond, and how AI-based technologies could serve most efficiently in the daily operation of these special entities.¹²⁵

¹²⁰ Lee, J. (2020) Artificial Intelligence and Human Rights: Four Realms of Discussion: Summary of Remarks. *Proceedings of the ASIL Annual Meeting*, 114. Available from: <https://doi.org/10.1017/amp.2021.47>. pp. 242–245.

¹²¹ Barrinha, A. and Christou, G. (2022) Speaking sovereignty: the EU in the cyber domain. *European Security*, 31(3), Available from: <https://doi.org/10.1080/09662839.2022.2102895>. pp. 356–376.

¹²² Kertysova, K. (2018) Artificial Intelligence and Disinformation: How AI Changes the Way Disinformation is Produced, Disseminated, and Can Be Countered. *Security and Human Rights*, 29, 1-4, 55-81, Available From: <https://doi.org/10.1163/18750230-02901005> [Accessed 30 June 2025]. pp. 55-81

¹²³ Mügge, D. (2023) The securitization of the EU's digital tech regulation. *Journal of European Public Policy* 30(7), Available from: <https://doi.org/10.1080/13501763.2023.2171090>. pp. 1431–1446.

¹²⁴ Varju, M. (2022) The Protection of Technology Sovereignty in the EU: Policy, Powers and the Legal Reality. *European Law Review*, 47(4), pp. 568-583.

¹²⁵ Fitsilis, F. and Lucke, V. J. (2023) Re-shaping Interparliamentary Cooperation Through Advanced Information Sharing. *Australasian Parliamentary Review*, 38(1), pp. 78-88.

6. CONCLUSIONS

Given the rapidly emerging parliamentary AI applications across Europe, this contribution argued for the necessity of an explicit normative legal framework for the inclusion of AI in the daily operation of parliaments. Since we are in Europe in the period of establishing normative legal regulation on AI-based technologies, this may be the proper moment to extend these endeavors into the field of parliamentary exploitation.

Since we discuss a rapidly emerging field, the legal framework should provide the fundamental principles to be complied with; however, a broad margin of movement should be left for national authorities on the grounds of national sovereignty, and also for private stakeholders fostering innovation in this sector.

In this study, we have made a cursory glance at the relevant European soft law instruments and also at the most promising European use cases. Then, the main potential components of a proposed European regulation focusing directly on parliamentary AI involvement have been discussed. As an alternative, the reconsideration of Parliamentary AI's risk classification in the EU AI Act has also been taken into account. These minor steps hopefully bring us closer to the final purpose: a normative legal framework at the European level for the parliamentary involvement of AI-based technologies.

LIST OF REFERENCES

- [1] Agora. (2021) *Brazil Ulysses Machine Learning for Transparency and Citizen Participation*. [online] Available from: <https://www.agora-parl.org/events-and-lectures/brazil-ulysses-machine-learning-transparency-and-citizen-participation> [Accessed 22 June 2025].
- [2] Aguiar De Lima, T. and Da Costa-Abreu, M. (2020) A survey on automatic speech recognition systems for Portuguese language and its variations, *Computer Speech & Language*, 62, Available from: <https://doi.org/10.1016/j.csl.2019.101055>. p. 101-155.
- [3] Androutsopoulou, A. et al. (2019) Transforming the communication between citizens and government through AI-guided chatbots. *Government Information Quarterly*, 36(2). Available from: <https://doi.org/10.1016/j.giq.2018.10.001>. pp.358–367.
- [4] Anthropic. (2024) *European Parliament expands access to their archives with Claude*. [blog entry] Available from: <https://www.anthropic.com/customers/european-parliament> [Accessed 22 June 2025].
- [5] Barber, H. (2025) *Argentina will use AI to 'predict future crimes' but experts worry for citizens' rights*. [online] The Guardian, Available from: <https://www.>

- theguardian.com/world/article/2024/aug/01/argentina-ai-predicting-future-crimes-citizen-rights
- [6] Bareis, J. and Katzenbach, C. (2022) Talking AI into being: The narratives and imaginaries of national AI strategies and their performative politics. *Science, Technology, & Human Values*, 47(5), pp. 855–881.
- [7] Barrinha, A. and Christou, G. (2022) Speaking sovereignty: the EU in the cyber domain. *European Security*, 31(3), Available from: <https://doi.org/10.1080/09662839.2022.2102895>. pp. 356–376.
- [8] Benedetto, I. et al. (2025) Leveraging large language models for abstractive summarization of Italian legal news. *Artificial Intelligence and Law*, 2025, Available from: <https://doi.org/10.1007/s10506-025-09431-3>
- [9] Bex, F. J. (2024) AI, Law and beyond. A transdisciplinary ecosystem for the future of AI & Law. *Artificial Intelligence and Law*, vol. 33, Available from: <https://doi.org/10.1007/s10506-024-09404-y> [Accessed: 22 Jun. 2025]
- [10] Botheim, S. S. (2022) *The Storting is considering big technology*. [online] Språkrådet. Available from: <https://sprakradet.no/aktuelt/stortinget-tingar-stor-teknologi/> [Accessed 30 Jun. 2025]
- [11] Brown F. (2024) *The right honourable chatbot? How MPs are considering using AI*. [online] Sky News. 1 December, Available from: <https://news.sky.com/story/the-right-honourable-chatbot-how-mps-are-considering-using-ai-13262273> [Accessed 22 Jun. 2025]
- [12] Chaudhary, G. (2024) Unveiling the Black Box: Bringing Algorithmic Transparency to AI, *Masaryk University Journal of Law and Technology*, 18(1), Available from: <https://doi.org/10.5817/MUJLT2024-1-4>. pp. 93–122.
- [13] Citino, Y.M. (2024) Leveraging automated technologies for law-making in Italy: Generative AI and constitutional challenges. *Parliamentary Affairs*. Available from: <https://doi.org/10.1093/pa/gsae040>
- [14] Committee for the Future of the Seimas. (2024) Lithuania. In *European Parliamentary Technology Assessment Network: Artificial Intelligence and Democracy 2024 Report*. [online] Oslo: European Parliamentary Technology Assessment (EPTA) Network. Available from: <https://eptanetwork.org/news/epta-news/24-publication/140-epta-report-2024> [Accessed 30 Jun. 2025]
- [15] Council of Europe. (2024) *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*. Vilnius
- [16] de Vos, H. and Verberne, S. (2020) Challenges of Applying Automatic Speech Recognition for Transcribing EU Parliament Committee Meetings: A Pilot

- Study. In: Fišer, D. Eskevich, M. and de Jong, F. (eds.) *Proceedings of the Second ParlaCLARIN Workshop*. Marseille, France: European Language Resources Association, Available from: <https://aclanthology.org/2020.parlaclarin-1.8/> [Accessed: 30 June 2025]
- [17] Dharmaraj, S. (2025). *AI Revolutionising India's Parliamentary Operations – OpenGov Asia*. [online] Available from: <https://opengovasia.com/2025/03/19/ai-revolutionising-indias-parliamentary-operations/> [Accessed 26 Jun. 2025]
- [18] Diaz, K. (2023) *Lawmakers Experiment With ChatGPT to Write Bills*. [blog entry] Governing. Available from: <https://www.governing.com/next/lawmakers-experiment-with-chatgpt-to-write-bills> [Accessed 22 June 2025]
- [19] Donahoe, E. and Metzger, M. M. (2019) Artificial Intelligence and Human Rights. *Journal of Democracy*, 30(2), Available from: <https://muse.jhu.edu/pub/1/article/721650> [Accessed: 30 June 2025]. pp. 115–126.
- [20] Drahmann, A. and Meuwese, A. (2022) AI and Lawmaking: An Overview. In: Custers, B. and Fosch-Villaronga, E. (eds.) *Law and Artificial Intelligence*. The Hague: T.M.C. Asser Press, Available from: https://doi.org/10.1007/978-94-6265-523-2_22. pp. 433–449.
- [21] Edler, J. et al. (2020) *Technology sovereignty: From demand to concept Perspectives*. [policy brief] Karlsruhe, Fraunhofer Institute for Systems and Innovation Research (ISI).
- [22] Eduskunta. (2022). *The World Summit of the Committees of the Future 12–13 October 2022*. [blog entry] Available from: <https://www.eduskunta.fi/world-summit-committees-future> [Accessed 22 Jun. 2025]
- [23] Cuatrecasas. (2025) *El Anteproyecto de Ley desarrolla el sistema de infracciones y sanciones de acuerdo con el Reglamento de IA*. [online] Available from: <https://www.cuatrecasas.com/es/spain/propiedad-intelectual/art/anteproyecto-ley-buen-uso-gobernanza-ia>
- [24] Etscheid, J. von Lucke, J. and Stroh, F. (2020) *Künstliche Intelligenz in der öffentlichen Verwaltung*. [online], Fraunhofer IAO: Stuttgart, Available from: <https://publica-rest.fraunhofer.de/server/api/core/bitstreams/d3d9f520-1fd4-4516-98d6-a3370c134155/content>
- [25] European Parliament resolution of 12 February 2019 on a comprehensive European industrial policy on artificial intelligence and robotics (2018/2088(INI))

- [26] European Parliament resolution of 12 February 2020 on automated decision-making processes: ensuring consumer protection and free movement of goods and services (2019/2915(RSP))
- [27] European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL))
- [28] European Parliament resolution of 19 May 2021 on artificial intelligence in education, culture and the audiovisual sector (2020/2017(INI))
- [29] European Parliament resolution of 20 May 2021 on shaping the digital future of Europe: removing barriers to the functioning of the digital single market and improving the use of AI for European consumers (2020/2216(INI))
- [30] European Parliament resolution of 20 October 2020 on intellectual property rights for the development of artificial intelligence technologies (2020/2015(INI))
- [31] European Parliament resolution of 3 May 2022 on artificial intelligence in a digital age (2020/2266(INI))
- [32] Faranda, A. and Lusardi, G. (2024) *Italian AI bill: Main issues and risks*. [online] Technology's Legal Edge. Available from: <https://www.technologyslegaledge.com/2024/05/italian-ai-bill-main-issues-and-risks/> [Accessed 26 Jun. 2025]
- [33] Feliba, D. (2024) *Reboot of Buenos Aires facial recognition plan fuels privacy fears*. [online], Context News, Available from: <https://www.context.news/surveillance/reboot-of-buenos-aires-facial-recognition-plan-fuels-privacy-fears>
- [34] Fitsilis, F. and Lucke, V. J. (2023) Re-shaping Interparliamentary Cooperation Through Advanced Information Sharing. *Australasian Parliamentary Review*, 38(1), pp. 78-88.
- [35] Fitsilis, F. (2021) Artificial Intelligence (Ai) in parliaments – preliminary analysis of the Eduskunta experiment, *The Journal of Legislative Studies*, 27(4), Available from: <https://doi.org/10.1080/13572334.2021.1976947>. pp. 621–633.
- [36] Fitsilis, F. and Rêgo de Almeida, P. G. (2024) Chapter 9: Artificial intelligence and its regulation in representative institutions. In: *Research Handbook on Public Management and Artificial Intelligence*, Cheltenham, UK: Edward Elgar Publishing. Available from: <https://doi.org/10.4337/9781802207347.00019> [Accessed 26 June 2025]
- [37] Fitsilis, F. Koryzis, D. and Schefbeck, G. (2022) Legal Informatics Tools for Evidence-Based Policy Creation in Parliaments. *International Journal of*

- Parliamentary Studies*, 2(1). Available from: <https://doi.org/10.1163/26668912-bja10031>. pp. 5–29.
- [38] Fitsilis, F. von Lucke, J. and De Vrieze, F. (2025) Inception, development and evolution of guidelines for AI in parliaments. *The Theory and Practice of Legislation*. Available from: <https://doi.org/10.1080/20508840.2025.2474791>. pp. 1–24.
- [39] Fitsilis, F. von Lucke, J. and Frank, S. (2023). A Comprehensive Research Workshop on Artificial Intelligence in Parliaments. *International Journal of Parliamentary Studies*, 3, 2, Available From: <https://doi.org/10.1163/26668912-bja10074> [Accessed 30 June 2025]. pp. 316–324.
- [40] Fytsilis, F. (2025) *4th Global Conference on Parliamentary Studies – Program*. [online] Available from: <https://hellenicocrteam.gr/4th-global-conference-on-parliamentary-studies-program/> [Accessed 26 Jun. 2025]
- [41] Ganzevles, J. Van Est, R. and Nentwich, M. (2014) Embracing variety: introducing the inclusive modelling of (Parliamentary) technology assessment. *Journal of Responsible Innovation*, 1(3), Available from: <https://doi.org/10.1080/23299460.2014.968439>. pp. 292–313.
- [42] Gialuz, M. and Quattrocchio, S. (2023) AI and the Administration of Criminal Justice in Italy. *International Review of Penal Law*, 2023(2). Available from: <http://www.penal.org/sites/default/files/files/A-01-23.pdf>
- [43] Granja P. (2023) The Portuguese Parliamentary Reporters’ Experience with Automated Speech Recognition Systems. *The Journal of Professional Reporting and Transcription*, 2/2023. Available from: <https://tiro.intersteno.org/2023/12/the-portuguese-parliamentary-reporters-experience-with-automatic-speech-recognition-systems/> [Accessed 30 Jun. 2025]
- [44] Guihot, M. Matthew, A.F. and Suzor, N.P. (2017) Nudging Robots: Innovative solutions to Regulate Artificial Intelligence. *Vanderbilt Journal of Entertainment and Technology Law*, Vol. 20, No. 2. Available from: <https://scholarship.law.vanderbilt.edu/jetlaw/vol20/iss2/2>. pp. 385–456.
- [45] Hankins, E. (2024) *Strengthening AI governance in Chile: GoBLab UAI and the importance of collaboration*. [online] Oxford Insights. Available from: <https://oxfordinsights.com/insights/strengthening-ai-governance-in-chile/>, [Accessed: 22 Jun. 2025.]
- [46] Homoki P. and Zódi Z. (2024) Large language models and their possible uses in law. *Hungarian Journal of Legal Studies*, vol. 64. (3) 2023. Available from: <https://doi.org/10.1556/2052.2023.00475>. pp. 435–455.

- [47] Inter-Parliamentary Union. (2024) *emphGlobal parliamentary community recommits to multilateralism for peace*. [online] Available from: <https://www.ipu.org/news/press-releases/2024-10/global-parliamentary-community-recommits-multilateralism-peace> [Accessed 26 June. 2025]
- [48] Inter-Parliamentary Union. (2022) *How AI helps the Italian Senate manage amendments*. [online] Available from: <https://www.ipu.org/innovation-tracker/story/how-ai-helps-italian-senate-manage-amendments> [Accessed 26 June. 2025]
- [49] Inter-Parliamentary Union. (2023) *A view from Estonia: AI for advanced beginners*. [online] Available from: <https://www.ipu.org/innovation-tracker/story/view-estonia-ai-advanced-beginners> [Accessed 26 June. 2025]
- [50] Inter-Parliamentary Union. (2024) *Guidelines for AI in parliaments*. [online] Available from: www.ipu.org/AIguidelines [30 June 2025]
- [51] IPU. (2024) *The impact of artificial intelligence on democracy, human rights and the rule of law*. Resolution adopted unanimously by the 149th IPU Assembly
- [52] Inter-Parliamentary Union. (2025). *Automated Hansard report system: Converting parliamentary audio to text using AI*. [online] Available from: <https://www.ipu.org/ai-use-cases/automated-hansard-report-system-converting-parliamentary-audio-text-using-ai> [Accessed 26 June. 2025]
- [53] Baptista, J. et al. (2020) Digital Work and Organisational transformation: Emergent Digital/Human Work Configurations in Modern Organisations. *The Journal of Strategic Information Systems*, 29(2).
- [54] Kawahara, T. (2012) Transcription System Using Automatic Speech Recognition for the Japanese Parliament (Diet), *Proceedings of the AAAI Conference on Artificial Intelligence*, 26(2). Available from: <https://doi.org/10.1609/aaai.v26i2.18962>
- [55] Kawahara, T. (2017) Automatic meeting transcription system for the Japanese parliament (diet). 2022 *Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)*, 1. Available from: <https://doi.org/10.1109/apsipa.2017.8282177>
- [56] Kawahara, T. Ueno S. & Morikawa M. (2020) Transcription system using ASR in the Japanese Parliament. *The Journal of Professional Reporting and Transcription*, 1/2020. Available from: <https://tiro.intersteno.org/2020/05/transcription-system-using-automatic-speech-recognition-in-the-j>

- [57] Kertysova, K. (2018) Artificial Intelligence and Disinformation: How AI Changes the Way Disinformation is Produced, Disseminated, and Can Be Countered. *Security and Human Rights*, 29, 1-4, 55-81, Available From: <https://doi.org/10.1163/18750230-02901005> [Accessed 30 June 2025]. pp. 55-81
- [58] Koryzis, D. et al. (2023) Disruptive Technologies for Parliaments: A Literature Review. *Future Internet*, 15(2), Available from: <https://doi.org/10.3390/fi15020066>
- [59] Krasner, S. D. (2016) The persistence of state sovereignty. In: Fioretos, O. Falleti, T. G. & Sheingate A. (eds.) *The Oxford handbook of historical institutionalism*. Oxford University Press. pp. 521–537
- [60] Kratid. (2022) *AI Kasutuslood*. [online] Available from: <https://www.kratid.ee/kasutuslood-kratid> [Accessed 26 Jun. 2025]
- [61] Kuhlmann, S. (2024) Government Use of Facial Recognition Technologies under European Law. In: Matulionyte, R. and Zalnieriute, M. (eds.) *The Cambridge Handbook of Facial Recognition in the Modern State*. Cambridge: Cambridge University Press (Cambridge Law Handbooks), pp. 127–138.
- [62] *Law no. 17/2021, On the Portuguese Charter of Human Rights in the Digital Age*, Portuguese Republic. In: Portuguese
- [63] Lee, J. (2020) Artificial Intelligence and Human Rights: Four Realms of Discussion: Summary of Remarks. *Proceedings of the ASIL Annual Meeting*, 114. Available from: <https://doi.org/10.1017/amp.2021.47>. pp. 242–245.
- [64] Lucke J. and Fitsilis F. (2023) Using Artificial Intelligence in Parliament - The Hellenic Case. in: Lindgren, I. et al. (eds.) *Electronic Government - EGOV 2023. Lecture Notes in Computer Science*, 2023/14130. Available from: https://doi.org/10.1007/978-3-031-41138-0_12
- [65] Mandri, J. M. (2019) *Judges Are Robotics: The State Is Looking for Ways to Implement Artificial Intelligence in the Judiciary* [online] Available from: <https://forte.delfi.ee/artikkel/85777829/kohtunikud-saavad-robotabilised-riik-otsib-voimalusi-kohtususteemis-tehisintellektirakendamiseks> [Accessed 30 June 2025]
- [66] Mügge, D. (2023) The securitization of the EU's digital tech regulation. *Journal of European Public Policy* 30(7), Available from: <https://doi.org/10.1080/13501763.2023.2171090>
- [67] Mügge, D. (2024) EU AI sovereignty: for whom, to what end, and to whose benefit? *Journal of European Public Policy*, 31(8). Available from: <https://doi.org/10.1080/13501763.2024.2318475>

- [68] Nascimento, P. et al. (2024) Automatic transcription system for parliamentary debates in the context of assembly of the republic of Portugal. *International Journal of Speech Technology*, 27, pp. 613-635.
- [69] National Library of Norway. (2023). *Norwegian Parliamentary Speech Corpus 2.0*. [online] Available from: <https://www.nb.no/sprakbanken/en/resource-catalogue/oai-nb-no-sbr-84/> [Accessed 30 Jun. 2025]
- [70] Necz, D. (2024) Rules over words: Regulation of chatbots in the legal market and ethical considerations. *Hungarian Journal of Legal Studies*, 64(3), Available from: <https://doi.org/10.1556/2052.2023.00472>. pp. 472–485.
- [71] Nesta. (2025) *The Brazilian Chamber of Deputies' LabHacker and eDemocracia*. [online], Available from: <https://www.nesta.org.uk/feature/six-pioneers-digital-democracy/the-brazilian-chamber-of-deputies-labhacker-and-edemocracia/>
- [72] Nortal. (2024) *How AI accelerates the legislative power of the Parliament of Estonia*. [online] Available from: <https://nortal.com/insights/how-ai-accelerates-the-legislative-power-of-the-parliament-of-estonia/> [Accessed 26 June. 2025]
- [73] Norwegian Board of Technology. (2024). *Norway In European Parliamentary Technology Assessment Network: Artificial Intelligence and Democracy 2024 Report*. [online] Available from: <https://eptanetwork.org/news/epta-news/24-publication/140-epta-report-2024> [Accessed 30 Jun. 2025]
- [74] Orwat, C. et al. (2024) Normative challenges of risk regulation of artificial intelligence, *NanoEthics*, 18(2). Available from: <https://doi.org/10.1007/s11569-024-00454-9>
- [75] Pangeanic Blog. (2024) *Pangeanic to implement AI transcription technology in Spanish Parliament*. [blog entry] 27 November. Valencia: Pangeanic. Available from: <https://blog.pangeanic.com/pangeanic-will-implement-ai-transcription-technology-in-spanish-parliament> [Accessed 30 June 2025]
- [76] Italian Senate. (2025) *Disegno di legge S. 1146 - 19^a Legislatura*. [online], Available from: <https://www.senato.it/leg/19/BGT/Schede/Ddliter/58262.htm>
- [77] Penagarikano, M. et al. (2023) Semisupervised Speech Data Extraction from Basque Parliament Sessions and Validation on Fully Bilingual Basque-Spanish ASR, *Applied Sciences*, 13(14), Available from: <https://doi.org/10.3390/app13148492>. pp. 84–92.
- [78] Public Sector Tech Watch. (2025) *GENAI4LEX-B: AI-powered legislative support in the Italian Chamber of Deputies*. [online] Available from: <https://interope>

- table-europe.ec.europa.eu/collection/public-sector-tech-watch/genai4lex-b-ai-powered-legislative-support-italian-chamber-deputies [Accessed 26 Jun. 2025]
- [79] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828. *Official Journal of the European Union* (OJ L 2024/1689) 12 July. Available from: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj> [Accessed 30 June 2025.]
- [80] Savaget, P. Chiarini, T. and Evans, S. (2019) Empowering political participation through artificial intelligence. *Science and Public Policy*, 46(3), Available from: <https://doi.org/10.1093/scipol/scy064>. pp. 369–380.
- [81] Scherer, M. U. (2016) Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, And Strategies. *Harvard Journal Of Law & Technology*, 29(2). Available from: <https://jolt.law.harvard.edu/articles/pdf/v29/29HarvJLTech353.pdf> [Accessed 26 June 2025]. pp. 358-376.
- [82] Solberg, P. E. and Ortiz, P. (2022) The Norwegian Parliamentary Speech Corpus. In: Calzolari, N. et al. (eds.) *Proceedings of the Thirteenth Language Resources and Evaluation Conference*. Marseille, France: European Language Resources Association. Available from: <https://aclanthology.org/2022.lrec-1.106/> [Accessed 30 Jun. 2025]. pp. 1003–1008.
- [83] Souza, E. et al. (2021) An Information Retrieval Pipeline for Legislative Documents from the Brazilian Chamber of Deputies, *Frontiers in artificial intelligence and applications*. Available from: <https://doi.org/10.3233/faia210326>. pp. 119-126.
- [84] Supreme Court of Estonia. (2024) *Artificial Intelligence: A Substitute or Supporter of Judges? - Yearbook of Estonian Courts* [online] Available from: <https://aastaraamat.riigikohus.ee/en/artificial-intelligence-a-substitute-or-supporter-of-judges/> [Accessed 22 Jun. 2025]
- [85] Tilde. (2020) *Custom neural machine translation engines help Seimas translators to significantly boost their productivity and efficiency*. [blog entry] Tilde.ai, 23 March. Available from: <https://tilde.ai/custom-neural-machine-translation-engines-helps-seimas-translators-to-significantly-boost-their-productivity-and-efficiency/> [Accessed 30 Jun. 2025]
- [86] Trembo, S. E. (2024) *In its Resolution, the Seimas has formulated the principles of use of artificial intelligence technologies in the public sector*. [online] Office of the Seimas of the Republic of Lithuania. Available from: <https://www.lrs.lt/sip/p>

- ortal.show?p_r=35403&p_k=2&p_t=288543&p6=25 [Accessed 30 Jun. 2025]
- [87] van Noordt, C. and Misuraca, G. (2020) Exploratory Insights on Artificial Intelligence for Government in Europe. *Social Science Computer Review*, 40(2). Available from: <https://doi.org/10.1177/0894439320980449>, pp. 426-444.
- [88] Varju, M. (2022) The Protection of Technology Sovereignty in the EU: Policy, Powers and the Legal Reality. *European Law Review*, 47(4), pp. 568-583.
- [89] Wahl, T. (2024) The Rise of Data and ai in Parliamentary Proceedings – The Norwegian Parliament, Stortinget. *International Journal of Parliamentary Studies* 4, 1. Available From: <https://doi.org/10.1163/26668912-bja10080> [Accessed 30 June 2025]
- [90] Žagar, A.P. (2024) *Exploring parliamentary AI debates with computational text analysis*. [blog entry] University of Helsinki. Available from: <https://www.helsinki.fi/en/researchgroups/reimagining-public-values-in-algorithmic-futures/whats-new/exploring-parliamentary-ai-debates-with-computational-text-analysis> [Accessed 30 Jun. 2025]
- [91] Ziouvelou, X. Giannakopoulos, G. and Giannakopoulos, V. (2022) Artificial Intelligence in the Parliamentary Context. In: F. Fitsilis and G. Mikros (eds.) *Smart Parliaments: Data-Driven Democracy*. European Liberal Forum. Available from: https://liberalforum.eu/wp-content/uploads/2022/11/Smart-Parliaments_ELF-Study_Techno-Politics_vol.4.pdf [Accessed 26 Jun. 2025]

DOI 10.5817/MUJLT2025-2-7

GIVE REALISTIC CYBER PEACE A CHANCE *

by

DAN JERKER B. SVANTESSON †

The topic of Cyber peace is receiving surprisingly little attention. Having considered some characteristics of Cyberspace affecting the topic of Cyber peace and having considered whether we benefit from trying to strictly define what we mean by Cyber peace, the article proceeds to offer a defence for the role that law may play towards Cyber peace. Against this background, the article proposes a focus on the three criteria Alfred Nobel articulated for his famous Peace Prize: (1) advance fellowship among nations, (2) the abolition or reduction of standing armies, and (3) the establishment and promotion of peace congresses, as a suitable point of departure towards Cyber peace. The article concludes that to move towards Cyber peace we need specific, practical, and realistic actions rather than lofty proclamations. Thus, it calls for the establishment of a realistic "Cyber Peace Agenda" and introduces ongoing work towards such an Agenda under the custodianship of the Norwegian Nobel Institute.

KEY WORDS

Cyber Peace, Cyberwar, Cybersecurity, Information Conflict, Sovereignty

* This article was written during my time as a Fellow at the Norwegian Nobel Institute. I am grateful to all the members of the Institute, as well as the other Fellows I got to work with, for their friendliness and for being so welcoming. I also take this opportunity to thank those who attended, and provided feedback, on the presentations I gave on this topic at the Nobel Peace Center (April 2025) and at the Peace Research Institute Oslo (May 2025).

† Professor, Bond University. Fellow, Norwegian Nobel Institute. Senior Fellow, Social Cyber Institute. E-mail: dasvante@bond.edu.au

1. INTRODUCTION

Cyberspace plays a central role in society. While helpful in many respects, this also creates an unavoidable dependency on Cyberspace. In turn, this dependency is a vulnerability, and it creates an attack surface that hostile actors seek to exploit. Those hostile activities force States to respond by a range of measures aimed at mitigating the associated risks. Conflict – in different forms – is now a prevalent feature of Cyberspace. Against this background, "Cyber peace" is more important than ever. Yet, the topic of Cyber peace is getting limited attention.

This article explores some steps that we can take towards Cyber peace. Such a venture may adopt a range of different starting points and methods. To identify some key steps that we can take towards Cyber peace, I here adopt Alfred Nobel's approach to the Peace Prize as the point of departure. This choice will also guide the structure adopted to a great extent.

In his final will of 1895, Nobel pointed to three criteria for the Peace Prize. As commonly translated, they are: (1) advance fellowship among nations, (2) the abolition or reduction of standing armies, and (3) the establishment and promotion of peace congresses.¹ I will structure the discussion of Cyber peace around these three criteria for two reasons. First, there is obvious value in examining how these criteria may be understood in the modern context of Cyberspace; after all, they are guiding the way in which the Peace Prize is awarded, and the Nobel Peace Prize is doubtlessly impacting how we think about peace. Second, while, by no means suggesting that this is the only option, I do contend that these three criteria may provide a helpful structure for analysing what is involved in the idea of "Cyber peace", and this is my attempt at showing why I have reached that conclusion.

The discussions result in a proposal for a "Realistic Cyber Peace Agenda" to include a set of proposed actions we may take in the pursuit of Cyber peace, and some thoughts on how this Agenda may be structured, developed, and used.

However, to prepare the ground for these discussions, it is necessary to first make some rudimentary observations about the nature of Cyberspace and what Cyber peace – or peace in Cyberspace – means and may look like. It is what we can observe in those discussions that has prompted my call for us to all be realistic about what we may expect. Yet, inaction is, in my view, not an option. I also briefly discuss a line of criticism that has been directed at the role that law may play in securing Cyber peace. As my discussion is

¹ The Nobel Prize. (2025) *Full text of Alfred Nobel's will*. [online] Available from: <https://www.nobelprize.org/alfred-nobel/alfred-nobels-will/> [accessed 11 August 2025].

largely focused on the law, it is appropriate to advance some defences against such criticism.

To conclude these introductory remarks, I hasten to acknowledge that there is much that could be said about the various topics addressed within this article. Topics such as the principle of distinction, the concept of sovereignty, and the issue of attribution deserve – and have received – detailed treatment elsewhere. Adding substantially to that is, however, not the aim here. Nor do I aim to comprehensively and systematically restate what others have said on such topics. Here the aim is to provide more of an examples-driven "birds eye" view of the topic of Cyber peace via a small selection of useful illustrations so as to hopefully point to some possible paths for the important, more detailed, work that lies ahead on the road towards Cyber peace.

2. THE NATURE AND ROLES OF CYBERSPACE

To understand Cyber peace, we must first realise that Cyberspace is both (1) its own war-fighting domain, and (2) supporting all other war-fighting domains (land, sea, air, and space). The former is illustrated e.g., by cyberattacks. But, as is elaborated upon below, it is also reasonable to see the Cyberspace domain as something broader than such cybersecurity issues. For example, it also includes information and cognitive warfare.

The fact that Cyberspace is supporting all other war-fighting domains is apparent when we consider the role that Cyberspace plays in everything from communications and targeting to logistics, situational awareness, and Command and Control. Especially if we include Cyberspace supporting all other war-fighting domains when we discuss Cyber peace, it is clear that offline peace is a necessary, but not sufficient, condition for Cyber peace; that is, we cannot have Cyber peace without offline peace, but offline peace does not guarantee Cyber peace. In contrast, perhaps it is possible to argue that we may have offline peace despite not having Cyber peace. In the end, this obviously comes down to how we chose to delineate Cyber peace from offline peace, and perhaps that distinction does not serve us as well as may instinctively be assumed. We will have reason to return to that topic a little later.

To complete the picture, before we can progress further, it must also be noted that, even where we approach Cyberspace as its own distinct war-fighting domain, this domain is not entirely cut off from the "real" physical world; after all, a cyberattack will often have serious real-world implications. In severe cases they may e.g., involve shutting down a hospital or causing a dam to open and cause flooding. This connection

between Cyberspace and the offline world is not unique to Cyberspace as a war-fighting domain. We see this also in many other settings; for example, cyber bullying – that occurs online – affects real people in the real world. This interconnectedness between Cyberspace and the offline world must always be kept in mind in any discussion of Cyber peace.

At any rate, perhaps the most important observation we can make when discussing the nature and roles of Cyberspace, is that Cyberspace offers an alternative means to achieving strategic gains historically unattainable without physical war. This comes in many different forms but is perhaps best illustrated by the so-called cognitive warfare that commonly forms part of the Cyberspace domain. As noted in the 2024 edition of US Department of Defense's annual report on Military and Security Developments Involving the People's Republic of China. "PLA articles on CDO [cognitive domain operations] state that seizing mind dominance in the cognitive domain and subduing the enemy without fighting is the highest realm of warfare."²

Importantly, all this points to just how multifaceted is the Cyberspace domain. Most people may immediately think of cyberattacks, but the Cyberspace domain is also characterised e.g., by a strong emphasis on information war (or perhaps better expressed as "information conflict"), espionage, and Open-Source Intelligence (OSINT). This means that Cyber conflict and Cyber hostilities can take many different forms.

Another noteworthy aspect of the Cyberspace domain is that it often is part of what is commonly discussed as the "grey zone" or "hybrid warfare". Put simply, these concepts, when used properly, seek to highlight the fact that Cyberspace activities frequently are carried out in times without open hostilities, and below the threshold for what counts as an "armed attack" under United Nations Charter, Article 51 (which then limits the defenders options), yet in times of high tension and with potentially serious effects on the victim State. We will have reason to examine this matter in more detail below. However, before leaving this topic, it is important to emphasise that, while the Cyberspace domain often is discussed in terms of "grey zone" or "hybrid warfare", Cyber operations can, and do, occur independently of hybrid strategies.

Finally, before leaving the discussion of the nature and roles of Cyberspace, it is also relevant to make some observations about the special features, or characteristics, of Cyberspace that affect these roles. First, it

² U.S. Department of Defense (2024) *Military and Security Developments Involving the People's Republic of China 2024*. [online] Available from: <https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2024.PDF> [accessed 11 August 2025].

is both common and useful to discuss the different "layers" of the Cyber domain. There is, of course, a physical layer made up of hardware in various forms such as the servers and cables that connect us. The significance of the physical layer from a Cyber defence perspective has been put on display lately with the large number of incidents in which ships from certain States have managed to accidentally, negligently, or intentionally, cut undersea communications cables e.g. in the Baltic Sea and around Taiwan.

In addition to that physical layer, we can distinguish between the logic layer consisting of software and applications, the data layer made up of the data that in many ways is the "lifeblood" of the Cyber landscape,³ and the social, persona, or cognitive layer made up of persons, real or fake, who act in one way or another online. All these layers, not just the physical layer, can be subject to various forms of attacks and they all need to be defended.

The second special feature of Cyberspace that I want to mention is its so-called "borderlessness". While we are used to our physical world being divided by various types of borders, whether they are between different States or within States, those legal constructs do not naturally map onto any of the mentioned layers apart from (to a degree) the physical layer. For example, data can generally flow easily across the legal constructs we call State borders, and different communities in the social layer may be organised e.g., according to interests rather than geographical locations.

A consequence of the noted "borderlessness" is that the Internet caters for a completely different degree of interconnectedness between people in different States than we are used to from the offline world. Many positive consequences can flow from this increased cross-border interaction. However, it also means that it is easier for people in one State to cause harm in another State.

A third characteristic of Cyberspace that must be noted when we discuss Cyber peace is the low threshold for engagement in conflicts. While there are private defence organisations also in the physical world, it is generally difficult for private individuals and organisations to take part in military conflicts; at the minimum they need to be physically present where the conflict takes place, and they need expensive equipment to be effective. In Cyberspace, neither of these thresholds apply. An individual can engage in a conflict from anywhere in the world and with the help of a relatively cheap computer or even a smart phone. Furthermore, the private sector, such as the major Internet companies, plays a significant role in the Cyberspace domain. This means that there is a potentially large number of types of actors that

³ The "data layer" is not always included in the discussions of the layers, but I think it is important to address it separately.

must be taken into account when discussing Cyber peace. As is elaborated upon in the below, this may both be an asset and source of risks.

Fourth, Cyberspace, just like dynamite – the invention that, beyond others, built Alfred Nobel's wealth – is an excellent example of what has been termed dual-use technologies; that is, technologies that may serve both civilian and military purposes. Beyond Cyberspace itself, most of its components and aspects of the online world are also examples of dual-use technology. Cyberspace may be used for peace, and it may serve the aims of war. The same is true about cloud computing, blockchain, emails, social media, websites, and the like.

The fifth characteristic of Cyberspace that must be kept in mind when working towards Cyber peace is that cyberattacks typically involve significant preparatory work. While that does not distinguish cyberattacks from kinetic attacks per se, the difference is found in where the preparatory work takes place. While exceptions certainly can be found, most kinetic attack will be prepared from the attacker's territory. In contrast, preparations or cyberattacks involves work in the intended victim's system. While a State may have a right to express concerns about the buildup of hostile troops in a neighbouring State, until an attack takes place, the current role of laws is often limited. But already the preparatory work prior to a cyberattack may well be argued to violate international law and would certainly contravene domestic laws in most cases.

Turning to the sixth characteristic of note for Cyberspace, perhaps it might be said that, while website technology made us all potentially worldwide publishers, social media truly facilitated the opportunity to "go viral". But social media also did something else. The content we published on our websites would be found and consumed primarily based on its relevance in relation to the searches of other users. In contrast, when it comes to social media, it is well-known that content that sparks strong emotional responses typically gets a far wider reach and greater engagement. It is not a particularly big step to take to imagine that these peculiar dynamics have shaped online behaviour, and in this regard, the social media platforms – and the choices they have made in the algorithms they adopt – have a lot to answer for.

Finally, and this has perhaps already been alluded to in the above, Cyberspace is now entwined into just about every aspect of life. This sets it apart from other areas in relation to which there are international efforts to create regulation. Contrast, for example, the important ongoing work by the United Nations Committee on the Peaceful Uses of Outer Space. Would it even be possible to start imagining a United Nations Committee

on the Peaceful Uses of Cyberspace? I think not as such a committee would be tasked with discussing almost every aspect of human life outside war. Agreement between States seems an impossibility. On the other hand, perhaps such a committee is just what we need to avoid the "siloing" that currently undermines progress in Cyberspace governance?

3. CAN WE DEFINE REALISTIC CYBER PEACE?

Can Cyberspace ever be at peace? The answer to that question doubtlessly depends on how we define peace. It also depends on how we define Cyberspace. The discussion above should have provided some guidance as to how I here approach the concept of Cyberspace. However, it is necessary to also say a few words about how we may best understand the word "peace" in the Cyberspace context.

While not speaking specifically about Cyberspace, it is rather telling that the Swedish Prime Minister, in January 2025 observed: *"Sweden is not at war, but not at peace either"*.⁴ It may safely be assumed that Sweden is not the only State that perceives the current international climate this way. But a particularly interesting aspect of this statement is that it challenges the traditional binary distinction between war and peace. Are we now in a period where this longstanding binary distinction no longer reflects reality? After all, States rarely declare war these days, "cyberwar" is difficult to define,⁵ and intense competition and conflict now takes place much more frequently below the threshold for war, than it does above that threshold. All this complicates any attempt to define Cyber peace.

Nevertheless, there are, unsurprisingly, several definitions around, and it has, for example, been noted that:

"An early use of the word "peace" in the context of cyberspace and the Internet is a 2008 forward [sic] written by the former Costa Rican president and Nobel laureate, Óscar Arias Sánchez, for the International Telecommunications Union's (ITU) report on the ITU's role in cybersecurity. He referred to the need to promote "peace and safety in the virtual world" as "an ever more essential part of peace and safety in our everyday lives" and the urgency of creating a "global framework" to provide cybersecurity. He implied that this safe place within cyberspace can be implemented

⁴ The Brussels Times (2025) Sweden is 'not at war' but not at peace either, says PM Kristersson. [online] Available from: <https://www.brusselstimes.com/1389724/sweden-is-not-at-war-but-not-at-peace-either-according-to-pm-kristersson> [accessed 11 August 2025].

⁵ Téllez Carvajal, E. and González Hernández, J. (2022) Reflections on the Concept of Cyberwar and the Contributions of the International Community in the Peaceful Use of Cyberspace, *Opinión Jurídica*, 21(46) Special Edition, pp. 1-23.

through intergovernmental coordination around cybersecurity practices.”⁶ (Internal references omitted)

Some definitions are relatively brief, such as Roff observing that “Cyber peace is the end state of cybersecurity. Yet it is not a mere absence of attacks, rather it is a more robust notion about the very conditions for security.”⁷ Others are more elaborate such as the definition provided by Shackelford, Douzet, and Ankersen in the Introduction to their seminal edited volume on Cyber peace:

“a positive cyber peace is defined here as a polycentric system that (1) respects human rights and freedoms, (2) spreads Internet access along with cybersecurity best practices, (3) strengthens governance mechanisms by fostering multistakeholder collaboration, and (4) promotes stability and relatedly sustainable development.”⁸ (Footnotes omitted)

Commenting on these four pillars, Marlin-Bennett has referred to Diehl’s observation that “some positive peace concepts muddle the distinction between the definitional aspects of peace and the causal conditions needed to produce peaceful outcomes.”⁹ Drawing upon this, she concludes that “the four cyber peace pillars may fall prey to this lack of conceptual clarity and, perhaps, to a sort of tautology.”¹⁰

Furthermore, while most people no doubt would happily endorse the ambitions expressed in the definition offered to us by Shackelford, Douzet, and Ankersen, it may be argued that not all what they include is absolutely needed to achieve what we may call Cyber peace. For example, could we not have positive Cyber peace¹¹ – that is, Cyber peace that involves “relations that are just, sustainable, and conducive human flourishing in multiple ways”¹² – in the absence of “multistakeholder collaboration”? And if there was no further spread of Internet access beyond what we have today, would that mean that

⁶ Marlin-Bennett, R. (2022) Cyber Peace: Is that a Thing? In: Shackelford, S., Douzet, F., & Ankersen C. (eds) *Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace*. Cambridge: Cambridge University Press, pp. 3–21, at 5.

⁷ Roff, H. M. (2016) *Cyber Peace: Cybersecurity Through the Lens of Positive Peace*. [online] Available from: https://static.newamerica.org/attachments/12554-cyber-peace/FOR%20PRINTING-Cyber_Peace_Roff.2fbbb0b16b69482e8b6312937607ad66.pdf

⁸ Shackelford, S. Douzet, F., & Ankersen, C. (2022) Introduction. In: Shackelford, S., Douzet, F., & Ankersen C. (eds.) *Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace*. Cambridge: Cambridge University Press, pp.19 – 31, at 24.

⁹ Diehl, P. (2019). Peace: A Conceptual Survey. In: *Oxford Research Encyclopedia of International Studies*. Oxford University Press.

¹⁰ Marlin-Bennett, R. (2022) Cyber Peace: Is that a Thing? In: Shackelford, S., Douzet, F., & Ankersen C. (eds) *Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace*. Cambridge: Cambridge University Press, pp. 3–21, at 14.

¹¹ Contrast to “negative peace”, understood as the mere absence of violence in a relationship.

¹² Marlin-Bennett, R. (2022) Cyber Peace: Is that a Thing? In: Shackelford, S., Douzet, F., & Ankersen C. (eds) *Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace*. Cambridge: Cambridge University Press, pp. 3–21, at 13.

we can never reach Cyber peace? Perhaps I am misunderstanding their definition, but at the very least, it seems to me that we must acknowledge that these pillars are all matters of degree and that the definition might have benefited from expressly addressing how that impacts the definition.

At any rate, we may here pause to make two observations. First, it seems clear that Cyber peace is something more than the mere absence of Cyber war and cyberattacks. This is a point with which I fully agree. Second, definitions of Cyber peace have so far been heavily focused on cybersecurity. However, as I have hinted at above, Cyber conflict takes many forms such as cognitive warfare, information warfare, and espionage. This, I think, needs to be reflected in any definition of Cyber peace. Put differently, we will not reach Cyber peace merely by focusing on cybersecurity; also this obviously complicates the task of achieving Cyber peace.

In the end, it may well be the case that academics, and not least legal academics (myself included), are overly concerned with definitions. Perhaps we should not seek to specifically define Cyber peace? After all, when it comes to a concept like Cyber peace, a definition is only useful if it: (1) helps encourage and guide our actions in the pursuit of that we seek to define (here, Cyber peace), and at the same time (2) it does not limit, exclude, or discourage actions that may help the pursuit of that we seek to define (here, Cyber peace).

With that in mind, I certainly endorse the view that the term Cyber peace cannot, and should not, be defined precisely, and that we rather should use the term to orient the mind toward the right choices, and that consequently “*it must remain somewhat open-ended. The definition cannot be watertight, but must be rather intuitive, and incremental in its list of ingredients.*”¹³

Against this background, we may now turn to the three criteria that Nobel included in his will in relation to the Peace Prize. Guided by those three criteria we can examine what may be done in the pursuit of Cyber peace even in the absence of a strict definition of Cyber peace. First, however, a few observations may usefully be made in defence of the role that law may play in the pursuit of Cyber peace.

¹³ Wegener, H. (2011) A Concept of Cyber Peace. In: International Telecommunication Union, *The Quest for Cyber Peace*. Available from: https://www.itu.int/dms_pub/itu-s/opb/gen/s-gen-wfs.01-1-2011-pdf-e.pdf, pp. 77-85, at 78.

4. IN DEFENCE OF "CYBER LEGALISM"

I see law as playing a major role in achieving Cyber peace. Indeed, it may well be the case that I, in this article, expose myself to legitimate criticism of having overlooked a range of other important mechanisms. Others will be better placed to add any such mechanisms to complete the picture.

The view that the law is central to Cyber peace is widely, but not universally, shared. Some commentators have sought to point out the inadequacy of international law as a tool to address hostilities in Cyberspace. This is healthy. We must always be prepared to discuss and evaluate the value of the tools on which we rely.

Here, I will seek to defend the role of the law. It must be understood, however, that I am *not* necessarily defending the structure and application of *current* law. Indeed, the article should make clear that I see a strong and widespread need for legal reform, but I do maintain a conviction that law must play a significant part in creating Cyber peace.

A particularly interesting and engaging discussion may be found in Kello's recent book "Striking Back". There he goes to great lengths to demonstrate that "Cyber legalism" – the doctrine that stresses the importance of existing international institutions and legal frameworks – fails and that we therefore must focus on a harsher, more aggressive, strategic doctrine instead. He argues that "*Until and unless the legal system is equipped with instruments to limit technological acts of unpeace [his term], policymakers must find a solution to problems of cyber conflict prevention elsewhere - in the realm of strategies to deter aggression by rational means*".¹⁴

In more detail, he advocates what he calls "punctured deterrence" which the reader late in his book finds out is retaliation carried out as a single action wherever and whenever best fits the victim's interest and capacities, in a manner of the victim's choosing, and that may be in response to a series of actions for their cumulative effect.¹⁵ We may, of course, question how many States in the world have the option to effectively adopt this punctured deterrence. Would, for example, Estonia in 2007 been able to, and well served by, adopting this doctrine in response to the Russian cyberattacks? Personally, I doubt it. Kello acknowledges the problem but unless his aim is simply to support the spreading "might makes right" doctrine, he could have done much more to explore alternatives for the vast majority of States that are not well positioned to rely on striking back as their response to cyber incidents.

¹⁴ Kello, L. (2022) *Striking Back: The End of Peace in Cyberspace – and How to Restore it*, New Haven: Yale University Press, p. 61.

¹⁵ Kello, L. (2022) *op. cit.*, pp. 143-144, p. 148.

At any rate, the main thrust of Kello's attack on "Cyber legalism" is built on two significant misunderstandings. First, he is, of course, correct to point out the aspects of legalism that do not work well, and doing so is important. But it is entirely misguided to see this as a question of either Cyber legalism or strategic doctrine. As they are not mutually exclusive, we must work via both as both may serve the goal of Cyber defence and ultimately Cyber peace.

The second main misunderstanding underpinning his attack on Cyber legalism relates to the war-peace distinction and has two parts. One frequently sees claims such as Kello's claim that "*cyber conflict often occurs along a spectrum between the poles of war and peace.*"¹⁶ At the same time, Kello complains that the "*existing legal framework reinforces the traditional war-peace binary that underpins Western strategic doctrine.*"¹⁷ This latter point is indeed a major issue, and – as discussed – we can probably all agree that the line between war and peace is not as clear in practice as it may be portrayed in theory. But the two claims Kello make are irreconcilable and thus, to the extent that this is meant to be a criticism of law, it lacks sting. If the existing legal framework is binary, there clearly cannot be any "spectrum between the poles of war and peace".

The second part of this misunderstanding relates to its focus. Any talk of hybrid war, grey zone war, or indeed a spectrum between the poles of war and peace leads the mind astray. What we do have, and what really is the concern, is hostile activities that are perceived as severe, perhaps even "war-like", but that nevertheless fall beneath the relevant key thresholds; in particular the Article 51 threshold for an "armed attack" found in the UN Charter.¹⁸ As hostile actors deliberately structure their attacks (and campaigns) so as to fit below the Article 51 threshold, they successfully cause damage without running the risk of a significant lawful response from the victim State. This must be seen as a flaw in the current legal structure and should be remedied.

Thus, the cure to this unfortunate, but from a historical perspective understandable, situation is found in: (a) international instruments acknowledging some right to respond also for attacks beneath the Article 51 threshold, or (b) State practice to evolve showing that States see such

¹⁶ Kello, L. (2022) *op. cit.*, p. 45.

¹⁷ *ibid.*

¹⁸ For a detailed discussion see e.g.: Haataja, S. (2019) *Cyber Attacks and International Law on the Use of Force The Turn to Information Ethics*, [online], CCDCOE, Available from: <https://cyberlaw.ccdcoe.org/wiki/Self-defence> [accessed 11 August 2025] and Pangrazzi S. (2021), *Self-Defence against Cyberattacks? Digital and Kinetic Defence*. In: ICT for Peace Foundation. *Self-Defence Against Cyberattacks?*, Geneva. Available from: <https://ict4peace.org/wp-content/uploads/2021/03/ICT4Peace-2021-Cyberattacks-and-Article51-1.pdf> [accessed 11 August 2025].

additional right as existing. The latter is, of course, a more uncertain and dangerous path.

It is easy to relate to the frustration Kello expresses in relation to international law, the disdain and hypocrisy with which it is treated by a growing number of States, and the weakness, or indeed lack, of its enforcement. However, international law plays several roles, and I wish to conclude this section defending international law by outlining what those roles are.

Combining the works of Hart¹⁹, Koskenniemi²⁰ and Svantesson²¹ one can argue that international law fulfills at least four different roles. International law is (1) a tool to decide legal disputes; (2) a tool to provide a framework to control, to guide, and to plan life out of court; (3) a tool to express and communicate the values of those who created the law; and (4) a tool – a surface or a playing board – on which political adversaries recognise each other as such and pursue their adversity in terms of something shared. Acknowledging these quite diverse roles of international law, it is difficult to maintain the argument that Cyber legalism's current inadequacies are fatal to law as a tool for Cyber peace, and at least to me, it seems clear beyond intelligent dispute that law must continue to play a role in the pursuit of Cyber peace.

5. THE FIRST CRITERIA: ADVANCE FELLOWSHIP AMONG NATIONS

If we are to understand how the first of Nobel's criteria applies in the context of Cyber peace, it is important to first recognise that the standard translation focused on advancing "fellowship among nations" amounts to a simplification of the Swedish original. The phrase used by Nobel in the Swedish original text of the will is "*folkens förbrödrande*". While it is not incorrect to translate the word "*folkens*" by referring to nations, "*folkens*" also means "the peoples". Thus, it is certainly proper to view Nobel's aim to be fellowship among people also within a domestic context, not merely on the level of the relationship between nations.

This fuller picture allows matters such as civil cyber war, and the suppression of online human rights within a State by the government of that State, to fall within the scope of what we here discuss as Cyber peace. Indeed, it may be argued that the conventional translation focusing on fellowship

¹⁹ Hart, H.L.A. (2012) *The Concept of Law*, 3rd ed. Oxford: Oxford University Press.

²⁰ Koskenniemi, M. (2011) *The Politics of International Law*, Hart Publishing.

²¹ Svantesson, D. (2015) A Jurisprudential Justification for Extraterritoriality in (Private) International Law. *Santa Clara Journal of International Law*, 13, p. 517.

among *nations* does not fully capture this and that a better translation would be "advancing fellowship among peoples" or "advancing fellowship among, and within, nations".²²

Importantly, the understanding of Nobel's first criteria advanced here is also a better fit with how the Committee awarding the Peace Prize actually has acted over the years. After all, on many occasions, the Nobel Peace Prize has been awarded to persons or organisations engaged in important conflicts-related human rights work rather than more directly in peace efforts specifically. Indeed, former chair of the Norwegian Nobel Committee, Berit Reiss-Andersen, has noted that "*The fraternity [fellowship] criteria covers, among others, human rights contributions to peace.*"²³ Against this background, it may be the case that those who have expressed criticism against the Peace Prize being awarded for important conflicts-related human rights work simply have read the text of the will too narrowly.

When discussing the criteria of advancing fellowship among (and within) nations, the first thing to note is that Cyberspace itself is a tool with a remarkable potential to do just that; advance fellowship among (and within) nations. As is commonly noted, Cyberspace has an unprecedented ability to connect people across national borders, and at least if we hold a generally optimistic view of humanity, it seems reasonable to expect that such increased connectivity between peoples ought to advance fellowship among (and within) nations.²⁴ However, we have reason to pause to consider whether this so far has brought us closer to, or further from, peace.

First of all, we may ask whether the world today is characterised by a higher degree of fellowship among nations than was the case in the pre-Cyberspace world. Exact criteria for such an assessment may be lacking, but it seems fair to say that there is a widespread and credible view that we are now considerably closer to World War III than we were in the early 90's when Cyberspace started to become an important aspect of society. Additionally, it may be argued that there is a higher degree of tension also

²² Critics of such a more expansive translation may argue that the peace movement at the time of Nobel's will was centered on nations. At the same time, however, it could be argued that there must have been a reason why Nobel chose the term "folkens" instead of alternatives explicitly limited to "nations".

²³ The Nobel Prize. (2025) *Behind the scenes of the Nobel Peace Prize*. [online] Available from: <https://www.nobelprize.org/behind-the-scenes-of-the-nobel-peace-prize/> [accessed 11 August 2025].

²⁴ Admittedly, it is also possible to take the opposite view and assume that increased contact between people automatically lead to a greater increase in friction and conflict rather than to advance fellowship among them. Much could be said about this, but the end conclusion of such a view is presumably that we are all better off not having any contact at all with each other and that we should make haste to dismantle the Internet and any other tools for communication. If so, this article is probably pointless.

among States that (at least currently) are unlikely to go to war against each other. Finally, one may point to the "Doomsday Clock" provided by the Bulletin of the Atomic Scientists' Science and Security Board as an indication of how close humanity is to self-annihilation. In the latest update (January 2025) it points to 89 seconds to midnight. The international situation as deteriorated considerably since then and yet that was the closest it has ever been to "midnight". In 1990, it was 10 minutes to midnight.

I hasten to acknowledge that the rather sad state in which we find international relations today is not only a result of our increasing dependence on Cyberspace. Thus, no definitive conclusions should be drawn. Yet, there are things we may point to – such as the propensity by some to use short messages on social media as an alternative to more classical diplomacy – that reasonably seem to be contributing to a deteriorating international relations landscape. Consequently, the reality of the world situation we face today does call into question any assertion that Cyberspace so far has advanced fellowship among nations.

Additionally, if we turn our attention to fellowship *within* nations as the discussion above suggested we ought to do as well, we can arguably also see how Cyberspace has led to a deterioration in "fellowship". In this respect, Cyberspace – and in particular social media – has had a devastating impact. Many societies are now more divided than ever before and the "filter bubbles" that ensure that our online exposure is restricted to content that tends to confirm our exiting views have been a driving force in this. Work towards social cohesion is crucial, and social media must play a more responsible role in the fight against harmful social division.

If we were to try to summarise the above, perhaps it may be said that the ability of Cyberspace to create connections among nations (and their peoples), has not yet resulted in the desirable fellowship among nations (and their peoples) that it has the potential to create. This should, however, not be seen as any criticism against Cyberspace. Cyberspace, as such, is neutral – it can be used for good, and it can be used for bad. Rather, the failure here lies in the governance of Cyberspace.

It was entirely predictable that Cyberspace would reflect human behaviour generally. As e.g., there are child abuse materials in the physical world, there was always going to be child abuse materials in Cyberspace. And as States seek to compete with each other in the physical world, they were bound to do so also online. We have not dealt with this well, and it may be said that law/regulation/governance has so far failed Cyberspace. Recognising the harm caused by certain uses of Cyberspace (e.g the content filter bubbles in social media), it is not enough to curse the private companies

that operate social media. The law must respond and set clear boundaries. Importantly, law has failed the promise offered by Cyberspace both by being overly intrusive and creating an environment of complex partly overlapping laws, and by being too passive not sufficiently addressing harmful content and practices online.

In all this, it must be remembered that Cyberspace is neither the problem, nor is it the cause of the problem. Rather, unless it is adequately protected, Cyberspace risks becoming the victim of how it is used and regulated. The question is then what we can do to shape the Cyberspace environment in a manner that helps it achieve its potential to advance fellowship among (and within) nations. The answer to such a question is clearly that there is much to be done; there are many issues that could be considered under the label of advancing fellowship among (and within) nations in the pursuit of Cyber peace. Here, however, I will limit myself to focusing on three illustrative examples of the types of issues we should consider in this context, namely: Internet openness and inclusiveness, delineation of jurisdiction, and the role of sovereignty. And given the space limitations associated with a journal article, I merely seek to showcase how addressing these issues may take us some steps towards Cyber peace.

5.1. INTERNET OPENNESS AND INCLUSIVENESS

While, as was acknowledged above, Cyberspace has not yet lived up to its potential to advance fellowship among (and within) nations, we should not give up. Cyberspace pioneers have given the world a wonderful tool. Now it is time for the legal community to "tame" it and make it serve humanity and peace via openness and inclusiveness.

I realise, of course, that my statement above may be highly offensive to those who still adhere to the mindset held by the early Cyber-libertarians. However, it is no longer – if it ever was – realistic to call for Cyberspace to be unaffected by law. That position, although recycled to a degree by the blockchain community, was conclusively defeated by reality and we need not revisit that debate here. It is sufficient to note that even with the role that the law has played so far, Cyberspace is not delivering on its potential to create fellowship among (and within) nations, and that we would be in an even worse position if we had adopted the Cyber-libertarian ideals; after all, we need e.g., international humanitarian law and human rights law as much online as we do offline.

An open and inclusive Cyberspace helps connect the world with the potential to foster cross-border trade, exchange of ideas, and scientific discoveries, as well as a sense of world community. We need legal structures

that support diversity and freedoms, that nevertheless facilitate societal cohesion instead of constantly amplifies divisions. All this can clearly favour peace both in a general sense and Cyber peace specifically.

5.2. DELINEATION OF JURISDICTION

To ensure that States can coexist in a peaceful manner, we need predictable and accepted rules for the allocation of each State's rights and duties; both to each other on a bilateral or e.g., regional level, and as members of a global community. We must reverse the emerging trend in which foreign laws are treated as merely a form of "trade barriers". That trend is harmful on multiple levels and shows a decreasing respect for the rule of law, and for each other among nations – the opposite of Nobel's first mentioned criteria for the Peace Prize.

In this context, jurisdiction is, and will remain, a key concept and an important tool both under public - and private international law. Put simply, we need rules for delineating legal authority and we get that in the form of jurisdictional rules. Indeed, if we examine how the regulation of Cyberspace has worked to-date, we find that, while there are some areas of harmonisation and coordination (such as in relation to the domain name system), the main tool is our rules regarding jurisdiction and applicable law; done well, they are tools to avoid conflict and promote peace, even though they – particularly from a private international law perspective – too rarely are discussed as tools for peace.

A key issue when it comes to applying jurisdictional rules in Cyberspace is that they are traditionally viewed as anchored in territoriality – not least when it comes to public international law – and it is widely acknowledged that territoriality is a poor fit for the online environment. Anchoring jurisdictional rules in territoriality is inappropriate and often requires arbitrary decisions about "where" various events take place; decisions that may spark unnecessary tensions. Thus, it frequently generates poor and unfair outcomes, and in a range of cases, territoriality simply cannot provide the answers needed; after all, if you are regulating processes occurring in a virtual world, location is always going to be no more than a manipulable legal fiction. These are sufficiently serious flaws to justify a search for better alternatives,²⁵ and by not relying on the ill-fitted concept of territoriality, we can devise jurisdictional rules that cause less international friction. This serves the goal of advancing fellowship among nations and ultimately the goal of Cyber peace.

²⁵ See e.g.: Svantesson, D. (2015) A New Jurisprudential Framework for Jurisdiction: Beyond the Harvard Draft, *American Journal of International Law Unbound*, 109, pp. 69-74.

5.3. THE ROLE OF SOVEREIGNTY

Sovereignty is a crucial concept for how States coexist,²⁶ and leading commentators have noted that sovereignty is one of the most politically loaded terms in the discussions of State behaviour in Cyberspace.²⁷ Indeed, it could be said that our ability to address some of the most pressing challenges facing humanity – such as the diverse areas of international conflict, the disinformation-driven decline in trust in society, human rights abuses, and threats to the environment – depends, in no small part, on how well we can work with sovereignty.

Perhaps due to its centrality in international law, the concept of "sovereignty" has spawned a large number of "newer" concepts, such as "digital sovereignty", "data sovereignty", and "information sovereignty", with dubious connection to the concept of sovereignty found in international law. In my view, these newer concepts are nothing but "a shoal of red herrings" detracting from the underlying reality that (a) the international law concept of sovereignty applies in Cyberspace, and (b) we need to find a way to make that concept work appropriately in Cyberspace.

Additionally, it seems that the increased use of the term "sovereignty" is resulting in an ever-lower level of shared understanding of what sovereignty is and what function(s) sovereignty fulfills. Such a lowering in the degree of shared understanding may be a conscious strategy by some States, but it is harmful and must be resisted. Nevertheless, it is also the case that the current mainstream thinking on sovereignty is ill-equipped for the modern world; not least in the Cyberspace environment.

To this may be added that sovereignty now is under threat on a level not seen since the end of World War II. At the January 2025 edition of the annual "Folk och Försvar"²⁸ conference in Sweden, esteemed Russia expert – Dr. Gudrun Persson of the Swedish Defence Research Agency – observed that:

*"The Russian view of the world order is largely based on a particular view of sovereignty and the multipolar world. According to this view, only a great power can be sovereign and decide for itself. Small states cannot do that. They are vassals or satellites to the great power and must bow [to the great powers]. According to this view, the world order must be based on a number of poles; Russia, USA, China, Brazil, India and so on. And now Putin is making great power claims."*²⁹

²⁶ See e.g.: *Ibid.*

²⁷ 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.

²⁸ Translates roughly as "Society and defence".

²⁹ Original Swedish: "Den ryska bilden av världsordningen bygger i hög grad på en särskild syn på suveränitet och den multipolära världen. Bara en stormakt kan enligt denna syn vara suverän och

Recently, the Trump administration has made a range of statements e.g., relating to Greenland, Panama, Gaza, and Ukraine, indicating that also the US – under the current regime – shares these troubling attitudes towards sovereignty. To this may be added China's longstanding aggressive attempts to impose dominance in the South China Sea, in the Pacific, and elsewhere, as well as its constant threat to occupy democratic Taiwan by force.

Our thinking on sovereignty must show awareness of this type of attitudes and the threat to peace to which they amount. Indeed, I argue that, in order to remain a valuable tool to serve the aim of peace, our work on defining sovereignty must seek to actively counter these attitudes – it must aim to equip the concept of sovereignty to serve as a shield against these attitudes. Doing so is not a case of so-called "lawfare", it is about fair laws. We must advocate the best version – or understanding – of sovereignty possible, not content ourselves with repeating (partially) obsolete mantras articulated over the past 100 years or so in a handful of cases. This represents an opportunity to also explore a conception of sovereignty that is not anchored in territoriality and thus would be more easily applied in the Cyberspace environment; all in the pursuit of Cyber peace.

6. THE SECOND CRITERIA: ABOLITION OR REDUCTION OF STANDING ARMIES

The idea of the abolition or reduction of standing armies may look different in Cyberspace compared to how it looks offline, and leading commentators such as Tzagourias and Biggio have pointed to the difficulties associated with discussing cyber-disarmament.³⁰

There are presently comparatively little by way of standing armies, in a traditional sense, in the Cyberspace environment, although Cyberspace forces are rapidly increasing in size. The dynamics of Cyberspace are such that a State does not require a large standing army to constitute a serious threat to other States. However, States do require a large standing army of cybersecurity expertise to minimise and mitigate the threats, including those posed by other States in Cyberspace. Such capabilities almost always overlap with civilian – private sector – cybersecurity capabilities, and it is not always

bestämma själv. Små Stater kan inte det. Dom är vasaller eller satelliter till stormakten och ska böja sig. Världsordningen ska enligt denna syn bygga på ett antal poler; Ryssland, USA, Kina, Brasilien, Indien och så vidare. Och nu gör Putin stormaktsanspråk." See Persson, G. (2025) "Vi vet vad Ryssland vill" - Gudrun Persson, docent Försvarsmakten [online video] Available from: https://youtu.be/H5RdtHiCE1o?si=_pLb7rOZ-zvWSol1 [accessed 11 August 2025].

³⁰ Tzagourias, N. and Biggio, G. (2021) Cyber-peacekeeping and international law. In: Tzagourias, N. and Buchan, R. (eds.) *Research handbook on international law and cyberspace*, 2nd ed., Northampton, Massachusetts. Edward Elgar Publishing, pp. 345-365.

possible, or meaningful, to distinguish between civilian and military when it comes to cybersecurity and cyber defence.

In the light of the above, as far as Cyberspace is concerned, the second criteria on which Nobel placed emphasis – the abolition or reduction of standing armies – should in my view be understood to be predominantly, if not exclusively, focused on offensive capabilities; indeed, offensive capabilities whether in the form of standing armies, or otherwise. Such offensive capabilities may be a concern also if produced on an *ad hoc* basis as frequently is the case where certain authoritarian States utilise non-State actors such as Cyber criminal groups.

There are several distinct aspects of the Cyberspace domain that could be highlighted when we discuss the criteria of abolition or reduction of standing armies. Below I briefly discuss three examples of such aspects, namely (1) recalibrating the positions of attackers and defenders, (2) abandoning the hidden use of non-State actors, and (3) Cyberspace as an alternative to the use of kinetic weapons. All three of those topics warrant extensive discussions and I am here constrained to merely introduce them superficially as illustrations without making any attempt to link into the literature engaging with the more intricate issues within each topic.

6.1. RECALIBRATING THE POSITIONS OF ATTACKERS AND DEFENDERS

Arguably the best way to apply the criteria of the abolition or reduction of standing armies to Cyberspace is to see it as a call to recalibrate the balance between attackers and defenders. We need to facilitate an environment capable of abolition or reducing the "attacker advantage" that currently is prevalent in the Cyberspace domain.

In the AI arms race, for example, we see a clear illustration of one aspect of the "attacker advantage". It is true that AI can be used in support of both offensive and defensive cyber measures. However, for an aggressor, AI technology can be seen as a success if it proves effective at least some of the times it is being used. In contrast, for a defender using AI technology, that technology must prove effective in nearly all cases to be of value. Imagine, for example, that a State is using AI technology both in its offensive capabilities and in its defensive capabilities. Imagine further that the technology in each task is effective at a rate of 50%. In such an instance, an evaluation would presumably conclude that the AI technology is highly effective in its offensive application, but ineffective to the degree of being useless in the defensive role.

The dynamics created by the "attacker advantage" may lead to a vicious circle where States view increased offensive capabilities as the

only meaningful response due to the inefficiency of defensive capabilities. Breaking such a chain of events is crucial for the abolition or reduction of standing armies in Cyberspace.

A central challenge for the defenders in Cyberspace is found in the lack of available personnel. This is often discussed in relation to cybersecurity experts, but it is an issue more broadly also impacting e.g., information conflicts. One obvious way to address this issue and help rebalance the comparative situation between attackers and defenders is found in education. We need more high-level cybersecurity experts, but we also need to work to increase the base-level cybersecurity knowledge in the public. This increase in capability will serve cyber defence, the fight against cyber crime, and ultimately Cyber peace.

In addition, we need to develop defender "surge capacity" via Cyber reserve forces and structures for promoting and harnessing volunteer capabilities. Admittedly, it may seem counterintuitive to call for an increase of the number of people engaged in Cyber defence as part of a move to abolish or reduce standing armies. However, such a view misses the point made above distinguishing between offensive and defensive capabilities. Cyberspace is a whole-of-society resource, and it requires a whole-of-society defence. Increasing society's capabilities to defend a vital resource such as the Cyberspace environment can, thus, not be contrary to Nobel's goal of the abolition or reduction of standing armies.

A related way to support defenders over attackers in the Cyberspace environment would involve refining the "principle of distinction"; that is, the principle requiring that parties to an armed conflict at all times distinguish between civilians and combatants and between civilian objects and military objectives.³¹ While the principle of distinction remains of central importance for guiding the behaviour of those engaging in cyberattacks, when attacks on a State's Cyberspace environment, as noted, is a whole-of-society matter, it is hard to see how the cyber defence could be anything but a whole-of-society matter. Thus, calls to keep civilians out of the cyber defence are unrealistic and yet such civilians need to be appropriately protected. In a sense, what I am proposing involves using a reformed version of the principle of distinction to give the defender an advantage by essentially limiting the principle's application to attackers only. Similar steps could be taken in relation to some other legal principles regulating conflicts.

³¹ ICRC. (2023) *The Principle of Distinction*. [online] Available from: https://www.icrc.org/sites/default/files/wysiwyg/war-and-law/03_distinction-0.pdf [Accessed 11 August 2025].

Another key step towards countering the attacker's advantage in Cyberspace could be taken if we can improve the attribution of cyberattacks and other hostilities, including mis- and dis-information campaigns. Current attribution challenges strongly favour the attacker, and they provide plausible deniability. Attribution is often technically difficult but that should only be seen as a sign that we need to put even more resources into developing better attribution techniques.³²

Finally, scholars such as Housen-Couriel have pointed to the role that information sharing can play in addressing the "attacker advantage": *"Typical informational asymmetries that have characterized cyber hostilities to the advantage of the attacker are addressed by the sharing of data."*³³ Also this may help rebalancing the positions of attackers and defenders in a manner favourable to Cyber peace, and such information sharing is not only useful in the context of cybersecurity, but obviously information sharing is at least equally important when it comes to information conflicts. Indeed, sharing of information e.g., relating to ongoing threats, may be crucial in the fight against mis- and dis-information.

In this context, we may also point to the importance of solidarity with the States that currently are less advanced in their use, and regulation, of the online environment. Information sharing with such States is important and should be supplemented by training and the sharing of practises. But it cannot just be a focus on "best practises" from the point of view of the more advanced States as too often is the case. The "best practises" from the advanced States must be adjusted to the specific context of the developing States and made to be useful in their specific environment; this is an important point often missed in various "bench-marking" studies.

6.2. ABANDONING THE HIDDEN USE OF NON-STATE ACTORS

Perhaps the greatest risk of unwanted escalation through Cyberspace activities stems from the fact that several States actively "outsource" a range of questionable, or directly illegal, activities to non-State actors. The reason States do this is obvious; it gives them plausible deniability. However, the risks are great as these non-State actors may not be as tightly controlled as regular Cyberspace forces, and may of course, have agendas of their own.

As argued above, cyber volunteers may be a useful addition for cyber defences, but peace and security in Cyberspace would be enhanced greatly

³² *Ibid.*

³³ Housen-Couriel, D. (2022) Information Sharing as a Critical Best Practice for the Sustainability of Cyber Peace. In: Shackelford, S., Douzet, F., & Ankersen C. (eds.) *Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace*. Cambridge: Cambridge University Press, pp. 39–63, at 53.

if we could prevent the use of such actors in offensive activities online, and, perhaps even more importantly, if we could ensure transparency in their use. In other words, States should agree to abandon the hidden use of non-State actors.

6.3. CYBERSPACE AS AN ALTERNATIVE TO KINETIC WEAPONS

While the risk of Cyberspace activities leading to conflict-escalation are commonly emphasised, several leading experts have also noted that Cyberspace activities may be used to de-escalate conflicts; the Cyberspace domain may be used as a much-needed off-ramp in serious conflict situations. In the words of Valeriano and Jensen: “Cyber operations are not clear paths to peace, but in the context of more dramatic options digital technologies can lead us down a road away from war.”³⁴ In this context, a commonly used example is found in the well-known Stuxnet operation attributed to Israel and the US resulting in a serious disruption of Iran’s ability to develop nuclear weapons.³⁵ The planting of the code that caused the harm may obviously be seen as a form of cyberattack – an aggression. Yet, it is easy to see that any kinetic alternative – such as an air strike, or less likely, a special forces raid, not to mention a full-scale military invasion – would have (a) caused collateral damage not caused via the cyberattack, and (b) involved a considerably higher risk of escalation.

With examples like this in mind, it seems clear that we ought to consider in more detail the circumstances under which we may be willing to sacrifice some Cyber peace in order to maintain peace in the offline world. Doing so clearly has the potential to support Nobel’s goal of abolishing, or at least reducing, standing armies as a whole. Indeed, if all international competition and conflict was limited to expressions in Cyberspace, there would be almost no need at all for standing armies in a traditional sense.

³⁴ Valeriano, B. and Jensen, B. (2022) De-escalation Pathways and Disruptive Technology. In: Shackelford, S., Douzet, F., & Ankersen C. (eds.) *Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace*. Cambridge: Cambridge University Press, 64–93, at 66.

³⁵ See e.g.: *Ibid.* and Marlin-Bennett, R. (2022) Cyber Peace: Is that a Thing? In: Shackelford, S., Douzet, F., & Ankersen C. (eds.) *Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace*. Cambridge: Cambridge University Press, pp. 3–21.

7. THE THIRD CRITERIA: ESTABLISHMENT AND PROMOTION OF PEACE CONGRESSES

Peace congresses of the kind that were common around the time when Nobel finalised his will at the end of the 1800s are no longer taking place. Thus, not least in the Cyberspace context, it may be worthwhile to read the criteria of establishing and promoting peace congresses broadly. And when doing so, there are numerous examples of attempts to coordinate and promote global peace efforts that may be noted. For example, to mention a few arbitrary examples we may note:

- The Paris Call for Trust and Security in Cyberspace;
- The various UN Groups of Governmental Experts (UNGA Res. 73/266 (Dec. 5, 2018)) and Open-Ended Working Groups (UNGA Res. 73/27 (Dec. 22, 2018));
- The Global Commission on the Stability of Cyberspace (GCSC), including its Norms of Responsible Behaviour in Cyberspace and Call to Protect the Public Core of the Internet;
- The Erice Declaration on Principles for Cyber Stability and Cyber Peace;
- The International Telecommunication Union's five principles for cyber peace; and
- The EU Institute for Security Studies' Advancing the Cyber Programme of Action (PoA).

All these initiatives are commendable, and there are of course others. In addition, there is also a wide range of more general attempts to coordinate Internet governance that have a more indirect, or indeed implicit, peace focus:

- Internet Governance Forum;
- The NETMundial Multistakeholder Statement;
- The Hague Charter for Accountability in the Digital Age;
- Internet & Jurisdiction Policy Network; and
- The UN's High-Level Panel on Digital Cooperation.

It is not my ambition here to discuss any of these initiatives. They were selected as illustrations only, and others have already discussed them in detail. For example, Douzet, Géry and Delerue expertly describe the history of several important developments with a particular emphasis on the complicated Cyber peace building dynamics within the various processed that have taken place within the United Nations' structures. Published

in 2022, they note that: “the renewed strategic competition and exacerbated geopolitical tensions have led states to engage not only in a cyber arms race, but also in a competition for normative influence.”³⁶ That was no doubt a correct assessment at that time. But the world has already changed considerably since then. Arguably the new environment in which we are now may lead to one of two outcomes. The first – and perhaps most likely – option is that the continued hardening of the strategic competition and exacerbated geopolitical tensions will lead to an even more intense cyber arms race and competition for normative influence. The second alternative is that the US continues to withdraw from the international community. That second option may well include increased, or at least a continued, cyber arms race but result in less competition for normative influence as there may no longer be any shared norms at all. Much is uncertain at the time of writing, and it is easy to agree with the claim that “The road to cyber peace is paved with malicious intentions.”³⁷

7.1. ESTABLISHING A REALISTIC CYBER PEACE AGENDA

Guided by the criteria of establishing and promoting peace congresses, I have called for what we may refer to as a “Realistic Cyber Peace Agenda” that brings together many of the points raised above throughout the article.³⁸ Part of the idea was that, at least when it comes to Cyber peace, we need specific, practical, and realistic actions more than we need lofty proclamations. In other words, drawing upon the observations about possible actions in the pursuit of Cyber peace that we have been able to tease out above via the three criteria included in Nobel’s will, we may start to form a sort of action plan for Cyber peace. While more work is needed to identify suitable agenda items, in the light of the above, some potential action items for such a Cyber Peace Agenda could, for example, include:

- Reforming the rules regarding jurisdiction;
- Reforming the rules regarding sovereignty;
- Improved tools for attribution; and
- Ban on the hidden use of non-State actors in Cyberspace.

³⁶ Douzet, F. Géry, A. and Delerue, F. (2022) Building Cyber Peace While Preparing for Cyber War. In: Shackelford, S. Douzet, F. & Ankersen C. (eds.) *Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace*. Cambridge: Cambridge University Press, pp. 170–193, at 191.

³⁷ Douzet, F. Géry, A. and Delerue, F. (2022) *Op. cit.* p. 171.

³⁸ The idea was first presented at a talk titled *Give (Realistic) Cyber Peace a Chance* held on 30 April 2025 at the Nobel Peace Center in Oslo, Norway. See Svantesson, D. (2025) Give (Realistic) Cyber Peace a Chance. In: Nobel Peace Center. [online] Available from: <https://www.nobelpeacecenter.org/en/events/give-realistic-cyber-peace-a-chance> [accessed 11 August 2025].

Already this short list of examples is ambitious. Yet it is obviously illustrative rather than exhaustive. My aim has been to point to *some* potential actions that would address some of the more obvious obstacles to Cyber peace highlighted above. There is clearly a range of other actions – such as clearer rules regarding cyberespionage, and a ban on attacks on undersea communications cables – that have not been discussed above but that could be added to this "Realistic Cyber Peace Agenda". Consequently, this must be treated as a "living document" and I invite suggestions of proposed actions to add.

Obviously, there are also many practical issues to be worked out. For example, it must be acknowledged that different persons will have different views of what is sufficiently "peace-related" and what is sufficiently "cyber-related" to be included on a Cyber Peace Agenda. Such matters must be discussed in the context of the Agenda as it may be unhelpful for the Agenda to become unnecessarily broad.

At any rate, it must be understood that each Agenda Item stands "on its own legs"; that is, while some connections may be found, they are all generally intended to be pursued as individual goals, not as a package. Thus, there is no need to seek agreement on a large number of Agenda Items at once. Rather, the path towards Cyber peace is made up of a number of independent Agenda Items each of which will take us closer to Cyber peace if achieved.

Moving forward with the Cyber Peace Agenda in a credible manner requires a leading peace-promoting institution with a strong international reputation becoming its custodian, and the Norwegian Nobel Institute has assumed this role. The Cyber Peace Agenda will be published in 2026. This is a major and crucial step. However, much work is needed before a credible Cyber Peace Agenda can be presented and diverse input is needed and will be sought as part of the work on the Agenda.

Apart from its potential to be agenda-setting by mapping out tangible steps that may be taken towards Cyber peace, and to raise the profile of Cyber peace work generally, the Cyber Peace Agenda will be a nice way to showcase the enduring relevance of Alfred Nobel's peace initiative, and to place that peace initiative in the Cyberspace environment that now is so central to humanity.

8. CONCLUDING REMARKS

This article has focused on the topic of Cyber peace. To set the scene, it highlighted certain aspect of Cyberspace that must be considered in this context. Furthermore, it discussed the extent to which defining Cyber peace is a fruitful exercise and concluded against doing so. It also addressed some criticism directed as the role that law may play in the Cyberspace domain. The discussion then turned to focus on the application of Nobel's three criteria for the world-famous, and much coveted, Peace Prize. Drawing upon a range of admittedly arbitrary examples, it was argued that a focus on Nobel's three criteria allows us to identify action items that may usefully be pursued with the aim of reaching Cyber peace.

This is important because peace cannot be taken for granted. Rather, we need to actively work for peace, and it is in uncertain times, such as those we are in now, that we must devote even more of our attention towards peace. This applies at least as much online as it does offline. On that note, we may pause to question whether it makes sense to work for Cyber peace specifically or whether it is better to just view such work as an aspect of peace work in general; after all, the text above has more than once highlighted the degree to which Cyber is entwined in the "real" world.

I argue that it, at least currently, is useful to focus specifically on Cyber peace. Doing so can bring attention to the work that needs to get done and may help raise the profile of peace work aimed at Cyberspace. So, for now, it remains relevant to speak of "cyberattacks", "cyberwar", "cyber peacekeeping",³⁹ and "Cyber peace" despite the fact that no sharp lines can be drawn between what is Cyber and what is not.

Cyber peace has only gained limited academic attention, and while there are plenty of civil society groups in the field of Cyberspace, only a comparatively small number of them have been engaging in explicit Cyber peace work. Perhaps this is linked, in some way, to the fact that there also does not seem to be much of a grassroots movement in favour of Cyber peace. Perhaps the general public perceives the Cyber risks as too technical and too abstract for such a movement to arise? The Cyber Peace Agenda under the custodianship of the Norwegian Nobel Institute can serve as a much-needed tool to raise the profile of Cyber peace.

Alfred Nobel's approach to peace was obviously coloured by the peace discussions of his time. Looking beyond his will, Nobel appears to have seen great potential in deterrence. Indeed, the Swedish historian Tägil notes that: *"In 1891, he commented on his dynamite factories by saying to the countess*

³⁹ Kleffner, J. and Harrison Dinniss, H. (2013) Keeping the Cyber Peace: International Legal Aspects of Cyber Activities in Peace Operations. *International Law Studies*, 89, p. 512.

[Bertha von Suttner]: *"Perhaps my factories will put an end to war sooner than your congresses, on the day that two army corps can mutually annihilate each other in a second, all civilised nations will surely recoil with horror and disband their troops."*⁴⁰ To this Tägil adds that *"Nobel did not live long enough to experience the First World War and to see how wrong his conception was."* But perhaps Nobel was not wrong at all. After all, he referred to "all civilised nations". Perhaps it is just the case that nations are not yet sufficiently "civilised"? And we may wonder whether they ever will be. With that doubt in mind, deterrence may have its limitations.

Today, Nobel might have expressed his criteria slightly differently. However, it seems to me that we can continue to draw inspiration, and indeed guidance, from the three criteria articulated in his will, signed by him in its final form 130 years ago, and referred to extensively above. Indeed, I would argue that the discussion above highlights the enduring value of Nobel's thinking about the criteria for the Peace Prize and more broadly, what is needed for peace.

In the context of Cyber peace specifically, and in relation to the aim of giving realistic Cyber peace a chance, this article has noted the initiative to establish a Cyber Peace Agenda that may help focus our attention at specific proposed actions in the pursuit of this otherwise quite abstract goal. The Agenda should be a living document and no doubt develop over time.

Perhaps the most significant observation that may be made from the above is that our pursuit of Cyber peace must be an ongoing sustained effort taking the form of many small steps, and hopefully some larger steps. It is a task for anyone who wants to contribute and as many of us as possible ought to implement, at least a subtle, "peace focus" in our daily work; that is, we need not necessarily change what we work on, but we ought to pause frequently and evaluate our work through the lens of Cyber peace. We must be realistic yet determined. That way, we can give Cyber peace a chance.

⁴⁰ The Nobel Prize. (2025) *Alfred Nobel's thoughts about war and peace*. [online] Available from: <https://www.nobelprize.org/alfred-nobel/alfred-nobels-thoughts-about-war-and-peace/> [accessed 11 August 2025].

LIST OF REFERENCES

- [1] CCDCOE. *Self-Defence*. [online] Available from: <https://cyberlaw.ccdcoe.org/wiki/Self-defence> [accessed 11 August 2025]
- [2] Diehl, P. (2019). *Peace: A Conceptual Survey*. In: *Oxford Research Encyclopedia of International Studies*. Oxford University Press.
- [3] Douzet, F. G ry, A. and Delerue, F. (2022) Building Cyber Peace While Preparing for Cyber War. In: Shackelford, S., Douzet, F. & Ankersen C. (eds.) *Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace*. Cambridge: Cambridge University Press, pp. 170–193.
- [4] Haataja, S. (2019) *Cyber Attacks and International Law on the Use of Force The Turn to Information Ethics*, [online], CCDCOE, Available from: <https://cyberlaw.ccdcoe.org/wiki/Self-defence> [accessed 11 August 2025]
- [5] Hart, H.L.A. (2012) *The Concept of Law*, 3rd ed. Oxford: Oxford University Press.
- [6] Housen-Couriel, D. (2022) Information Sharing as a Critical Best Practice for the Sustainability of Cyber Peace. In: Shackelford, S., Douzet, F., & Ankersen C. (eds.) *Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace*. Cambridge: Cambridge University Press, pp. 39–63
- [7] ICRC. (2023) *The Principle of Distinction*. [online] Available from: https://www.icrc.org/sites/default/files/wysiwyg/war-and-law/03_distinction-0.pdf [Accessed 11 August 2025].
- [8] Kello, L. (2022) *Striking Back: The End of Peace in Cyberspace – and How to Restore it*, New Haven: Yale University Press.
- [9] Kleffner, J. and Harrison Dinniss, H. (2013) Keeping the Cyber Peace: International Legal Aspects of Cyber Activities in Peace Operations. *International Law Studies*, 89.
- [10] Koskenniemi, M. (2011) *The Politics of International Law*, Hart Publishing.
- [11] Marlin-Bennett, R. (2022) Cyber Peace: Is that a Thing? In: Shackelford, S., Douzet, F., & Ankersen C. (eds.) *Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace*. Cambridge: Cambridge University Press, pp. 3–21.
- [12] Michael N. Schmitt (Gen. ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge, Cambridge University Press, 2017
- [13] 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)
- [14] Pangrazzi S. (2021), Self-Defence against Cyberattacks? Digital and Kinetic Defence. In: ICT for Peace Foundation. *Self-Defence Against Cyberattacks?*, Geneva. Available from: <https://ict4peace.org/wp-content/upload>

- s/2021/03/ICT4Peace-2021-Cyberattacks-and-Article51-1.pdf [accessed 11 August 2025].
- [15] Roff, H. M. (2016) *Cyber Peace: Cybersecurity Through the Lens of Positive Peace*. [online] Available from: https://static.newamerica.org/attachments/12554-cyber-peace/FOR\%20PRINTING-Cyber_Peace_Roff.2fbbb0b16b69482e8b6312937607ad66.pdf
- [16] Shackelford, S. Douzet, F., & Ankersen, C. (2022) Introduction. In: Shackelford, S., Douzet, F., & Ankersen C. (eds.) *Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace*. Cambridge: Cambridge University Press, pp. 19 – 31
- [17] Svantesson, D. (2015) A Jurisprudential Justification for Extraterritoriality in (Private) International Law. *Santa Clara Journal of International Law*, 13, p. 517.
- [18] Svantesson, D. (2015) A New Jurisprudential Framework for Jurisdiction: Beyond the Harvard Draft, *American Journal of International Law Unbound*, 109, pp. 69-74.
- [19] Svantesson, D. et al. (2023) On sovereignty. *Masaryk University Journal of Law and Technology*. 17 (1), pp. 33–85
- [20] Téllez Carvajal, E. and González Hernández, J. (2022) Reflections on the Concept of Cyberwar and the Contributions of the International Community in the Peaceful Use of Cyberspace, *Opinión Jurídica*, 21(46) Special Edition, pp. 1-23.
- [21] The Brussels Times (2025) *Sweden is 'not at war' but not at peace either, says PM Kristersson*. [online] Available from: <https://www.brusselstimes.com/1389724/sweden-is-not-at-war-but-not-at-peace-either-according-to-pm-kristersson> [accessed 11 August 2025].
- [22] The Nobel Prize. (2025) *Alfred Nobel's thoughts about war and peace*. [online] Available from: <https://www.nobelprize.org/alfred-nobel/alfred-nobels-thoughts-about-war-and-peace/> [accessed 11 August 2025].
- [23] The Nobel Prize. (2025) *Behind the scenes of the Nobel Peace Prize*. [online] Available from: <https://www.nobelprize.org/behind-the-scenes-of-the-nobel-peace-prize/> [accessed 11 August 2025].
- [24] The Nobel Prize. (2025) *Full text of Alfred Nobel's will*. [online] Available from: <https://www.nobelprize.org/alfred-nobel/alfred-nobels-will/> [accessed 11 August 2025].
- [25] Tsagourias, N. and Biggio, G. (2021) Cyber-peacekeeping and international law. In: Tsagourias, N. and Buchan, R. (eds.) *Research handbook on international*

law and cyberspace, 2nd ed., Northampton, Massachusetts. Edward Elgar Publishing, pp. 345-365.

- [26] U.S. Department of Defense (2024) *Military and Security Developments Involving the People's Republic of China 2024*. [online] Available from: <https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2024.PDF> [accessed 11 August 2025].
- [27] United Nations Charter, Article 51.
- [28] Valeriano, B. and Jensen, B. (2022) De-escalation Pathways and Disruptive Technology. In: Shackelford, S., Douzet, F., & Ankersen C. (eds.) *Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace*. Cambridge: Cambridge University Press, 64–93.
- [29] Wegener, H. (2011) A Concept of Cyber Peace. In: International Telecommunication Union, *The Quest for Cyber Peace*. Available from: https://www.itu.int/dms_pub/itu-s/opb/gen/s-gen-wfs.01-1-2011-pdf-e.pdf, pp. 77-85.

<<< ARTICLES

BOOK REVIEWS >>>

DOI 10.5817/MUJLT2025-2-8

BRIDGING THE GAP: A REVIEW OF CYBERSECURITY FÜR MANAGER

by

JAN HOSPES *

Pufahl, M. Paulsen, P. and Arndt, P. (2024) Cybersecurity für Manager Cybergefahren wirksam begegnen – das Kompetenzmodell für die Praxis. Wiesbaden: Springer Gabler, 113 p.

1. INTRODUCTION

As legal and operational consequences of cyber incidents mount, particularly with the EU's NIS2 Directive's provisions aiming at management, the need for cybersecurity literacy among executives is urgent. In this context, *Cybersecurity für Manager: Cybergefahren wirksam begegnen – das Kompetenzmodell für die Praxis*¹ seeks to equip business leaders with a structured and accessible guide to understanding and managing cyber risks. This book is aimed squarely at non-technical executives—CEOs, managing directors, board members—and emphasizes management-level accountability, strategic integration, and practical measures. English-language markets have rather long offered management-oriented cybersecurity texts.² Starting around 2020, there has been an increase in the number of cybersecurity books aimed at management in English³ In 2022, the German-speaking region was served

* Ph.D. student, Masaryk University, Faculty of Law, Institute of Law and Technology. E-mail: jan.hospes@gmail.com

¹ Pufahl, M. Paulsen, P. and Arndt, P. (2024) *Cybersecurity für Manager Cybergefahren wirksam begegnen – das Kompetenzmodell für die Praxis*. Wiesbaden: Springer Gabler, 113 p.

² Touhill, G. J. and Touhill, C. J. (2014) *Cybersecurity for Executives: A Practical Guide*. New Jersey: Wiley & Sons, 386 p.

³ Blum, D. (2020) *Rational Cybersecurity for Business: The Security Leaders' Guide to Business Alignment*. Berkeley: Apress, 333 p.; Parenty, T. J. and Domet, J. J. (2019) *A Leader's Guide to Cybersecurity: Why Boards Need to Lead—and How to Do It*. Brighton: HBR, 240 p.; Houchin, D. (2021) *Cybersecurity for Executives, Managers, and Leaders: Arcane Knowledge of the Dark Art for Superior Decision Making: The Cyber Kill Chain*. Ad Hoc Press, 89 p.

with *Chefsache Cybersicherheit*⁴ published in 2022, with which the book in question, *Cybersecurity for Managers* shares the market and which tends to focus on sources of risk and measures. By contrast *Cybersecurity for Managers* presents a more abstract perspective that includes governance principles, which can certainly be seen as a unique selling point in the German-speaking market.

2. STRUCTURE AND KEY AREAS

The book opens with a suite of cybersecurity trends including high-level technologies—such as artificial intelligence, quantum cryptography, and Zero Trust architectures. In the following *Cybersecurity für Manager* is structured around a conceptual "Cybersecurity Competence Model" composed of a core and concentric rings. The model addresses the fundamental question: *Why* should an organization care about cybersecurity? Here, legal obligations, reputational risks, and financial exposure are discussed. The middle ring concerns *what* needs to be protected, spanning data, human factors, and infrastructure. The outer rings focus on *how* to protect it—covering governance, assessments, security operations, digital identity management, and Zero Trust architectures.

This is followed by the main part of the book, which is dedicated to the outer rings of the mentioned model. Risk management is presented as the central element of implementation, detailing a process that includes asset identification, threat modeling, and prioritization of countermeasures. Further key points of implementation include digital identity and access management and the application of Zero Trust principles are introduced.

The final chapter contains interviews with cybersecurity experts who provide insight into topics covered in the book, such as identity management and zero trust architectures, as well as new topics such as management of cybersecurity during large-scale events.

⁴ Köhler, T. R. (2021) *Chefsache Cybersicherheit: Der 360-Grad-Check für Ihr Unternehmen*. Campus Verlag, 272 p.

3. ASSESSMENT OF THE CONTENT

The introduction of advanced topics seems more akin to optimization layers than foundational building blocks of a cybersecurity management system. For managers who engage with cybersecurity as a governance and compliance challenge, this emphasis may obscure more immediate priorities: understanding their current risk posture, ensuring incident readiness, and establishing basic control structures. In this sense, the book opens with the “cherry on top” of a cybersecurity strategy, potentially diverting early attention away from the groundwork most urgently needed in non-technical leadership circles. For comparison, *Cybersecurity for Executives* provides guidance on how to develop a cybersecurity strategy.⁵ In addition, the mechanisms described here tend to be purchased from third-party providers. This gives the impression that a high level of cybersecurity is rather to be achieved by purchasing external tools than through an internal management structure. This is particularly evident in the parallel reading with *Chefsache Cybersicherheit*, which also addresses newer security concepts such as use of artificial intelligence, but in a more reflective and less prominent manner.⁶

As a conceptual framework, the Cybersecurity Competence Model is elegantly simple and visually intuitive and offers a coherent logic that mirrors how many executives are accustomed to thinking about strategic priorities. This structure lowers the barrier to entry for non-specialists, allowing them to grasp not only the technical domains of cybersecurity, but also the rationale behind them. In a landscape saturated with fragmented tools and checklists, this integrated approach is a strength.

Yet the model also reveals certain limitations when examined through a practical lens. While it organizes areas of concern effectively, it does not always provide clear prioritization within them. Managers who are early in their cybersecurity maturity journey may struggle to distinguish between foundational tasks and aspirational ones—an issue compounded by the model’s outer rings, which package advanced strategies alongside more basic governance steps without clearly sequencing them. Moreover, the model relies heavily on abstraction; it tells managers *what kinds* of measures they should pursue, but only loosely connects those categories to concrete examples, metrics, or decision points. For organizations seeking operational guidance rather than structural orientation, the model offers a compass—but not a map. A certain prioritization is made by emphasizing identity management and zero trust in Chapter 3, but it should be noted here as well that these are also rather newer and specific concepts which leads

⁵ Touhill, G. J. and Touhill, C. J. (2014) *op. cit.* p. 95 seq.

⁶ Köhler, T. R. (2021) *op. cit.* p. 185.

the conscious reader to ask why particularly these are presented. The same applies to the interviews in the final chapter. It is not entirely clear why focus is set on novelties or, with regard to the interview on cybersecurity at major events, on topics that are not actually mentioned in the book and are not part of its core subject matter.

Legal frameworks such as the GDPR and the NIS/NIS2 directives are woven into the discussion, reinforcing the point that cybersecurity is not optional but mandatory—and increasingly enforceable at the individual executive level. Indeed, under the NIS2 Directive, executives can be held personally liable for the consequences of a cyberattack in cases of proven gross negligence, placing cybersecurity squarely within the scope of fiduciary and compliance duties at the top of the corporate hierarchy. However, the information provided does not seem sufficient to allow for a legal assessment, for example, to enable managers to determine when it is better to refer an issue to a legal expert.

Cybersecurity für Manager appears prescient, yet it presents blind spots. The book strongly emphasizes the importance of management commitment, framing it as the foundation of effective cybersecurity. Throughout the text, the authors argue that security cannot be left solely to the IT department, and they explicitly call for board-level oversight, formalized risk governance, and clear responsibility structures. However, while the book clearly communicates that leadership must “own” cybersecurity, it stops short of exploring how such commitment can be cultivated within organizations.

Cybersecurity für Manager offers a well-organized, accessible, and legally informed guide to cybersecurity for non-technical executives. Its model is conceptually sound and practically actionable. Yet the book gives little priority to internal levers such as incentive structures, role modeling, accountability mechanisms, or integration into strategic KPIs. In this respect, it outlines the necessity of commitment without fully equipping readers to implement or sustain it—especially in organizational cultures where cybersecurity has traditionally been viewed as a peripheral issue. While *Cybersecurity für Manager* briefly acknowledges the increasing importance of interconnected digital ecosystems, it stops short of offering concrete guidance on how executives should evaluate and secure third-party dependencies—whether through contractual controls, supplier audits, or cross-organizational risk assessments.

4. CONCLUSION

First and foremost, *Cybersecurity für Manager* should be read as a wake-up call—a well-structured alert to the fact that cybersecurity is no longer an operational afterthought but a central pillar of corporate governance. It succeeds in making the issue approachable for non-technical executives and provides a clear introduction to the key methods, frameworks, and standards shaping contemporary cybersecurity practice. For managers looking to move beyond awareness into execution, further reading is necessary, particularly to understand how to prioritize controls, sequence maturity steps, and implement technical and procedural safeguards in detail. The strength of the book lies in showing the breadth of the field and the strategic stakes involved; its limitation is that it offers orientation more than instruction when it comes to setting up a cybersecurity strategy.

LIST OF REFERENCES

- [1] Pufahl, M. Paulsen, P. and Arndt, P. (2024) *Cybersecurity für Manager Cybergefahren wirksam begegnen – das Kompetenzmodell für die Praxis*. Wiesbaden: Springer Gabler, 113 p.
- [2] Touhill, G. J. and Touhill, C. J. (2014) *Cybersecurity for Executives: A Practical Guide*. New Jersey: Wiley & Sons, 386 p.
- [3] Blum, D. (2020) *Rational Cybersecurity for Business: The Security Leaders' Guide to Business Alignment*. Berkeley: Apress, 333 p.
- [4] Parenty, T. J. and Domet, J. J. (2019) *A Leader's Guide to Cybersecurity: Why Boards Need to Lead—and How to Do It*. Brighton: HBR, 240 p.
- [5] Houchin, D. (2021) *Cybersecurity for Executives, Managers, and Leaders: Arcane Knowledge of the Dark Art for Superior Decision Making: The Cyber Kill Chain*. Ad Hoc Press, 89 p.
- [6] Köhler, T. R. (2021) *Chefsache Cybersicherheit: Der 360-Grad-Check für Ihr Unternehmen*. Campus Verlag, 272 p.

MUJLT Official Partner (Czech Republic)

**ROWAN[®]
LEGAL**

ROWAN LEGAL, advokátní kancelář s.r.o
<https://rowan.legal>

Cyberspace 2024 Partners

ROWAN[®]
LEGAL

ZÁKONY **PRO**
LIDI

 **CODEXIS[®]**

 **Wolters Kluwer**

CATERING
FOR YOU 

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

Taniya Malik: Freedom of Internet and State Control: A Case Study on Internet Shutdowns in India.....	97
Zahra Hemmat, Mohammad Mehraeen, Rahmatolloah Fattahi, Farhad Shirani: Aligning Iran's Legislation with Sustainable Development Goals: A Topic Modeling Approach.....	127
Tamás Pongó, Renáta Kálmán, Réka Brigitta Szaniszló, Norbert Tribl: Oversight Board – An Effective Tool to Protect Free Speech?.....	151
Philippe Prince Trito, Ilse Carolina Torres Ortega: Jurists of the Gaps: Large Language Models and the Quiet Erosion of Legal Authority.....	179
Maciej Bujalski: On the Possible Use of Databases to Secure Receivable Debts...	205
Boldizsár Szentgáli-Tóth, Rudolf Berkes: Artificial Intelligence in the Service of Parliaments: Some Arguments for the Necessity of a Normative Legal Framework at the European Level.....	237
Dan Jerker B. Svantesson: Give Realistic Cyber Peace a Chance.....	273

LIST OF BOOK REVIEWS

Jan Hospes: Bridging the Gap: A Review of Cybersecurity für Manager.....	305
---	-----