Vilnius University Press

Contents lists available at Vilnius University Press

Teisė
2025, Vol. 134, pp. 16–26

ISSN 1392-1274 eISSN 2424-6050
DOI: https://doi.org/10.15388/Teise.2025.134.2

Digital Services Act: The Holy Grail of Cybersecurity?

Michał Byczyński

ORCID ID: https://orcid.org/0000-0001-6856-0627
Ph.D. Candidate
Attorney-at-law Trainee
Doctoral School of Social Sciences
Faculty of Law and Administration
University of Lodz
https://ror.org/05cq64r17
Kopcinskiego 8/12, 90-232 Lodz, Poland
E-mail: mbyczynski@lodz.adwokatura.pl

Digital Services Act: The Holy Grail of Cybersecurity?

Michał Byczyński

(University of Lodz (Poland))

This article explores the potential of the *Digital Services Act* (DSA) as a pioneering model for global digital governance. DSA, introduced by the European Union, seeks to establish a robust regulatory framework that addresses the complexities of the digital age, with a focus on platform accountability, transparency, and the protection of user rights. Through its comprehensive provisions, DSA aims to standardize approaches to content moderation, tackle disinformation, and enhance user privacy, thus setting new standards for digital responsibility. The article examines DSA's alignment with the fundamental human rights, emphasizing its capacity to inspire similar regulations worldwide. By promoting transparency, safeguarding freedom of expression, and fostering cross-border regulatory cooperation, DSA demonstrates a holistic approach that could guide international efforts in cybersecurity and digital governance. This study underscores DSA's potential to influence global regulatory practices, offering insights into how it may foster a safer and more accountable digital ecosystem on an international scale. On the other hand, it highlights the fundamental challenges of attempting to implement a DSA-like agreement on a global scale.
Keywords: Digital governance, platform accountability, freedom of expression, cybersecurity, content moderation.

Skaitmeninių paslaugų aktas: kibernetinio saugumo Šventasis Gralis?

Michał Byczyński

(Lodzės universitetas (Lenkija))

Straipsnyje nagrinėjamas Skaitmeninių paslaugų aktas (SPA) kaip novatoriško pasaulinio skaitmeninio valdymo modelis ir jo potencialas. Šiuo Europos Sąjungos priimtu aktu siekiama sukurti tvirtą reguliavimo sistemą, kuri padėtų spręsti sudėtingas skaitmeninio amžiaus problemas, ypač daug dėmesio jame skirta platformų atskaitomybei, skaidrumui ir naudotojų teisių apsaugai. Nustatant naujus skaitmeninės atsakomybės standartus, SPA išsamiomis nuostatomis siekiama suvienodinti turinio moderavimo metodus, kovoti su dezinformacija ir stiprinti naudotojų privatumą. Straipsnyje taip pat nagrinėjama šio akto atitiktis pagrindinėms žmogaus teisėms, pabrėžiamas jo potencialas paskatinti panašių reglamentų

Received: 09/01/2025. **Accepted:** 31/03/2025

kūrimą visame pasaulyje. Remiantis SPA nuostatomis didinti skaidrumą, saugoti saviraiškos laisvę ir stiprinti tarpvalstybinį reguliavimo bendradarbiavimą, demonstruojamas holistinis požiūris, kuriuo galima vadovautis tarptautinėse kibernetinio saugumo ir skaitmeninio valdymo iniciatyvose. Tyrime taip pat pabrėžiamas SPA numatomomis galimybėmis formuoti pasaulines reguliavimo praktikas, atskleidžiama, kaip jis gali prisidėti prie saugesnės ir skaidresnės skaitmeninės ekosistemos tarptautiniu mastu. Kita vertus, jame išryškinami pagrindiniai iššūkiai, kylantys siekiant įgyvendinti į SPA panašų susitarimą pasauliniu mastu.
Pagrindiniai žodžiai: skaitmeninis valdymas, platformų atsakomybė, saviraiškos laisvė, kibernetinis saugumas, turinio moderavimas.

Introduction

The advent of the COVID-19 pandemic precipitated an unprecedented global shift toward an increased digital dependency, revealing profound vulnerabilities in the existing legislative frameworks governing cybersecurity (United Nations, 2020, p. 1–2). As governments worldwide implemented lockdowns and social distancing measures, individuals and organizations were compelled to adopt digital platforms for virtually every aspect of daily life, including work, education, commerce, healthcare, and social interaction (OECD, 2020, p. 2). This massive change to online spaces not only highlighted the indispensability of digital services but also exposed significant regulatory gaps in safeguarding users against cyber threats and in terms of protecting fundamental human rights in the digital realm (European Commission, 2020, p. 3–7).

This paper investigates the regulatory implications and challenges posed by the *Digital Services Act* (DSA) in the context of human rights protection and global cybersecurity governance. The study employs doctrinal legal analysis and review of the currently existing regulatory frameworks. The primary aim of this research is to assess DSA's potential as both a protective tool for human rights and a model for international digital governance.

A review of literature was conducted, encompassing legal texts, policy papers, and academic articles. Key sources include primary legislation such as DSA, foundational documents in international human rights law, and reports from intergovernmental organizations. By synthesizing these diverse sources, this research situates DSA within broader debates about digital governance and regulatory harmonization. Unlike prior studies, which predominantly analyze DSA's provisions in isolation, this paper adopts an interdisciplinary lens, integrating insights from human rights law, cybersecurity policy, and the regulatory theory. This approach facilitates the understanding of the interplay between digital platform accountability and the protection of individual freedoms.

The objectives of this paper are twofold: first, to explore the extent to which DSA addresses systemic risks to human rights in the digital sphere; and second, to consider its potential as a scalable framework for international adoption. The central research questions include: (1) How does DSA align with the international human rights standards? (2) What are the practical challenges associated with its implementation? (3) Can DSA's principles be effectively adapted to diverse legal and cultural contexts worldwide?

This paper examines whether DSA has the potential to effectively serve as a protective tool for human rights protection within the digital space (Section 1) and assesses its potential as a model for global cybersecurity regulations (Section 2). Through analysis of its provisions, implementation challenges, and the balance it strikes between regulation and fundamental freedoms, the study aims to contribute to the ongoing discourse on digital governance and the protection of human rights in the age of the internet.

1. The importance of the Digital Services Act

1.1. Legislative background and rationale

The primary rationale behind DSA was to update the regulatory framework established by the e-Commerce Directive of 2000 (Directive 2000/31/EC). The e-Commerce Directive was pioneering in its time, providing foundational legal principles for electronic commerce and the liability of intermediary service providers. It introduced concepts such as the limited liability for mere conduits, caching, and hosting services, which facilitated the growth of the internet by allowing platforms to operate without being held responsible for the user-generated content, provided that they acted upon notification of illegal content (Edwards, 2005, p. 312–315).

However, over the past two decades, the digital landscape has undergone transformative changes (Van Dijck *et al*., 2018, p. 1–2). The exponential growth of digital services and the emergence of social media giants fundamentally altered the online environment. Platforms like *Facebook*, *Google*, *Twitter*, and others became central in the way how people communicate, access information, and engage in social and political discourse. These platforms evolved from passive intermediaries to active shapers of content through algorithms that curate and recommend content to users, often without due transparency.

The limitations of the e-Commerce Directive became evident as it failed to address issues such as algorithmic amplification of content, targeted advertising based on personal data, the rapid spread of disinformation, hate speech, and other forms of harmful and/or illegal content. The lack of clear responsibilities for platforms in moderating the content and protecting the user rights led to inconsistencies in how the illegal or harmful content was handled (Husovec, 2017, p. 25–31). The absence of robust enforcement mechanisms allowed some platforms to operate with minimal accountability, leading to calls for more stringent regulations (Kuczerawy, 2018, p. 19).

High-profile incidents, such as the Cambridge Analytica scandal – where the personal data of millions of Facebook users were harvested without consent for political advertising (Cadwalladr *et al.*, 2018) – or the massive spread of disinformation during elections and the pandemic, highlighted the need for updated regulations (Bayer *et al*., 2019, p. 124–131). These events eroded public trust in digital platforms and underscored the potential harm that unregulated digital services could cause to individuals and societies (Zuboff, 2019, p. 226, 265, 475).

1.2. Core provisions and human rights objectives

DSA introduces a range of obligations for different types of digital services, scaling responsibilities according to the size and impact of the platform (European Parliament, 2022, Recital 41).

One of the key aspects is the requirement for transparency Platforms are mandated to disclose their content moderation practices, providing users with insight into how decisions are made regarding the removal or downgrading of content (European Parliament, 2022, Articles 15.1, 24). This approach reinforces procedural fairness and supports the users' right to be informed about actions affecting their online presence. Regular transparency reports must be published, detailing the number of content removals, reasons, and methods employed (European Parliament, 2022, Article 15.1.a, b, c, d). These reports play a critical role in ensuring that users understand the application of content moderation tools, especially automated systems, and in highlighting the safeguards which those platforms implement to prevent moderation errors that could inadvertently infringe on lawful expression (European Parliament, 2022, Article 15.1.b, c, e).

Another critical provision is the imposition of due diligence obligations. The act mandates that platforms conduct regular assessments of systemic risks to their users' rights, including risks to privacy, freedom of expression, and the dissemination of illegal content (European Parliament, 2022, Article 34). Platforms are required to implement measures to mitigate identified risks, such as adjusting their algorithms, enhancing user controls, and increasing resources for content moderation (European Parliament, 2022, Article 34.1). Providers of very large online platforms and of very large online search engines, due to their significant societal influence, must adopt additional safeguards and accountability standards, as their operations usually carry broader implications for the digital information ecosystem and public trust (European Parliament, 2022, Article 34.1, 2).

Additionally, DSA introduces accountability mechanisms. Platforms must provide users with accessible mechanisms to contest content moderation decisions, including the right to appeal and receive explanations for the actions taken (European Parliament, 2022, Article 17). This emphasis on accountability underlines DSA's commitment to due process and the protection of freedom of expression. Furthermore, DSA establishes a cooperative framework between platforms and national authorities, obliging platforms to share relevant data for effective supervision and enforcement in cases of illegal content. This cooperation reinforces the overarching goal of aligning digital operations with the public interest and legal standards (European Parliament, 2022, Article 18).

DSA also addresses the protection of minors and vulnerable groups by introducing additional safeguards tailored to these users' needs. By virtue of recognizing the heightened risk of harm faced by these groups, the regulation mandates that platforms implement special measures, such as restrictions on targeted advertising based on profiling, to protect minors from inappropriate or manipulative content. This focus on user protection reflects a broader ethical responsibility towards creating a safe and inclusive digital space for all (European Parliament, 2022, Articles 28, 33, 35.1.j).

Furthermore, DSA requires platforms to ensure advertising transparency (European Parliament, 2022, Article 26). Platforms are required to ensure that their users can easily identify advertisements and understand who is behind the content (European Parliament, 2022, Article 26.1.a, b). Additionally, information regarding the targeting parameters must be accessible to users, allowing them to understand how and why specific ads reach them. Such transparency in digital advertising practices aims to mitigate the potential for manipulative or deceptive tactics, aligning advertising with ethical standards that respect user autonomy (European Parliament, 2022, Article 26.1.c).

Recognizing the importance of independent research in understanding the digital platforms' impact, DSA allows vetted researchers to access platform data under certain conditions (European Parliament, 2022, Article 40). This provision facilitates meaningful studies on systemic risks, informing policy decisions that address the digital platforms' societal impact while promoting a research-driven approach to governance.

In summary, DSA provisions enhance human rights protection in the digital environment by emphasizing transparency, accountability, and procedural fairness. Requirements for platforms to disclose content moderation practices and publish regular reports provide users with an insight into decisions that affect their freedom of expression, thereby reducing the risk of arbitrary restrictions on speech. Additionally, the obligation for platforms to assess risks to users' rights demonstrates a commitment to prioritizing fundamental rights in digital regulation. On the other hand, specific protections for vulnerable groups, through restrictions on targeted advertising and profiling, reflect an awareness of their increased vulnerability to manipulation and exploitation.

Such approach enhances transparency and enables more effective oversight of individual rights in the digital realm, which increasingly shapes public discourse and social attitudes.

1.3. Importance of DSA in addressing infodemic

The term 'infodemic' refers to the rapid and far-reaching spread of both accurate and inaccurate information during a crisis, such as the COVID-19 pandemic (World Health Organization, 2020). During the pandemic, false information about the virus's origins, transmission, treatments, and vaccines spread rapidly on social media platforms (Cinelli *et al.*, 2020, p. 1–2). This misinformation led to confusion, undermined public health measures, and resulted in harmful behaviors and violence (Kouzy *et al.*, 2020, p. 8). The *World Health Organization* (hereinafter: WHO) highlighted the infodemic as a major obstacle in managing the pandemic effectively (World Health Organization, 2020).

The DSA's approach to addressing this issue involves enhancing the transparency of platform operations and mandating the use of fact-checking mechanisms (European Parliament, 2022, Articles 14, 15, 35). Platforms are required to assess the risks of disinformation and take measures to prevent the amplification of false content (European Parliament, 2022, Articles 34, 35). This includes collaboration with designated trusted flaggers, such as reputable fact-checking organizations and civil society groups, who can notify platforms of illegal or harmful content for swift action (European Parliament, 2022, Article 22).

Moreover, DSA emphasizes algorithmic accountability. Platforms must be transparent about their recommendation systems and allow users to influence the algorithms that curate their content feeds (European Parliament, 2022, Article 27). Users should have options to view content in non-personalized ways, thus reducing the echo chamber effect that can exacerbate the spread of disinformation (European Parliament, 2022, Articles 27.3, 38). Additionally, platforms are encouraged to provide tools that enable users to report misleading information easily and access authoritative sources (European Parliament, 2022, Article 16).

By mandating these comprehensive measures, DSA aims to safeguard the public's right to access verified information, while addressing the harms associated with disinformation. Through its provisions, DSA envisions a digital ecosystem where technological advancement complements the protection of human rights, fostering a safe, transparent, and equitable online environment for users.

1.4. Will DSA work?

DSA, despite its well-intentioned goals, has sparked criticism. Scholars have pinpointed several issues that underscore the tension between regulation and rights protection within the DSA framework. Two of the most pressing concerns include DSA's reliance on vague and broad terminology and the structural constraints it imposes on the freedom of expression.

A primary criticism of DSA is its dependence on terms that are both vague and overly broad, such as 'illegal content' and 'disinformation', which are not sufficiently defined. This lack of clarity, especially in key provisions like Articles 3 and 9, grants the Member States substantial discretion in interpreting and enforcing these terms. As a result, national authorities have the latitude to define 'illegal content' in ways that may vary widely across the EU, reflecting differing national standards and legal frameworks. For instance, what constitutes 'disinformation' in one state may be seen as protected expression in another, leading to potential overreach where some content may be removed or restricted arbitrarily, based on divergent local laws (Ó Fathaigh *et al.*, 2021, p. 13).

The vagueness surrounding 'disinformation' is particularly concerning. Scholars argue that, without a precise definition, disinformation can be constructed in ways that support political or ideological agendas, resulting in the possible removal of content that merely expresses dissent or minority viewpoints. Furthermore, because DSA permits national interpretations of disinformation, some Member States might adopt criminal sanctions against it, by treating certain forms of expression as illegal content.

Although DSA professes commitment to upholding freedom of expression, its regulatory architecture introduces constraints that risk curtailing this right in structural ways. By obliging platforms to address broad and ambiguous categories of content-such as "public security risks" or "threats to public health," DSA encourages the use of extensive content moderation practices (European Parliament, 2022, Article 34.1.a, c, d). However, these tools, while efficient, lack the capacity to discern nuanced context, which is essential for distinguishing harmful content from lawful, albeit potentially controversial, expression.

AI-driven automatic filtering relies on probabilistic approaches and is contingent upon the training set utilized, potentially resulting in both false positives (elimination of harmless or advantageous information) and false negatives (continuation of harmful content) (Dias, 2020, p. 637). This challenge is compounded by the fact that AI systems struggle with understanding context, irony, and the diverse cultural or linguistic subtleties of user-generated content. Consequently, platforms may err on the side of caution, resulting in an over-removal of content and inadvertently chilling legitimate speech (Dias, 2020, p. 637).

Moreover, automated filtering systems often operate on pre-defined datasets that reflect specific biases and assumptions, potentially leading to discriminatory outcomes. Scholars argue that, under the DSA's framework, platforms are incentivized to adopt conservative content moderation practices to mitigate risk, leading to an online environment where freedom of expression is curtailed by the overzealous enforcement of vaguely defined terms (Barata, 2021, p. 19–21).

To sum up, DSA's reliance on vague terminology and its structural implications for content moderation raise substantial concerns. These aspects of DSA not only challenge the harmonization of digital rights across the Member States (European Parliament, 2022, Recital 106) but also, ironically, place fundamental freedoms, particularly freedom of expression, at risk.

2. DSA as a Model for Global Cybersecurity Regulations

In an era where digital platforms transcend national borders, the urgency for harmonized regulatory approaches has become increasingly evident. This section delves into the potential of DSA as a model for international regulatory efforts, the ways through which it can influence global policies, and the challenges and considerations associated with its adoption outside the European Union.

2.1. Global relevance of DSA's principles

DSA is underpinned by fundamental principles such as transparency, accountability, protection of human rights, and the promotion of a safe online environment, aligning with universal values recognized in international human rights instruments, including the Universal Declaration of Human Rights (United Nations, 1948, Article 19) and the International Covenant on Civil and Political Rights (United Nations, 1966, Article 17). These shared values create a strong foundation for the potential adaptation of DSA in various jurisdictions (Kulesza, 2024, p. 143). As societies across the world confront challenges like data breaches, disinformation, cybercrime, and the erosion of democratic processes, DSA's comprehensive approach thus offers a holistic framework capable of addressing these issues (World Economic Forum, 2020, p. 10).

Cybersecurity threats, which frequently cross national boundaries, often exploit gaps in jurisdictional coverage and regulatory inconsistencies (Interpol, 2022). By setting common standards, DSA facilitates coordinated responses to cyber incidents, thereby mitigating vulnerabilities that malicious actors could

exploit. Furthermore, the EU's influence as a significant global actor backed by substantial economic and political weight solidifies the potential for its regulatory approaches to become benchmarks for other states (Young, 2015, p. 19–20). DSA's innovative mechanisms in areas such as platform regulation, user protection, and content moderation may inspire analogous legislation worldwide, thus promoting the gradual harmonization of digital policies.

2.2. Pathways for international adoption and adaptation of similar cybersecurity solutions

The EU can strategically leverage its diplomatic channels to advocate for the principles embedded in DSA through participation in multilateral agreements and global forums. By initiating and maintaining dialogues on digital governance, the EU can champion the incorporation of DSA-like provisions in international agreements, thereby fostering a broader consensus on key regulatory standards (Novelli, 2024, p. 24). Initiatives such as the EU's Digital Single Market Strategy have already underscored the importance of international cooperation (European Commission, 2015). Expanding these initiatives to integrate the DSA principles could, moreover, pave the way for knowledge sharing, capacity building, and collaborative policy development with partner nations (Savin, 2021, p. 3).

Another strategic pathway for amplifying the DSA's global influence may be embedding its standards into trade agreements. The EU's trade deals frequently include provisions related to digital trade, data protection, and e-commerce (European Commission, 2021). By incorporating DSA principles into these agreements, the EU can encourage trading partners to adopt similar regulatory standards, thus creating a more consistent and fair global regulatory landscape which would protect both European businesses and consumers (Hadjiyianni, 2021, p. 243–264).

Additionally, the formation of transnational networks of regulatory authorities could facilitate the dissemination and adoption of DSA-like regulations. Such networks could serve as platforms for sharing best practices, engaging in joint training initiatives, and coordinating enforcement activities (Drezner, 2007, p. 95–100). For instance, existing frameworks like the Global Privacy Assembly and the International Conference of Information Commissioners demonstrate how collective regulatory collaboration can be effective (Global Privacy Assembly, 2021). Expanding these networks to include digital service regulations could, in turn, enhance global regulatory coherence (Koppell, 2010, p. 288).

2.3. Challenges in global implementation

Adapting DSA to diverse legal systems and cultural contexts presents significant challenges. States vary widely in their approaches to critical issues such as freedom of expression, privacy rights, state surveillance, and the extent of governmental involvement in internet regulation (DeNardis, 2014, p. 2–11). For instance, some countries may prioritize strict state control over the digital content for political or cultural reasons, which can conflict with the DSA's emphasis on user rights and platform accountability (MacKinnon, 2012, p. 42–46). Thus, implementing DSA-like regulations necessitates a nuanced understanding of the local norms, legal traditions, and societal values.

Moreover, the building of the necessary institutional infrastructure, technical expertise, and legal frameworks to support these regulations poses additional challenges. Without adequate resources and institutional support, even the most ambitious regulations may fall short of their objectives, resulting in enforcement gaps and potential market imbalances (Weiss *et al.*, 2014, p. 515). This challenge is particularly pronounced in developing or transitional economies, where the capacity to build and sustain complex regulatory frameworks may be limited. Therefore, international cooperation, especially from

more developed states and organizations, can play a pivotal role in aiding less-resourced countries to implement effective digital regulations (World Bank, 2016, p. 292–305).

Resistance from powerful stakeholders, particularly multinational technology corporations wary of increased compliance costs and regulatory constraints, is another significant obstacle. Such companies may lobby against stringent regulations or even limit their services in markets with more demanding standards, as evidenced by previous disputes over data protection laws. Additionally, governments with an interest in maintaining strong control over digital spaces or reluctance to expose state practices to scrutiny may resist adopting regulations that emphasize transparency and accountability (Powers *et al.*, 2015, p. 5–6, 111). Consequently, balancing the interests of these stakeholders with the need to protect user rights and maintain regulatory integrity requires a multifaceted strategy that encompasses skilled negotiation, strategic compromises, and clear communication of mutual benefits (Rodrik, 2011, p. 204).

While the DSA embodies principles such as respect for human rights, adherence to the rule of law, and the promotion of democratic governance, advocating these values in regions where different governance models prevail presents a significant challenge (DeNardis, 2014, p. 15–16). In cases of authoritarian regimes, implementation of DSA-inspired frameworks may require a more subtle approach that accommodates political sensitivities while still advancing core principles (Ruggie, 2014, p. 90–91).

While the international human rights law provides a strong foundation for promoting these principles, the inconsistent application and enforcement of such laws across various states complicate efforts to build a unified regulatory framework. For instance, countries with robust human rights protections may find it easier to align with DSA-like regulations, whereas states with restrictive policies on freedom of expression and privacy may pose significant challenges (Kulesza, 2024, p. 144–145).

The implementation of DSA-like regulations is also affected by global power dynamics and competition for technological leadership. The EU's position as a regulatory trendsetter is both an asset and a source of potential friction. On one hand, the EU's leadership in digital regulation can inspire other regions to adopt similar frameworks, thus creating a more cohesive global approach to digital governance. On the other hand, contrasting philosophies on internet governance, data sovereignty, and state intervention among the major powers such as the United States and China, can lead to conflicting interests and regulatory fragmentation (Yang, 2020, p. 5–8). For instance, the U.S. approach tends to prioritize market-driven solutions with minimal regulatory intervention, whereas China's model emphasizes extensive state control and surveillance (Olszewska, 2022, p. 67–72).

Moreover, the EU's promotion of the DSA model must navigate the challenge of building coalitions and partnerships so that to ensure broader acceptance. To achieve this, the EU could focus on multilateral engagements and collaborative initiatives that highlight the shared advantages of adopting comprehensive digital regulations. This approach could include joint projects, shared research, and pilot programs that showcase the effectiveness of the DSA principles in addressing common challenges.

Finally, the EU must remain vigilant in addressing the perception of regulatory imperialism, where its promotion of DSA could be seen as imposing its standards on other states. Collaborative efforts that include input from non-EU states and stakeholders can foster a sense of ownership and partnership, which is essential for sustainable and meaningful implementation of DSA-inspired regulations on a global scale.

Conclusions

1. DSA marks a significant advancement in digital regulation, aiming to create a balanced framework that upholds human rights while ensuring cybersecurity. By addressing the responsibilities of digital platforms and enhancing protections for users, DSA has the potential to reshape the digital landscape positively.
2. While ambitious, DSA's success will depend on effective implementation, enforcement, and the ability to adapt to the evolving technologies and societal needs. DSA has the potential to serve as a model for global efforts to regulate digital services and enhance cybersecurity.
3. By fostering international collaboration and emphasizing ethical, human-centric approaches, the EU can contribute to shaping a digital future that respects human dignity, promotes innovation, and protects against emerging threats.
4. The diversity and plurality of actors within the international community, however, present a significant challenge to establishing a single, consistent framework for protecting human rights in the digital environment.

Bibliography

Legal acts

United Nations. (1966). International Covenant on Civil and Political Rights. General Assembly resolution 2200A (XXI) [online]. Available at: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights [Accessed 30 October 2024].

United Nations. (1948). Universal Declaration of Human Rights. General Assembly resolution 217 A (III) [online]. Available at: https://www.un.org/en/about-us/universal-declaration-of-human-rights [Accessed 30 October 2024].

European Parliament and Council of the European Union. (2022). Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC. Official Journal of the European Union, L 277, 27 October, p. 1–102 [online]. Available at: https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng [Accessed 30 October 2024].

Special literature

Bayer, J., Bitiukova, N., Bard, P., Szakács, J., Alemanno, A., Uszkiewicz, E. (2019). *Disinformation and Propaganda: Impact on the Functioning of the Rule of Law in the EU and its Member States.* European Parliament.

Cinelli, M., Quattrociocchi, W., Galeazzi, A., Valensise, C., Brugnoli, E., Schmidt, A. L., Scala, A. (2020). The COVID-19 Social Media Infodemic. *Scientific Reports*, 10(1), 16598, https://doi: 10.1038/s41598-020-73510-5.

DeNardis, L. (2014). *The Global War for Internet Governance.* Yale University Press.

Dias Oliva, T. (2020). Content moderation technologies: Applying human rights standards to protect freedom of expression. *Human Rights Law Review*, 20(4), 607–640.

Drezner, D. W. (2007). *All Politics Is Global: Explaining International Regulatory Regimes.* Princeton University Press.

Edwards, L. (2005). The Problem with Privacy. *International Review of Law, Computers & Technology*, 19(3), 325–333.

Gorwa, R., & Garton Ash, T. (2020). Democratic Transparency in the Platform Society. In: Dijck, K.; Poell, T.; de Waal, M. (Eds.), *The Platform Society: Public Values in a Connective World*. Oxford University Press, 268–289.

Hadjiyianni, I. (2021). The European Union as a Global Regulatory Power. *Oxford Journal of Legal Studies,* 41(1), 243–264.

Husovec, M. (2017). *Injunctions Against Intermediaries in the European Union: Accountable but Not Liable?* Cambridge University Press.

Koppell, J. G. S. (2010). *World Rule: Accountability, Legitimacy, and the Design of Global Governance.* University of Chicago Press.

Kouzy, R., Abi Jaoude, J., Kraitem, A., El Alam, M. B., Karam, B., Adib, E., ... & Baddour, K. (2020). Coronavirus Goes Viral: Quantifying the COVID-19 Misinformation Epidemic on Twitter. *Cureus*, 12(3), https://10.7759/cureus.7255

Kuczerawy, A. (2018). The Power of Positive Thinking: Intermediary Liability and the Effective Enforcement of Removal Obligations. *Journal of European Consumer and Market Law*, 7(2), 69–79.

Kulesza, J. (2024). Human Rights and Social Media: Challenges and Opportunities for Human Rights Education. In: Mihr, A.; Pierobon, C. (Eds.), *Polarization, Shifting Borders and Liquid Governance: Studies on Transformation and Development in the OSCE Region*. Springer, 139–154.

MacKinnon, R. (2012). *Consent of the Networked: The Worldwide Struggle for Internet Freedom.* Basic Books.

Novelli, C., Hacker, P., Morley, J., Trondal, J., Floridi, L. (2024). A Robust Governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities. *European Journal of Risk Regulation*, 1–25, https://doi.org/10.1017/err.2024.57.

Ó Fathaigh, R., Helberger, N., Appelman, N. (2021). The perils of legally defining disinformation. *Internet policy review*, 10(4), 2022–2040.

Olszewska, K. (2022). Cyfrowy nadzór w chińskim modelu autorytarnego kapitalizmu. Uniwersytet Wrocławski. *Studia nad Autorytaryzmem i Totalitaryzmem*, 44(3), 65–73.

Powers, S. M., Jablonski, M. (2015). *The Real Cyber War: The Political Economy of Internet Freedom.* University of Illinois Press.

Rodrik, D. (2011). *The Globalization Paradox: Democracy and the Future of the World Economy*. W. W. Norton & Company.

Ruggie, J. G. (2014). *Just Business: Multinational Corporations and Human Rights.* W. W. Norton & Company.

Savin, A. (2021). The EU Digital Services Act: Towards a More Responsible Internet. Copenhagen Business School, CBS LAW Research Paper No. 21-04, *Journal of Internet Law*.

Van Dijck, J., Poell, T., De Waal, M. (2018). *The Platform Society: Public Values in a Connective World.* Oxford University Press.

Weiss, T. G., Wilkinson, R. (Eds.). (2014). *International Organization and Global Governance.* Routledge.

Yang, F. (2020). China's Approach to Cyber Sovereignty. *Journal of Cyber Policy*, 5(2).

Young, A. R. (2015). The European Union as a global regulator? Context and comparison. *Journal of European Public Policy*, *22*(9), 1233–1252. https://doi.org/10.1080/13501763.2015.1046902

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* PublicAffairs.

Other sources

Barata, J. (2021). *The Digital Services Act and its Impact on the Right to Freedom of Expression: Special Focus on Risk Mitigation Obligations.* Platforma por la Libertad de Infoacion.

Cadwalladr, C., Graham-Harrison, E. (2018). *Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach* [online]. Avaiable at: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election [Accessed 30 October 2024].

European Commission (2015). *A Digital Single Market Strategy for Europe. COM(2015) 192 final* [online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52015DC0192 [Accessed 30 October 2024].

European Commission (2020a). *Shaping Europe's Digital Future. Publications Office of the European Union* [online] (modified 2020-02-01). Available at: https://commission.europa.eu/system/files/2020-02/communication-shaping-europes-digital-future-feb2020_en_4.pdf [Accessed 30 October 2024].

European Commission (2021). *EU Trade Agreements* [online]. Available at: https://ec.europa.eu/trade/policy/countries-and-regions/negotiations-and-agreements [Accessed 30 October 2024].

Interpol (2022). *Interpol Global Crime Trend Summary Report* [online]. Available at: https://www.interpol.int/content/download/18350/file/Global%20Crime%20Trend%20Summary%20Report%20EN.pdf [Accessed 30 October 2024].

OECD (2020). *Keeping the Internet Up and Running in Times of Crisis* [online] (modified 2020-05-04). Available at: https://www.oecd.org/en/publications/keeping-the-internet-up-and-running-in-times-of-crisis_4017c4c9-en.html [Accessed 30 October 2024].

United Nations (2020). *The Impact of Digital Technologies*. *Policy Brief* [online] (modified n.d.). Available at: https://www.un.org/en/un75/impact-digital-technologies [Accessed 30 October 2024].

World Bank (2016). *World Development Report 2016: Digital Dividends. World Bank Publications* [online] (modified n.d.). Available at: https://www.worldbank.org/en/publication/wdr2016 [Accessed 30 October 2024].
World Economic Forum (2020). *Global Technology Governance: A Multistakeholder Approach* [online]. Available at: https://www3.weforum.org/docs/WEF_Global_Technology_Governance.pdf [Accessed 30 October 2024].
World Health Organization (2020). *Infodemic Management* [online] (modified n.d.). Available at: https://www.who.int/health-topics/infodemic#tab=tab_1 [Accessed 30 October 2024].

Michał Byczyński, Mgr., is Attorney-at-law Trainee and a Ph.D. candidate at the University of Łódź, Poland. His research focuses on human rights law and new technologies. He is an alumnus of the Hague Academy of International Law and a member of the European Society of International Law. He is a cybersecurity and AI security specialist (certified by *CyberPeace Institute* in Geneva and *Microsoft*), actively involved in educating about digital rights, providing legal support, and advocating for policy changes.

Michał Byczyński yra teisės magistras, advokato padėjėjas ir doktorantas Lodzės universitete (Lenkija). Jo mokslinių tyrimų sritis – žmogaus teisės ir naujųjų technologijų teisė. Autorius yra Hagos tarptautinės teisės akademijos alumnas bei Europos tarptautinės teisės draugijos narys. Būdamas sertifikuotas kibernetinio saugumo ir dirbtinio intelekto saugumo specialistas („CyberPeace Institute“, Ženeva; „Microsoft“), jis aktyviai užsiima skaitmeninių teisių švietimu, teikia teisinę pagalbą ir pasisako už politines permainas.