UNIVERSITY OF BIALYSTOK
FACULTY OF LAW

BIALYSTOK LEGAL STUDIES

BIAŁOSTOCKIE STUDIA PRAWNICZE

BIAŁYSTOK 2025 VOLUME 30 no. 4

BIALYSTOK LEGAL STUDIES
BIAŁOSTOCKIE STUDIA PRAWNICZE

VOLUME 30 no. 4

The original version of the journal is a print one.

ISSN 1689–7404

e-ISSN 2719–9452

Volume Theme Editor: Elżbieta Kużelewska

Language Editors: Ewa Gorlewska, Claire Taylor-Jay

Statistical Editor: Ewa Glińska

Graphic and Typographic Development: Eliza Wasilewska, Jerzy Banasiuk

Cover Design: Bogusława Guenther

Publisher: Faculty of Law, University of Białystok; Temida 2

All volumes can be purchased from Wydawnictwo Temida 2. Address: ul. A. Mickiewicza 1, 15-213 Białystok, Poland. E-mail: temida2@uwb.edu.pl, Tel. +48 85 745 71 68

Spis treści

Contens

Bialystok Legal Studies
Białostockie Studia Prawnicze
2025 vol. 30 no. 4

sciendo

DOI: 10.15290/bsp.2025.30.04.01

Received: 22.05.2025
Accepted: 05.08.2025

Michał Ożóg
University of Bialystok, Poland
m.ozog@uwb.edu.pl
ORCID ID: 0000–0002–4315–5235

Radosław Puchta
University of Bialystok, Poland
radoslaw.puchta@gmail.com
ORCID ID: 0000–0002–3562–1136

The Right Not to Use the Internet and Protection against the Digital Divide: Some Preliminary Remarks[1]

Abstract: This article discusses the concept of the so-called 'right not to use the internet' in the context of the digital divide. Multiple measures, undertaken at national and supranational levels with the purpose of ensuring the digital transition, have led to the expansion of the online sphere. At the same time, and despite the continuing commitments of public authorities to strengthen digital accessibility, the number of people deprived of full access and the capacity to use new information and communication technologies remains relatively high, even within developed countries. Furthermore, the current digital revolution undermines freedom of choice regarding internet use, imposing a de facto obligation to be constantly online. The authors argue that the concept of the right not to use the internet may serve as a compelling argument when making policies to counteract any digital inequalities and to preserve the fundamental freedom of choice, including the freedom to be offline.

Keywords: right not to use the internet, digital constitutionalism, digital divide, digital accessibility, internet access

1 The paper is funded by the National Science Centre, Poland, under the OPUS call in the Weave programme (UMO-2023/51/I/HS5/01417), and Flemish Research Foundation (FWO Funding Agreement G000325N). The article is also financially supported by the Polish Minister of Science under the 'Regional Initiative of Excellence' (RID) programme.

Introduction

It is hard to deny that nowadays, rapid developments in the technology sector are deeply affecting daily lives, rising serious questions about the possibility for everyone to fully enjoy their fundamental rights and freedoms in the digital age. Just as each revolution at some point begins to devour its own children, the current so-called 'digital revolution' also gives rise to certain side effects that pose challenges from the perspective of human rights protection. Ubiquitous digitalisation in fact results in the necessity, or rather an obligation, to use new information and communication technology (ICT) in order to get access to various services or products that have often become only available online. In other words, digital technologies are now no longer merely optional tools serving to ease our private, professional and social lives, but impose themselves as indispensable. This in turn means that some people may face different digital barriers, as they cannot financially afford the necessary devices or mobile applications (digital poverty), or they lack sufficient skills to operate them effectively (digital illiteracy). For others, the key problem might be the interference with their freedom of choice regarding the use of digital technologies and the coercion to be constantly online. Any wish to stay offline could then lead to the marginalisation or even exclusion of an individual from certain spheres of activity. As a result, the phenomenon of a digital divide emerges, which seriously undermines the exercise of many basic human rights, such as the right to protection of one's private and family life, the right to information and freedom of expression, the right to education, etc.

The concept of the 'right not to use the internet' is fairly new doctrinally and is still at the conceptualisation stage (Susi, 2025). Nevertheless, some scholars have already recognised its high potential as a compelling ethical and legal argument in the debate about how to prevent undesirable repercussions from widespread digitalisation and how to maintain people's freedom of choice for living a more analogue life (Kloza, 2024; Terzis, 2025). This article aims to broaden this doctrinal analysis of the right not to use the internet in the context of the positive duties of public authorities to ensure all necessary legal and factual conditions for the full enjoyment of basic human rights by everyone. We argue that the right not to use the internet, considered as a component of the catalogue of so-called 'digital rights', requires that each person shall be given a real option to choose analogue forms of interaction with the outside world, and therefore that a certain amount of offline reality shall be protected so as to guarantee the feasibility of acquiring information, goods and services in some non-digital way. To give reasons for this assertion, we outline major negative consequences of the ongoing process of mass digitalisation and depict the measures that are usually undertaken in response, which mostly result in a further decline of the offline sphere. In this context, we introduce the concept of the right not to use the internet and try to demonstrate its usefulness regarding the need to provide effective protection from the coercion to be constantly online, In the article, we apply research

methods commonly used in legal studies, such as the descriptive and conceptual methods. We analyse both supranational and national legal frameworks related to the issue of the accessibility of digital products and services, as well as relevant soft law. A dogmatic description of the concept of the right not to use the internet then serves to assess possible applications of this newly emerging digital right when developing legal solutions against digital coercion.

1. Universal digitalisation and its side effects

Since the beginning, the development of new ICT has been enthusiastically embraced by policymakers as a useful means of fostering economic and social progress. It soon became commonly assumed that this newly emerging 'digital economy' might ensure dynamic and stable economic growth (Gomes et al., 2022). At both supranational and national levels, multiple policy documents and legislation have begun to be adopted with the purpose of boosting the digitalisation process in the fields of, for instance, goods trade, services, education or public administration. Already in 2002, access to the internet was recognised as a universal service under European Union law (European Parliament & Council of the European Union. (2002, 7 March). Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services (Universal Service Directive). At the same time, because of 'the need to make further progress to keep the development of the e-economy as a priority on the European policy agenda', the eEurope 2005 Action Plan was launched (Council of the European Union, 2003). In 2010, in the aftermath of the Great Recession of 2007–2009, the European Commission presented the 'Digital Agenda for Europe', aimed at delivering sustainable economic and social benefits from a 'Digital Single Market' based on fast and ultra-fast internet and interoperable applications (European Commission, 2010). According to its assumptions, proper implementation of this agenda was supposed to spur innovation, economic growth and improvements in daily life for both EU citizens and businesses.

From the perspective of human rights law, the question has arisen, however, as to whether such a dynamic digitalisation of virtually all spheres of an individual's social, commercial or civic activity requires the guarantee of a new fundamental right, referred to as a 'right to internet access' (Best, 2004; De Hert & Kloza, 2012). Although the existence of such a right has not been explicitly acknowledged in any act of international law, universal internet access has been recognised as an indispensable tool for realising a range of human rights, combating inequality and accelerating development and human progress (La Rue, 2011). In 2012, the United Nations' Human Rights Council adopted its first resolution on the promotion, protection and enjoyment of human rights on the internet. The Council affirmed that 'the same rights that people

have offline must also be protected online', and it called upon all states to 'promote and facilitate access to the internet'. In parallel, in 2014, the Parliamentary Assembly of the Council of Europe adopted Resolution 1987 (2014), 'the right to internet access', in the light of which 'everyone shall have the right to internet access as an essential requirement for exercising rights under the European Convention on Human Rights', and therefore that 'the member States should recognise the fundamental right to internet access in law and in practice' (Council of Europe Parliamentary Assembly, 2014). This document placed particular emphasis on the requirements of the affordability, interoperability and integrity of internet services, taking into account the latest technological developments, and underlined the duty of the Member States to 'increase their efforts to ensure internet access for people with special needs and disadvantaged internet users'. Over the past decades, a clear evolution can be discerned in the approach of the European Court of Human Rights in cases where digital issues have arisen in the context of fundamental rights, as evidenced, for example, by the creative interpretation of the provisions of the Convention to formulate a standard for the protection of individual rights on the internet. In addition to the internet accessibility standard, attention is paid to the need to respect a number of other values of democratic societies, including in particular the right to privacy enshrined in Article 8 of the Convention (Wiśniewski, 2021, pp. 114–131). Subsequently, access to and use of the internet has been a constant focus of attention for international bodies responsible for protecting human rights (Szoszkiewicz, 2018). At the same time, at the national level, a new right to internet access has been constitutionalised either directly, by adopting a constitutional amendment act, or indirectly, through the creative jurisprudence of apex courts; examples of such countries include Portugal and Greece. Since 1997, the Portuguese Constitution has guaranteed everyone access to public information technology networks (Ożóg & Puchta, 2025, pp. 94–95).

Notwithstanding this favourable, sometimes even naively enthusiastic, approach to internet access, commonly regarded as a means of ensuring general well-being for all, various side effects of the digital revolution have become increasingly apparent over time. Given the fact that many goods and services – both public (e.g. submission of a tax return or registration for a medical consultation) and private (e.g. handling of a bank or insurance account) – have become available exclusively or mostly through specific websites or mobile applications, internet use, at least in some cases, has turned out to be de facto compulsory. In other words, a 'right to internet access' has transformed into a kind of obligation to get online and use ICT. For some people, universal digitalisation has resulted in limiting their freedom of choice as to how they might interact (online or offline) within horizontal and vertical relations. In the other words the horizontal perspective concerns equivalent bodies (individuals versus individuals), while the vertical perspective concerns individuals versus public authorities and we analyze the right not to use the Internet in both legal relationships, taking into account the specific circumstances of the individual. For others, in turn, this pro-

cess has brought new barriers that impede or restrain their capability to get certain goods or services. Such barriers might be due to a lack of financial resources needed to acquire the necessary devices and services from an internet provider, as well as a lack of sufficient skills to operate constantly more sophisticated ICT (so-called 'digital illiteracy'). As a result, a new phenomenon of a 'digital divide' has arisen, reinforcing already existing social, economic and political inequalities (Ragnedda, 2017).

This phenomenon of a 'digital divide' was already recognised in the last decade of the 20th century. During research in the late 1990s, a series of surveys was conducted by the National Telecommunications and Information Administration in the USA, with the aim of assessing the number and characteristics of 'information-disadvantaged' people (so-called 'Have Nots'). It was concluded that the divide between those with access to new technologies and those without was at that time 'one of America's leading economic and civil rights issues' (NTIA, 1999). In 2001, the OECD defined the 'digital divide' as a gap between individuals, households, businesses and geographic areas at different socio-economic levels with regard both to their opportunities to access ICT and to their use of the internet for a wide variety of activities (OECD, 2001). It soon became clear that such inequalities within access to and use of the internet are related to criteria such as income, age, education and geographic location. As the notion of a 'digital divide' might suggest that there is a simple division between two clearly separated social categories ('Haves' and 'Have Nots'), analysis of the phenomenon as 'a range of positions extending across whole populations – from people having no access and use at all to those with full access and using several applications every day' (van Dijk, 2020, p. 10) has been proposed. At the same time, some other terms have been promoted to describe these digital inequalities, and in particular the notion of 'digital poverty', understood as somebody's inability to interact with the online world fully, when, where and how they need to (Allmann, 2022). In contrast to the digital divide, digital poverty 'cannot be seen in dichotomic terms (i.e., digitally poor versus digitally rich) but as a continuum where different degrees of digital poverty could be observed' (Ragnedda et al., 2022, p. 5).

Although the existence of various barriers to the use of new ICT has been known for years, and despite the fact that endless efforts have already been made to remove such barriers, the phenomenon of digital inequality persists, and in some parts of the world is even increasing (Heeks, 2022). It might be said that the more goods and services have been transferred to the digital world, the more social, economic and political exclusion there is in the analogue one. According to the International Telecommunication Union's statistics, in 2024 fully 5.5 billion people were online, which represented only 68% of the world population. It means that 2.6 billion people, one-third of the global population, still did not have enough access to the internet. In the ITU's opinion, 'universal connectivity remains a distant prospect' (International Telecommunication Union, 2024, p. 1). As far as the European Union is concerned, 94% of all households surveyed in 2024 had access to the internet (Eurostat, 2024), but still about 2.4% of the

EU's 450 million inhabitants (i.e. nearly 11 million) could not afford an internet connection (World Economic Forum, 2023). The statistics of the Polish Central Statistical Office show that although 95.9% of households had internet access in 2024, the percentage of 16 – to 74-year-olds with at least basic digital skills was still only 48.8%. What is more, while at least basic digital skills were possessed by 73.5% of 16 – to 25-year-olds and by 72.1% of 25 – to 34-year-olds, the percentage was only 13.7% within the age group of 65 – to 75-year-olds. In addition to these inequalities based on age, differentiation related to territorial criteria (the degree of urbanisation) is also noticeable, as among rural residents the percentage of people with at least basic digital skills is significantly lower compared to the percentage of residents of small and large cities (33%, 45% and 55%, respectively) (Statistics Poland, 2024).

2. Common measures to address the digital divide

From the perspective of human rights law, the digital divide implies new impediments to the full enjoyment of several fundamental rights and freedoms (Saraceni, 2020). An inability to access the internet and to make use of new ICT equals an inability to freely exercise, for instance, the right to lead a private life in undisturbed contact with relatives and friends, the right to acquire and disseminate information and opinions, the right to participate actively in public and private life, the right to obtain appropriate healthcare, and the right to education, as well as the right to access cultural goods and services, etc. In the framework of the United Nations' Convention on the Rights of Persons with Disabilities, adopted in 2006, and to enable persons with disabilities to live independently and participate fully in all aspects of their life, state parties have agreed to take all appropriate measures to promote access for such people to new information and communication technologies and systems, including the internet. European institutions adopted the European Declaration on Digital Rights and Principles for the Digital Decade in 2023, announcing their commitment to 'a digital transformation that leaves nobody behind' (European Parliament et al., 2023). According to the wordings of this Declaration, everyone throughout the EU should have access to affordable and high-speed digital connectivity, as well as the right to education, training and lifelong learning enabling the acquiring of all basic and advanced digital skills. The Polish Constitution of 1997 prohibits any discrimination in social, political or economic life on any grounds; such a prohibition also applies to an individual's activities in digital reality. The Constitutional Court has stated that 'technological development expands the sphere of human functioning' and has noted that 'although the Constitution does not explicitly refer to the functioning of the individual in the virtual space, the protection of the constitutional freedoms and rights of individuals in connection with the use of the internet and other electronic means

of remote communication is no different from that concerning traditional forms of communication or other activities' (Judgment of the Constitutional Tribunal, 2014).

The existence of any barriers hampering individuals from exercising their fundamental rights and freedoms implies the positive obligation of public authorities to undertake every necessary action to overcome such barriers. It is up to competent supranational or national authorities to choose appropriate measures, provided that these are adequate, effective and proportionate. However, when it comes to removing barriers to digital inclusion, it seems that the most common answer to the side effects of the phenomenon of universal digitalisation is simply more digitalisation. In practice, countering digital exclusion most often involves seeking to facilitate accessibility and the use of services in the virtual world, and no provision is made for an offline option as a voluntarily chosen alternative that would not put the individual at a disadvantage. In other words, policy – and lawmakers are willing to adopt measures which, in general, consist in imposing on public entities as well as on private sector actors various new duties regarding the availability of goods and services offered online.

For instance, in 2016, European lawmakers adopted Directive 2016/2102 on the Accessibility of the Websites and Mobile Applications of Public Sector Bodies, also referred to as the Web Accessibility Directive. The objective was above all to harmonise national laws, regulations and administrative provisions related to the accessibility requirements of the websites and mobile applications of public sector bodies so as to make such websites and applications more accessible to their users, in particular to persons with disabilities, on the basis of common accessibility requirements. This Directive imposes on EU Member States the obligation to 'ensure that public sector bodies take the necessary measures to make their websites and mobile applications more accessible by making them perceivable, operable, understandable and robust' (European Parliament & Council of the European Union, 2016). Websites and mobile applications shall be presumed to be in conformity with these requirements where they meet the European harmonised standard EN 301 549 v3.2.1 (2021–03) (European Commission, 2021). Pursuant to this Directive, public sector bodies are supposed to provide and regularly update a detailed, comprehensive and clear accessibility statement on the compliance of their websites and mobile applications with these accessibility requirements. Each statement shall also include, firstly, information on those parts of the content that are not accessible, an explanation of the reasons for such inaccessibility and, where appropriate, information on the accessible alternatives; secondly, a description of and a link to a feedback mechanism enabling any person to notify the body concerned of any failure to comply with the accessibility requirements; and thirdly, a link to the enforcement procedure in the event of an unsatisfactory response. The Member States have therefore been obliged to set up an adequate and effective enforcement procedure, for example by enabling users to lodge a complaint with the ombudsman for failure to comply with the provisions of the Directive.

In addition, taking into account the fact that no matter how accessible a website is, it cannot be used without a suitable computer or smartphone, in 2019 European lawmakers adopted Directive 2019/882 on the Accessibility Requirements for Products and Services, which concerns products and services such as computers and operating systems, smartphones, tablets, e-readers and dedicated software, payment terminals and automated teller machines, as well as ticketing and check-in machines, consumer banking services, e-commerce services, and parts of services related to air, bus, rail and waterborne passenger transport, etc. This Directive, also referred to as the European Accessibility Act, obliges EU Member States to ensure that economic (this time private) operators place on the European market only such products, or provide only such services, that comply with the common accessibility standards set out in European law. Economic operators must ensure that they design, manufacture and place on the market products (or that they design and provide services) which correspond to multiple requirements listed in relevant annexes attached to Directive 2019/882, which have passed through a special conformity assessment procedure and bear the CE marking affixed to them (in the case of products) or include information assessing how the service meets applicable requirements. At the same time, competent national market surveillance authorities have been vested with the task of evaluating whether products meet applicable requirements, and in the event of non-compliance they may call on the economic operator concerned to take all appropriate corrective action or, in the absence of such action, to withdraw the product from the market. The Member States are supposed to establish, implement and periodically update adequate procedures in order to check the compliance of services with the requirements of this Directive, should follow up complaints or reports related to any case of non-compliance, and should verify whether the economic operator has taken the necessary corrective action. The European Accessibility Act should be implemented in national law by issuing appropriate legal regulations from 28 June 2025.

So as to implement the above-mentioned European directives, Polish lawmakers have enacted new national legal frameworks, namely the 2019 Act on Digital Accessibility of Public Entities' Websites and Mobile Applications (referred to as the DAA) and the 2024 Act on Ensuring the Compliance by Economic Operators with Accessibility Requirements Related to Certain Products and Services. These two legislative measures, together with the 2019 Act on Ensuring Accessibility for People with Special Needs, are designed to create a coherent system for protecting vulnerable people's needs (Mędrzycki, 2025). According to the DAA, 49 elements of technical requirements listed in its annex shall be met for the websites and mobile applications of public sector entities to be considered as enabling digital accessibility at the required level. These elements correspond to the Web Content Accessibility Guidelines (WCAG) success criteria (Marzec & Pietrasiewicz, 2020). A public sector entity fulfils its duty to ensure the digital accessibility of its website or application if the latter is functional, compatible, perceivable and

understandable in accordance with the relevant provisions of the Polish standard that implements the EN 301 549 V3.2.1:2021 standard.

At this point, it is premature to assess the real impact of the measures taken. It seems that the current understanding of service accessibility is not fully adequate for the needs of all people. First and foremost, the issue of people who express a preference to remain offline by choice has still not been addressed. The remedies outlined above are combined with the belief that it is necessary to provide access to the network and its services to people with special needs, which in itself, of course, deserves a positive assessment, but accessibility should be understood here, more broadly, also as the ability to decide to remain offline. This should apply to a situation in which an individual is fully capable of using the internet and the digital services it offers and has the necessary technical conditions, but is not interested in this form of activity. Respecting her choice is closely linked to respecting human freedom and decision-making autonomy, which is at the heart of the modern democratic state. Nonetheless, efforts to promote digital accessibility support those already interested in using the Web and are not combined with any measures to protect the interests of those who would like to preserve their analogue way of living. The reasons for such a decision are irrelevant and should not be subject to assessment by public authorities. Respecting somebody's choice to be offline means, however, seeking to maintain alternative forms of activity alongside the digital ones. In other words, it is crucial to ensure that, as far as possible, any activity or service carried out via the network is also available in an analogue manner. Exclusion from a certain aspect of public life solely because of one's attitudes towards new digital ICT should also be considered as a kind of digital divide.

3. The right not to use the internet as a pertinent argument in combating the digital divide

The concept of the 'right not to use the internet' is a more recent doctrinal idea and has not been explicitly expressed in any modern legal acts. Nonetheless, it may be deduced from the 'classical' human rights and freedoms as a new guarantee necessary for effective protection in the so-called 'digital age'. It has been aptly noted that 'assuming that the non-use of the internet merits protection, human rights might be invoked as a means to protect individuals from the obligation to use the internet […] As the use of the internet could be protected by means of human rights law, it follows that the opposite – its non-use – could too be protected thereby' (Kloza, 2024, p. 3). In other words, a new right not to use the internet – or, at least, some safeguards from digital coercion – may be rightly interpreted from existing human rights law and justify the need to preserve adequate non-virtual space for human activity. In the face of overwhelming digitalisation, though, some reinterpretation of the norma-

tive content of the conventional or constitutional provisions in force seems somehow obvious and desirable from the point of view of the adaptability of human rights law to changing social and technological realities. For example, as freedom of access to new digital services has been recognised as part of the 'classical' freedoms of opinion and expression (Constitutional Council of the French Republic, 2009), it might be justly assumed that the right to information also requires the opposite, which is the maintenance of alternative, non-digital ways of accessing the information and data resources one needs. It therefore seems questionable that if, under Polish law, a given public authority places a piece of public information on a website dedicated to acting as a 'bulletin of public information', such information ceases to be available in an analogue manner (e.g. in writing or orally), even if this is requested by the rightsholder (Wyporska-Frankiewicz, 2023). Furthermore, some commonly adopted conventional or constitutional provisions may also serve as an at least indirect textual anchorage for reconstructing the right not to use the internet. Taking here the example of the existing conventional and constitutional requirements to ensure healthy and hygienic conditions of work, it is rational to argue that such requirements constitute a sufficient legal basis for the so-called 'right to disconnect' (or simply the 'right to be offline'), which is becoming more and more broadly recognised within European legal systems (Vargas-Llave et al., 2020).

Taking, in turn, the right to internet access as an autonomous human right, it may then be argued that the normative content of such a right shall always be viewed in two contexts, positive and negative, as is usually the case for many other fundamental rights and freedoms. Freedom of conscience and religion, for instance, is commonly understood as both freedom 'to' (freely choose) one's own religion, and freedom 'from' (professing) any religion. Similarly, the freedom of association in unions also includes the so-called negative freedom of association, by which is meant the ability to decide not to belong to any trade union without suffering negative consequences because of such a decision. The freedom to choose and pursue a given occupation also inevitably includes the possibility of deciding to change one's current occupation or not to have any; one of the elements of this freedom is, therefore, the freedom to decide simply not to work. From this perspective, the right to internet access, in negative terms, implies a freedom from being forced to make use of the network and the services offered on it. From the point of view of legislative technique, the right not to use the internet would thus require that, on the one hand, a real option for refusing the use of digital means of interaction is provided, and that, on the other hand, an individual willing to benefit from such an option is not subject to any sort of exclusion which would lead to discrimination against him in social, political or economic life. It seems that in terms of guaranteeing the individual's right not to use the internet, there should be both a negative element, in the form of an injunction to respect the decision not to use the internet, and a need for public authorities to take positive action by creating appropriate legal and institutional solutions to pro-

tect those opting out. In other words, public actors cannot be indifferent to non-users of the internet, and alternative solutions must be implemented in the real world.

From this perspective, the right not to use the internet is not merely a negative right, where the task of public authorities would be simply not to interfere with the individual's activity. An effective realisation of such a digital right also implies certain positive actions by public authorities, such as adjusting the legal framework with the purpose of assuring non-digital access to services and products, without any additional barriers for those who would prefer not to use digital tools, in comparison to those acting online. In other words, proper regulation of the right not to use the internet should be combined with the enactment of a programmatic norm that would oblige lawmakers to shape legislation in such a way that making use of digital tools will not be the only option in the future. In doing so, it is desirable to define a long-term strategy for measures to be taken so as to respect somebody's decision to remain offline. Situations when there is no other option than acting via the internet should be absolutely exceptional and proportional. Even in such cases, however, some measures need to be adopted to prevent a digital divide. For instance, some specialised social assistants might be appointed to help digitally excluded persons with accessing services or products which are only available online (Mędrzycki, 2024). Another conceivable solution could be so-called 'Digital Senior Clubs' (*Cyfrowe Kluby Seniora*), which have been opened in Poland since 2022. Different public organisations may seek financial support from the Polish government for creating such clubs in order to increase the digital skills of elderly people and to counteract their digital exclusion (Polish Ministry of Family, Labour and Social Policy, 2022).

Conclusion

One might be tempted to say that remaining offline today is a modern luxury that is increasingly difficult to afford. Reaping the benefits of innovation, however, should be the right of every person, but not an obligation on them to make use of new technological solutions. Offline status is an asset that is not available to everyone, so efforts should be made to protect freedom of choice (Kloza, 2024, p. 5). It is becoming increasingly difficult, if not impossible, to adopt a negative or indifferent attitude towards the phenomenon of universal digitisation without worsening one's situation. It is not a matter of merely guaranteeing the right to remain offline, but of creating a level playing field between those who consciously choose to operate offline and those who prefer to operate online; the choice to remain offline should not be combined with any automatic deterioration of the protection of one's basic rights and freedoms. Bridging the divide between the analogue and the virtual worlds in the area of public life is the current challenge for lawmakers. It should be borne in mind that any revolution – and the so-called 'digital revolution' is no exception – brings profound social

changes, which are usually combined with the emergence of a new social stratification, if only because of different abilities to adapt to new conditions, including digital ones. The new dimension of the general principle of equal treatment emerges precisely in social relations with the virtual world.

Every democratic society should put the need to protect and maximise freedom of choice at the forefront, rather than an obligation to operate in one predetermined way. This is especially important in a time of mass digitisation and the unknown direction of its further development. The possibility of opting for an offline way of life should thus be explicitly promoted. Undoubtedly, the concept of a right not to use the internet may serve as a compelling argument while making policies to counteract digital inequalities and to preserve the fundamental freedom of choice, which includes the freedom to operate offline.

REFERENCES

Allmann, K. (2022). *UK digital poverty evidence review 2022*. Digital Poverty Alliance Community. https://kiraallmann.com/publications/

Best, M. L. (2004). Can the internet be a human right? *Human Rights & Human Welfare*, *4*(1), 23–31. https://digitalcommons.du.edu/hrhw/vol4/iss1/13

Constitutional Council of the French Republic. (2009, 10 June). Decision no. 2009–2580 DC (HADOPI).

Council of Europe Parliamentary Assembly. (2014, 9 April). Resolution 1987 (2014): The Right to Internet Access. https://pace.coe.int/en/files/20870

Council of the European Union. (2003, 18 February). Resolution of 18 February 2003 on the Implementation of the eEurope 2005 Action Plan (O. J. C 48, 28.02.2003).

De Hert, P., & Kloza, D. (2012). Internet (access) as a new fundamental right: Inflating the current rights framework? *European Journal of Law and Technology*, *3*(3). https://ejlt.org/index.php/ejlt/article/view/123

European Commission. (2010, 19 May). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Agenda for Europe. https://eufordigital.eu/library/a-digital-agenda-for-europe/

European Commission. (2021, 11 August). Commission Implementing Decision (EU) 2021/1339 of 11 August 2021 Amending Implementing Decision (EU) 2018/2048 as Regards the Harmonised Standard for Websites and Mobile Applications (O. J. L 289, 12.08.2021).

European Parliament & Council of the European Union. (2002, 7 March). Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services (Universal Service Directive) (O. J. L 108, 24.04.2002).

European Parliament, & Council of the European Union. (2016, 26 October). Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the Accessibility of the Websites and Mobile Applications of Public Sector Bodies (O. J. L 327, 02.12.2016).

European Parliament, & Council of the European Union. (2019, 17 April). Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on The Accessibility Requirements for Products and Services (O. J. L 151, 07.06.2019).

European Parliament, Council of the European Union, & European Commission. (2023). European Declaration on Digital Rights and Principles for the Digital Decade (2023/C 23/01) (O. J. C 23, 23.01.2023).

Eurostat. (2024, December). *Digital economy and society statistics – households and individuals*. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_households_and_individuals

Gomes, S., Lopes, J. M., & Ferreira, L. (2022). The impact of the digital economy on economic growth: The case of OECD countries. *Revista de Administração Mackenzie*, *23*(6), 1–31. https://doi.org/10.1590/1678–6971/eRAMD220029.en

Heeks, R. (2022). Digital inequality beyond the digital divide: Conceptualizing adverse digital incorporation in the global south. *Information Technology for Development*, *28*(4), 688–704. https://doi.org/10.1080/02681102.2022.2068492

International Telecommunication Union. (2024, 27 November). *Measuring digital development: Facts and Figures*, *2024*. https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx

Judgment of the Constitutional Tribunal of the Republic of Poland of 30 July 2014 on the case of *Case Name*, Judgment no. K 23/11.

Kloza, D. (2024). The right not to use the internet. *Computer Law & Security Review*, *52*, https://doi.org/10.1016/j.clsr.2023.105907

La Rue, F. (2011, 16 May). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* (A/HRC/17/27). United Nations Human Rights Council. https://digitallibrary.un.org/record/706331?v=pdf

Marzec, E., & Pietrasiewicz, A. (2020). Commentary on Article 5. In K. Czaplicki & G. Szpor (Eds.), *Ustawa o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych*. LEX/el, https://sip.lex.pl/#/commentary/587810335/607775?tocHit=1&cm=RELATIONS

Mędrzycki, R. (2024). Dostępność cyfrowa i dostęp cyfrowy a wykluczenie społeczne – związki oczywiste i nieoczywiste. In A. Gryszczyńska, G. Szpor, & W. R. Wiewiórkowski (Eds.), *Internet. Solidarność cyfrowa (Digital Solidarity)* (pp. 46–55). C.H. Beck.

Mędrzycki, R. (2025). Commentary on Article 1. In A. Cebera, K. Czaplicki, J. G. Firlus, E. Marzec, M. Szyrski, & R. Mędrzycki (Eds.), *Ustawa o zapewnianiu spełniania wymagań dostępności niektórych produktów i usług przez podmioty gospodarcze. Komentarz.* LEX/el. https://sip.lex.pl/#/commentary/587997959/795399/medrzycki-radoslaw-red-ustawa-o-zapewnianiu-spelniania-wymagan-dostepnosci-niektorych-produktow-i...?cm=RELATIONS

Ministry of Family, Labour and Social Policy of the Republic of Poland. (2022, 2 September). *12 milionów dla Cyfrowych Klubów Seniora*. https://www.gov.pl/web/cyfryzacja/12-milionow-dla-cyfrowych-klubow-seniora

National Telecommunications and Information Administration. (1999). *Falling through the net: Defining the digital divide*. https://www.ntia.gov/sites/default/files/data/fttn99/contents.html

Organisation for Economic Co-operation and Development (OECD). (2001, 1 January). *Understanding the digital divide* [OECD digital economy papers, 49]. http://dx.doi.org/10.1787/236405667766

Ożóg, M., & Puchta, R. (2025). The right not to use the internet: Toward a negative digital freedom in Polish law. In D. Kloza, E. Kużelewska, E. Lievens, & V. Verdoodt (Eds.), *The right not to use the internet: Concept, contexts, consequences* (pp. 92–105). Routledge. https://doi.org/10.4324/9781003528401

Ragnedda, M. (2017). *The third digital divide: A Weberian approach to digital inequalities*. Routledge.

Ragnedda, M., Ruiu, M. L., Addeo, F., Ruiu, G., Pellegrino, D., & Posner, M. (2022). *Living on the edge of digital poverty*. The British Academy. https://www.thebritishacademy.ac.uk/publications/living-on-the-edge-of-digital-poverty/

Saraceni, G. (2020). Digital divide and fundamental rights. *Humanities and Rights Global Network Journal*, *2*(1), 66–91. https://doi.org/10.24861/2675–1038.v2i1.27

Sejm of the Republic of Poland. (2019, 19 July). Ustawa z dnia 19 lipca 2019 r. o zapewnianiu dostępności osobom ze szczególnymi potrzebami [Act on Ensuring Accessibility for People with Special Needs] (Dz.U.2024.1411).

Sejm of the Republic of Poland. (2019, 4 April). Ustawa z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych [Act on Digital Accessibility of Public Entities' Websites and Mobile Applications] (Dz.U.2023.1440).

Sejm of the Republic of Poland. (2024, 26 April). Ustawa z dnia 26 kwietnia 2024 r. o zapewnianiu spełniania wymagań dostępności niektórych produktów i usług przez podmioty gospodarcze [Act on Ensuring the Compliance by Economic Operators with Accessibility Requirements Related to Certain Products and Services] (Dz.U.2024.731).

Statistics Poland. (2024, 21 October). *Information society in Poland in 2024*. https://stat.gov.pl/en/topics/science-and-technology/information-society/information-society-in-poland-in-2024,2,14.html

Susi, M. (2025). Framing the right not to use the internet. In D. Kloza, E. Kużelewska, E. Lievens, & V. Verdoodt (Eds.), *The right not to use the internet: Concept, contexts, consequences* (pp. 44–63). Routledge. https://doi.org/10.4324/9781003528401

Szoszkiewicz, Ł. (2018). Internet access as a new human right? State of the art on the threshold of 2020. *Adam Mickiewicz University Law Review*, *8*, 49–62. https://doi.org/10.14746/ppuam.2018.8.03

Terzis, G. (2025). Ethical meditations for a human right to an analogue life. In D. Kloza, E. Kużelewska, E. Lievens, & V. Verdoodt (Eds.), *The right not to use the internet: Concept, contexts, consequences* (pp. 7–28). Routledge. https://doi.org/10.4324/9781003528401

United Nations, General Assembly. (2006, 13 December). Convention on the Right of Persons with Disabilities. https://social.desa.un.org/issues/disability/crpd/convention-on-the-rights-of-persons-with-disabilities-crpd

United Nations, Human Rights Council. (2012, 5 July). The Promotion, Protection and Enjoyment of Human Rights on the Internet (A/HRC/RES/20/8). https://docs.un.org/A/HRC/RES/20/8

Van Dijk, J. (2020). *The digital divide*. Wiley.

Vargas-Llave, O., Weber, T., & Avogaro, M. (2020, 28 July). *Right to disconnect in the 27 EU member states* [working paper WPEF20019]. Eurofound. https://www.eurofound.europa.eu/en/publications/eurofound-paper/2020/right-disconnect-27-eu-member-states

Wiśniewski, A. (2021). The European Court of Human Rights and internet-related cases, *Białostockie Studia Prawnicze*, *26*(3), 109–133. https://doi.org/10.15290/bsp.2021.26.03.06

World Economic Forum. (2023, 14 August). *Bridging the digital divide in the European Union*. https://www.weforum.org/stories/2023/08/how-to-bridge-the-digital-divide-in-the-eu/

Wyporska-Frankiewicz, J. (2023). Commentary on Article 14. In A. Piskorz-Ryń & M. Sakowska-Baryła (Eds.), *Ustawa o dostępie do informacji publicznej. Komentarz*. LEX/el. https://sip.lex.pl/#/commentary/587931786/803880keyword=Ustawa%20o%20dost%C4%99pie%20do%20informacji%20publicznej.%20Komentarz&tocHit=1&cm=SFIRST

Bialystok Legal Studies
Białostockie Studia Prawnicze
2025 vol. 30 no. 4

sciendo

DOI: 10.15290/bsp.2025.30.04.02

Received: 30.03.2025
Accepted: 05.08.2025

Joanna Wegner
University of Lodz, Poland
jwegner@wpia.uni.lodz.pl
ORCID ID: 0000–0003–2773–6651

The Constitutionalization of the Internet and the Right to Non-Use

Abstract: The author discusses the phenomenon of non-use, defined as a conscious refusal to use the internet, and its constitutional justification. She defends the thesis according to which an individual's decision not to use the internet, and thus electronic communication, may have a constitutional background. It is also discussed that the traditionally understood principle of freedom of form should not be subject to an exception that makes the effectiveness of administrative proceedings dependent on their performance electronically, especially through an ICT system. This constitutionally guaranteed right cannot be hindered by a lack of or deficiency in the necessary statutory regulations. The introduction of a procedural regulation about the right not to use the internet within the laws on administrative and tax proceedings is postulated.

Keywords: constitutionalization, non-use attitude, administrative procedures, proportionality

Introduction

The intensive development of modern technologies and the ubiquity of communication and data transmission have led to a need to introduce regulations dedicated to these issues, although initially the normative order of the internet (as it is called by Kettermann (2020, p. 61)) was a work of interaction between existing regulations and new forms of social activity and accompanying technologies. It can be observed that in this phase of 'digital transition', there was an adaptation through the dynamic interpretation of regulations previously applied only in the analogue world (de Gregorio, 2022, p. 7). Examples of such regulations are primarily provisions of civil law:

on property, in particular intellectual property, on the protection of personal data, or on contracts. Without diminishing the role of global businesses in building the digital world, which has been emphasized in the literature, significance should also be attributed to nation states and their administrations (de Gregorio, 2022, p. 7). While transnational corporations have long recognized the potential of electronic communication and concluding contracts remotely, delivering material goods based on online offers, and multiplying goods and services used exclusively in virtual reality (especially entertainment broadly understood, including computer games), public administration in many countries has only recently begun using the possibilities of the digitalized world. In a sense, public administration is catching up, learning from the experience gained in private companies. As Lessing has aptly noted, the interactions between administrations and businesses are mutual, and as a result of the interpenetration of the private and public spheres, a 'change in the effective architecture of the internet' (2006, pp. 60 is taking place. The aim of this article is to verify the thesis that the concept of non-use has a constitutional basis, allowing for the protection of individuals who do not use modern technologies when dealing with public administration. It has been based on comparative legal, sociological and dogmatic research. In various parts of the text, the terms 'the right not to use the internet', 'freedom from internet use' and 'a non-use attitude' appear. I understand the first two as equivalent, a right to refuse to use the internet and freedom from obligation in this respect, the sources of which I seek in constitutional regulations. I use the term 'non-use attitude' to describe a sociologically interesting behaviour that assumes reluctance or resignation about using the internet.

1. The Digitalization of public life in the light of fundamental rights and freedoms

The development of regulations dedicated to the computerization of public life has caused various consequences in the sphere of individual rights and freedoms, especially fundamental ones. The necessary reaction by the legislature in this situation is described by a concept called 'the constitutionalization of the internet', a 'process by which a constitution is introduced into a legal order, whether domestic, or […] international' (Jamart, 2014, pp. 57). What is more, according to Jamart, 'global constitutionalism embraces the idea that a constitution should govern our globalized world, keeping in mind that the form and substance of such a global constitution may have little to do with that of domestic constitutions. There is a continuum of global constitutionalism visions [including] support for a world government that would resemble domestic governments' (Jamart, 2014, pp. 57–58). Global constitutionalism is described as 'not a comprehensive concept but rather an amalgamation of ideas (key themes), with some thinkers stressing certain features and some thinkers stressing other features of what they be-

lieve would be constitutive of a global constitution' (Schwöbel, 2011, p. 51). The concept refers among other things to 'recognition of individuals' rights' (Schwöbel, 2009, p. 4), and provides useful parameters for evaluating the meaning and significance of the internet's freedom and principles (Jamart, 2014, p. 57).

A question about the effects of this phenomenon on the legal system and the legal situation of the individual naturally arises. It seems particularly interesting to consider whether a non-use attitude towards the internet, which has recently become increasingly common, may also be entitled to constitutional protection. The example of Poland proves that the isolation of the pandemic has become a kind of catalyst for the introduction of new technologies to public administration and the proceedings conducted by it. Previously, the implementation of the option of handling a case online, which was formally available, posed quite a few difficulties for administrations, which rarely initiated actions aimed at launching electronic delivery based on Article 39(1) of the Code of Administrative Procedure (Sejm of Poland, 1960) – a provision in force since 21 November 2005.

Moreover, this provision has been amended many times, proving the helplessness of the legislature in its striving to implement the postulate of the computerization of administration. It was only during the pandemic that a significant change was made to Article 14 of the Code of Administrative Procedure, consisting in the admission of online services, the preparation of documents in electronic form and their automatic generation; this was a result of the addition of paragraphs 1(a)–(d) to this provision, based on Article 61 of the Act of 18 November 2020 on Electronic Delivery (Sejm of Poland, 2020c). The assumption of these regulations was, generally speaking, to limit the personal contact of persons involved in administrative proceedings for health and safety reasons, but without prejudice to the proceedings' course or the identification of individual entities, and ensuring the integrity and confidentiality of the information sent, as well as the reliability and integrity of data sent in both directions. In the same period, the Act of 16 April 2020 on Specific Support Instruments in Connection with the Spread of the SARS-Cov-2 Virus (Sejm of Poland, 2020a) was adopted, with Article 39(3) being added to the Code of Administrative Procedure; this extends the scope of application of ICT (information and communications technology) systems that were previously used to a small extent by the administrative organ (Holtgrewe, 2014, 11–14).

The issue of the digitization of administration has not bypassed EU legal acts, as exemplified by Regulation (EC) no. 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC, Regulation (EU) no. 2024/903 of the European Parliament and of the Council of 13 March 2024 Establishing Measures for a High Level of Public Sector Interoperability within the Union (Interoperable Europe Act), Regulation (EU) no. 2021/694 of the European Parliament and of the Council of 29 April 2021 Establishing the Digital Europe Pro-

gramme and repealing Decision (EU) 2015/2240, and Directive (EU) of the European Parliament and of the Council no. 2016/2102 of 26 October 2016 on the Accessibility of Websites and Mobile Applications of Public Sector Bodies. This issue has also been the subject of discussion in international law for years, both in terms of the potential of new technologies in the service of administration and the protection of universal and free access to the internet (Mayer, 2001; Perritt, 2000; Uepermann-Wirtzack, 2010). The intensive activities of the legislature, directed at human actions on the internet, do not escape issues covered by the subject of the protection of fundamental rights and freedoms. Several important points can be distinguished here.

Firstly, new threats have emerged to these rights and freedoms, as exemplified by interference with the right to privacy, the secrecy of correspondence and even identity theft, as well as violations of property rights through hacks of electronic bank accounts. The not-uncommon cases of mass leaks of the personal data of users of ICT systems, medical information and data on individuals collected by employment offices and by universities are an increasingly serious problem in modern societies (Wittenberg, 2023). Scientists emphasize that the availability of certain methods of ensuring the security of collected data does not guarantee that unlawful takeover of it will not occur (Jałowiecka, 2023). The reported threats necessitate the development of not only new methods of securing data, but also the creation of relevant regulations in the field of public law.

Secondly, as a result of the transferal of part of human activity to the virtual world, the rights of citizens, which were previously only exercised in the analogue world, should now also be available in the online sphere. Here, we can point out the need to ensure the protection of personal rights in connection with online activity, the protection of ownership of digitally available and exercised rights, security of data storage and the circulation of currencies constituting a means of payment on the internet.

Thirdly, the protection of individual rights in the case of disputes about law in the constitutional sense should be subject to implementation in courts. Among the problems that emerge in this area, we can mention the identification of the defendant, because the complexity of the subjective structures of suppliers of various online goods and services as currently created complicates the implementation of the obligation to identify the defendant. The lack of spatial restrictions on activities means that the other party to the contract can be located anywhere in the world, which in turn makes it difficult to find a court competent to resolve any dispute and a law governing the established relationship of obligation, not to mention certain language obstacles or lack of knowledge of foreign law. The diversity and degree of the development of services that may constitute the subject of obligations performed on the internet may additionally complicate the construction of the claim. Regardless of this, the issue of enforcing a judgment that upholds a claim, especially forcibly, appears problematic. One may wonder about the formula for pursuing and realizing redress for damages incurred in connection with virtual activity. This may need moving de-

pending on what exactly is on the internet – it could equally be 'damage on the internet' or 'property on the internet'.

Fourthly, the consequence of the computerization of administration is a modification of the procedural rights and obligations of an individual and of methods of shaping public law relations. Despite the availability of the first regulations in this area, the administrative organ initially had difficulty fulfilling the requests of individuals to put electronic correspondence into circulation, but currently, many administrative proceedings have been transferred to the virtual world in their entirety. The ICT systems used for this purpose allow all procedural activities to be carried out without the need for physical contact between the party to the proceedings and the administrative body. These technologies, which streamline the proceedings and reduce their costs, have proven to be convenient for the administrative organ. Electronic forms have also become popular, standardizing requests and eliminating the applicant's freedom of expression. By excluding the possibility of entering unconventional information or providing additional data that does not fit in the form, the administrative organ automatically avoids difficult cases that deviate from the average (Dudek, 2023). The facilitation and acceleration of proceedings are therefore accompanied by a standardization of their subjects, which in reality could differ. It can therefore be seen that the form procedure may result in an effect where a sort of fiction as to the content of the request is adopted, which is determined by the section of the application. In the current legal system, there are already proceedings being conducted in which communication with the authority takes place exclusively electronically; an example are those in matters of agricultural payments. The freedom to choose the form of application that existed until recently, guaranteed by Article 63(1) of the Code of Administrative Procedure, has been abandoned.

2. The computerization of administrative proceedings and procedural guarantees

In its original wording, the provisions of Article 22(1) and (3) of the Act of 5 February 2015 on Payments under Direct Support Schemes (Sejm of Poland, 2015) provided that applications for payments were to be submitted on a form made available on the agency's website or sent to the farmer if he or she had submitted an application in the previous year. As a result of the amendment made on the basis of Article 1(4) of the Act of 10 January 2018 Amending the Act on Payments under Direct Support Schemes and Certain Other Acts (Sejm of Poland, 2018), the method of submitting applications was reformed, limiting it to a form on the website of the Agency for Restructuring and Modernization of Agriculture. This regulation is still in force, on the basis of Article 17 of the Act of 8 February 2023 on the Strategic Plan for the Common Agricultural Policy for 2023–2027 (Sejm of Poland, 2023). Under the cur-

rent legal regulation, customs law activities, including primarily the submission of declarations and their correction on the basis of Article 173(1) of Regulation (EU) 2013/679 of the European Parliament and of the Council of 9 October 2013 Establishing the Union Customs Code (European Parliament & European Council, 2013), are also made exclusively electronically.

The legislature has therefore adopted the principle in these matters that without access to the internet, understood as technical hardware capabilities or the ability to operate appropriate devices, it is not possible to submit or modify a request to the authority. Transferring certain categories of administrative proceedings to IT systems assumes that the party to such proceedings uses a computer and appropriate software, has access to the internet and uses it. Therefore there is a doubt as to whether imposing such requirements constitutes an excessive restriction on access to proceedings for entities who, for whatever reason, do not use a computer, other electronic devices or the internet. In the current legal system, this problem applies only to proceedings conducted by administrative organs, as opposed to court procedures, within which there is – so far – neither the possibility nor the obligation to conduct electronic communication, nor for the parties to participate in procedural activities in the ICT system. However, the content of regulations relating to administrative proceedings determines the position of a party to court proceedings.

3. Access to administrative proceedings and the exercise of the right to a court hearing

If we are dealing with an individual's dispute about a right examined by administrative organs, the realization of the right to a court hearing, within the meaning of Article 45(1) of the Constitution of the Republic of Poland and thus also Article 6(1) of the Convention on Human Rights and Fundamental Freedoms, depends on the prior exhaustion of administrative proceedings (Judgment of the Constitutional Tribunal, 1998; Judgment of the Constitutional Tribunal, 2000). Since these proceedings are treated as preliminary, any restrictions on access to them must be considered as barriers to initiating a trial. Their admissibility must therefore meet the criteria of the proportionality test, resulting from Article 31(3) of the Constitution of the Republic of Poland. The technical conditions for communication with administrative organs imposed by the legislation may raise constitutional doubts, especially in the reality of the domestic imperfections of the functioning of the internet. One may wonder whether in this aspect the constitutionalization of the internet should be understood as the legislature's obligation to establish a guarantee of universal access to the network without any costs being incurred. If the functioning of the state and its organs in relations with citizens is to take place digitally, one should expect the removal of existing obstacles that are difficult for individuals to overcome.

Since certain elements of functioning in society are implemented exclusively via the internet, it means that this communication channel should be available universally, without exception. Technical obstacles to access to the network still constitute a serious problem. Although, according to statistical data for 2024, 95.9% of households already have access to the internet, at the same time there were as many as 2,482,606 so-called 'next-generation access' white spots, i.e. addresses without an internet service providing a bandwidth of at least 100 MB/s (Minister of Digitalization and Connection Institute, 2024, pp. 5–6, 9). Connecting to a network of sufficient quality to send the necessary data may therefore prove impossible in some locations. Thus the participation of an individual in proceedings conducted via an ICT system may be blocked. Other situations may result from temporary technical difficulties or the failure of the internet, the electrical network that determines the operation of broadband internet, or the mobile network, based on which the so-called mobile internet operates.

The legislature did not decide to provide detailed regulations for cases of this type of disruption or, even more so, its legal consequences, which seems understandable given the variety of causes and circumstances of such events. However, this does not mean that they should automatically have negative consequences for the individual. It should be postulated that, firstly, the administration should bear full responsibility for the proper functioning of the system, and secondly, the citizen should be released from the obligation to prove such events, which are not always fully tangible, and the state of probability should be considered sufficient even in proceedings conducted on the basis of the adversarial principle; an example of this is the procedure regulated in Article 66(2) of the Act of 8 February 2023 on the Strategic Plan for the Common Agricultural Policy for 2023–2027 (Sejm of Poland, 2023) or Article 15(2) of the Act of 10 July 2015 on Supporting the Sustainable Development of the Fisheries Sector with the Participation of the European Maritime and Fisheries Fund (Sejm of Poland, 2020b), in which, regulated by the provision of Article 7 of the Code of Administrative Procedure, the burden of proof was modified in such a way that, following the example of civil proceedings, the proof obligation rests with the person who derives legal consequences from the claim.

The case law of administrative courts seems to protect such a higher level of protection of the procedural rights of an individual. An example of the procedural guarantees of a party to proceedings conducted via an ICT system, understood in this way, is the view contained in the justification of the judgment of the Supreme Administrative Court of 22 January 2025, according to which:

The fact that […] the system remains at the exclusive disposal of the public administration makes it difficult, if not impossible, for the complainant to prove errors or obstacles encountered in using the system. These conditions mean that the appropriate level of guarantee of fair proceedings requires that, in order to challenge the effectiveness of an action performed using an ICT system, it is sufficient to merely

substantiate – instead of prove – the circumstances indicating obstacles in access to or operation of the system.

It can be added that the exclusion of the obligation to apply the provision of Article 7 of the Code of Administrative Procedure – as is sometimes the case in separate proceedings – and the limitation by law of the principle of objective truth derived from this provision to the obligation to assess the collected evidence cannot lead to releasing the administrative organ from the proper organization of the proceedings or to going beyond the limits of the law as stated in Article 7 of the Constitution. In the principle of legalism resulting from this provision, I would see the constitutional sources of procedural guarantees also carried out within the ICT system.

Apart from the problems of technical accessibility, obstacles to using the internet include the non-use attitude presented by part of society. This consists of a conscious refusal to use the internet despite having the technical possibility. The risks indicated above related to the imperfection of technology, possible disruptions in its functioning and uncertainty of the effects of such events, as well as the high level of complexity and the lack of uniformity of legal regulations, may cause a – justifiable, it seems – reluctance on the part of an individual to use IT tools, including in relations with the administrative organs or courts.

4. The phenomenon of non-use and its causes

The heterogeneity of reasons for individuals to stop connecting to the internet has already been noted in scholarship, including choosing a negative attitude towards for the internet, for example dictated by a need for an 'internet detox', protection against access to information offered on the internet or lack of sufficient financial possibilities or skills (Kloza, 2024, p. 3). Sociological studies conducted in European countries have shown that the reasons for not using the internet are indeed complex and go beyond superficial associations. Since access to this medium is possible regardless of social status, then giving up using it should be associated with other factors.

It has been shown that people who are in a worse personal, social or economic situation than the average citizen tend to be less involved in using modern information and communication technologies (Helsper & Reisdorf, 2013, p. 94).[1] A certain stereotype has also been verified, according to which men are more interested in and familiar with using the internet. As it turns out, more frequent access to new technologies by men – usually for professional reasons – is a significant factor increasing

1 According to statistics, around 7 million Britons have never used the internet. Today, 5% of the population remains offline, which is around 2,8 million (Petrosyan, 2024). In Poland, about 12% of the population does not use the internet, although it is estimated that this is over 4,000,000 inhabitants, because official statistical publications take into account the number of inhabitants of a given territory, not the citizens of a given country (All 4 Comms, 2024; Kemp, 2024; Sas, 2025).

their share among people over 65 who use the internet. It has also been proven that in this age group and older, using the internet is more frequent in the case of users living together with other people. Loneliness is therefore a factor that reduces the level of interest in the internet (van Deursen & Hellsper, 2015).

The reason for a reluctance to use the internet is not one's level of wealth, but primarily, in 50% of cases, because of lack of interest, as scientists from Oxford have shown based on a representative 2,057 surveys completed by people aged 14 and older. Among those who do not use the internet, issues such as lack of access or skills or concerns about costs were mentioned next. These gained importance only in the case of people who gave up using the internet (so-called ex-users), but not in relation to people who have never done so (so-called non-users). It is worth emphasizing that the obstacle of lack of access, revealed by younger people, disappeared among older people, who emphasized the problem of insufficient skills. People who were lonely or shy were definitely more absorbed in access to the internet, and they saw barriers in free access to the network rather than other factors (Helsper & Reisdorf, 2013, p. 95).

The problem of lack of interest occurs particularly in societies where access to the internet is common. In Sweden, where 95% of the population has the opportunity to use it, over 62% of users over the age of 66 give up this medium. Lack of interest also occurs regardless of the level of wealth of the society. It has even been observed in Switzerland, considered a wealthy country, where the internet is treated as a common good (Kappeler et al., 2020, pp. 7–9). The concept of lack of interest is capacious and can mean a real lack of willingness to reach for the possibilities created by the internet, as well as fully understandable fears of increasingly aggressive cybercrime or violations of privacy, or the increasingly well-described phenomena of information overload and other stimuli from electronic media, information smog (Tadeusiewicz, 1999, p. 97), disinformation, a state of overstimulation dangerous to human health (Rarot & Wójcik, 2023) or increasingly better and more frequently diagnosed electrosensitivity (Belpomme & Irigaray, 2020; Röösli et al., 2010). As it turns out, the benefits of the mass flow of data and information often conceal threats that science is only just discovering and exploring, and it is difficult to fully define them at the moment.

The paradox is that – as sociologists have proven – an obligation to use internet communication, the fulfilment of which could serve to facilitate access to administrations for individuals who are limited to some extent in handling their matters in person, i.e. elderly people, those isolated due to various personality problems, those with disabilities, or those who are shy and withdrawn, may intensify the state of exclusion of those who have already been affected by unfavourable socio-economic patterns and negative attitudes towards the internet. Therefore the computerization of administration should be accompanied by an effort to equalize differences between individuals. Otherwise, the consequence of increasing the reach of computerized administration would be a deepening of the social stratification between the information elite and the digital underclass (Kappeler et al., 2020, p. 9). More educated people

use the internet more often than those who remain less educated (van Deursen & Helsper, 2015, pp. 185–186), and acquiring the missing knowledge and skills in later life undoubtedly becomes more difficult. There are still individuals in society for whom this is a difficult barrier to overcome.

The reasons for presenting a non-use attitude are diverse. Analysis of sociologists' views and statistical data, as well as applicable law, proves that the reasons for reluctance to use the internet in modern society are concerns about the protection of one's health or emotional state, protection against cybercrime, the security and integrity of data transmitted on the internet, disinformation and reducing the risk of using devices and systems without sufficient skills, as well as avoiding cases of disruption in the functioning of modern technologies and devices. At least some of the circumstances listed are justified by the content of fundamental freedoms and rights as subject to constitutional protection.

5. Legal protection for those who do not use the internet

It is enough to refer to the provisions of Articles 47, 51(1) and 68 of the Constitution, which guarantee the protection of personal health, the security of personal data and the privacy of an individual, to confirm the thesis about the constitutional reinforcement of the non-use attitude in relations with public administrations. I therefore believe that the right to non-use, or more precisely freedom from using the internet, is not an independent human right that would require the intervention of the legislature, but is a derivative of existing rights and freedoms, while remaining determined by the conscious choice of the individual and therefore dependent on the accompanying individual motivation (which is not necessarily revealed externally) (Kloza, 2024, p. 3).[2]

The legislature is obliged to shape the legal system in such a way that the right to protect constitutionally secured values can be implemented. An example of a legal solution that can serve this purpose is the one adopted in the Act of 19 July 2019 on Ensuring Accessibility for People with Special Needs (Sejm of Poland, 2024). Article 6(3)(d) of this Act establishes the obligation of administrative organs to provide assistance to a person who does not have sufficient skills or technical capabilities, and even to organize communication with a person with special needs in the form specified in their application. This provision specifies the minimum requirements for ensuring accessibility for people with special needs, which are included in the scope of information and communication accessibility, among other things, and which ensure, at the request of the person with special needs, communication with a public entity in the form specified in the application. The category of a person with special needs includes any person who, due to their external or internal characteristics, or

2 Kloza also emphasizes the view which assumes the development of a separate human right in parallel with the content of the freedom I have described.

due to the circumstances in which they find themselves, must take additional actions or apply additional measures in order to overcome a barrier in order to participate in various spheres of life on an equal basis with other persons. Assuming that the non-use attitude constitutes one of the listed internal characteristics of an individual, such a person should be classified in the category of persons entitled to the treatment guaranteed in the above-mentioned provision. The cited regulation does not correspond to the relevant procedural provisions, because neither the provisions of the Code of Administrative Procedure nor the acts regulating separate administrative proceedings or proceedings not bearing the characteristics of a jurisdictional-type procedure contain appropriate regulations that take into account respect for the right resulting from the provision of Article 6(3)(d) of the Act within the framework of administrative proceedings.

Conclusion

The constitutional basis of the non-use attitude leads to the conclusion that it is necessary to introduce appropriate regulations into the code-level regulations (i.e. the Code of Administrative Procedure and the Tax Ordinance) that guarantee the individual the right to participate in proceedings without the need to use the internet. Moreover, the traditionally understood principle of freedom of form should not be subject to an exception that makes the effectiveness of the proceedings dependent on their performance electronically, especially through an ICT system. In the current legal status, such regulations are already in force, as exemplified by the aforementioned Article 17 of the Act of 8 February 2023 on the Strategic Plan for the Common Agricultural Policy for the years 2023–2027, raising doubts as to compliance with the provisions of the Constitution. Since the exercise of a constitutionally guaranteed right cannot be hindered by a lack of or a deficiency in the necessary statutory regulations, one may wonder about the effects of an individual's formulation before a court of an allegation of defectiveness of the regulation that obliges participation in administrative proceedings using the internet. This problem will probably have to be faced by the administrative courts if non-users decide to consistently defend the validity of their attitude by initiating disputes with administrations. Only *ad casu* can the reasons emerge that require deliberation when considering the validity of imposing the obligation to communicate electronically on an entity in a specific category of proceedings. The constitutionalization of the non-use attitude also means that the validity of its expression should be subject to analysis in the context of the criteria for the admissibility of proportionate restrictions on constitutional rights and freedoms established in the provision of Article 31(3) of the Constitution. It seems that while the legislation may require an entrepreneur to communicate electronically, the act should guarantee other entities the possibility of at least equivalent contact in a analogue form.

REFERENCES

All 4 Comms. (2024, 24 April). *Social media in Poland – marketing statistics to know in 2024*. https://all-4comms.com/social-media-in-poland-marketing-statistics-to-know-in-2024 (URL)

Batko, K., & Billewicz, G. (2013). E-usługi w biznesie i administracji publicznej. *Studia Ekonomiczne*, *136, pp. 47–63;*.

Belpomme, D., & Irigaray, P. (2020). Electrohypersensitivity as a newly identified and characterized neurologic pathological disorder: How to diagnose, treat, and prevent it. *International Journal of Molecular Sciences*, *21*, 1–20.

de Gregorio, G. (2022). *Digital constitutionalism in Europe: Reframing rights and powers in the algorithmic society*. Cambridge University Press.

Dudek, M. (2023). *Administracyjne postępowanie uproszczone*. C.H. Beck.

European Council and European Parliament. (2013, 9 October). Regulation Establishing the Union Customs Code ((EU) 2013/679) (Journal of Laws, UE L.2013.269.1).

European Parliament. (2014, 23 July). Regulation (EC) no. 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC (Journal of Laws, UE L.2014.257.73).

European Parliament. (2016, 26 October). Directive (EU) no. 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the Accessibility of Websites and Mobile Applications of Public Sector Bodies (Journal of Laws, UE L.2016.327.1).

European Parliament. (2021, 29 April). Regulation (EU) no. 2021/694 of the European Parliament and of the Council of 29 April 2021 Establishing the Digital Europe Programme and Repealing Decision (EU) 2015/2240 (O. J. EU L.2021.166.1).

European Parliament. (2024, 13 March). Regulation (EU) no. 2024/903 of the European Parliament and of the Council of 13 March 2024 Establishing Measures for a High Level of Public Sector Interoperability Within the Union (Interoperable Europe Act) (Journal of Laws, UE L.2024.903).

Gov.pl. (2023, 29 November). *Największy wyciek danych medycznych w Polsce. Sprawdź, czy Twoje dane też wykradziono*. https://www.gov.pl/web/baza-wiedzy/najwiekszy-wyciek-danych-medycznych-w-polsce-sprawdz-czy-twoje-dane-tez-wykradziono

Helsper, E. J., & Reisdorf, B. C. (2013). A quantitative examination of explanations for reasons for internet nonuse. *Cyberpsychology, Behaviour, and Social Networking*, *2, pp. 94–99*.

Holtgrewe, U. (2014), New new technologies: The future and the present of work in information and communication technology. *New Technology, Work & Employment*, *29*(1), 9–24.

Jałowiecka, A. (2023). Wyciek danych z systemu teleinformatycznego na przykładzie działalności wybranych organów administracji publicznej. *Prawo Mediów Elektronicznych*, *1*, 4–11.

Jamart, A. C. (2014), *Internet freedom and the constitutionalization of internet governance* iIn R. Radu, J.-M. Chenou, & R.H. Weber (Eds.), Evolution of Global Internet Governance. Principles and Policies in the Making (pp. 57–76). Heidelberg: Springer. https://doi.org/10.1007/978–3-642–45299-4_4

Judgment of the Constitutional Tribunal of 9 June 1998, K 28/97.

Judgment of the Constitutional Tribunal of 10 July 2000, SK 12/99.

Judgment of the Supreme Administrative Court of 22 January 2025, I GSK 1042/21.

Kappeler, K. Festic, N., & Lanzer, M. (2020). Who remains offline and why? Growing social stratification of internet use in the highly digitized Swiss society. *Media Change & Innovation*, *10*. pp. 1–30

Kemp, S. (2024, 23 February). *Digital 2024: Poland*. DataReportal. https://datareportal.com/reports/digital-2024-poland (URL)

Kettermann, M. C. (2020). *The normative order of the internet: A theory of rule and regulation online*. Oxford University Press.

Kloza, D. (2024). The right not to use the internet. *Computer Law & Security Review: The International Journal of Technology Law & Practice*, *52*.

Koenig C. *Vorlesung allgemeines Verwaltungsrechteinschließlich Verwaltungsprozessrecht*. https://www.docsity.com/de/docs/skript-allgemeines-verwaltungsrecht-mit-verwaltungsprozessrecht-teil-verwaltungsverfahrensrecht/5730371/, pp. 13–32.

Konieczna, K. (2024). Miejsce powstania szkody jako podstawa jurysdykcji szczególnej dla roszczeń o naprawienie szkody doznanej w związku z rozpowszechnianiem w Internecie dyskredytujących wypowiedzi. *Gdańskie Studia Prawnicze*, *3*. Pp. 189–200

Lessing, L. (2006). *Code Version 2.0*. http://www.codev2.cc/download+remix/Lessig-Codev2.pdf

Mayer, F. C. (2001). Review essay: The internet and public international law – worlds apart? *European Journal of International Law*, *12*, 617–622.

Minister of Digitalization and Connection Institute. (2024). *Polska w zasięgu stacjonarnego dostępu do internetu*. https://www.gov.pl/web/cyfryzacja/juz-jest-sprawdz-nowy-raport-polska-w-zasiegu-z-danymi-z-internetgovpl

Perritt, H. H. (2000). The internet is changing the public international legal system. *Kentucky Law Journal*, [*VOLUME 88*], 2–50.

Petrosyan, A. (2024, 4 March). *Share of individuals using the internet in the United Kingdom (UK) from 2002–2024*. Statista. https://www.statista.com/statistics/1124328/internet-penetration-uk

Podgórecki, A. (1962). *Charakterystyka nauk praktycznych*. PWN.

Radu, R., Chenou J.-M., & Weber, R. H. (2014). *The evolution of global internet governance principles and policies in the making*. Springer.

Rarot, H., & Wójcik, T. (2023). Kryzys informacyjny i milczenie w perspektywie filozoficzno-kulturowej. *Kultura i Wartości*, *35*, 59–79.

Romaniuk, P. (2019. *Wyzwania stawiane administracji publicznej w zakresie rozwoju e-usług*. In Z. Duniewska & Rabiega (Eds.), *Standardy współczesnej administracji i prawa administracyjnego* (pp. 271–282).

Rööslia, M., Mohlera, E., & Frei, P. (2010). Sense and sensibility in the context of radiofrequency electromagnetic field exposure. *Comptes rendus physique*, *11*, 576–584.

Sas, A. (2025, 19 June). *Number of internet users in Poland from 2016 to 2024*. Statista. https://www.statista.com/statistics/955204/poland-internet-users, pp. 1 – 55

Schwöbel Ch (2011), Global Constitutionalism in International Legal Perspective

Sejm of Poland. (1960, 14 June). Act of 14 June 1960: Code of Administrative Procedure (Journal of Laws of 2024, item 572).

Sejm of Poland. (2015). Act of 5 February 2015 on Payments under Direct Support Schemes (Journal of Laws of 2015, item 308).

Sejm of Poland. (2018). Act on Payments under Direct Support Schemes and Certain Other Acts (Journal of Laws of 2018, item 311).

Sejm of Poland. (2020a). Act of 16 April 2020 on Specific Support Instruments in Connection with the Spread of the SARS-Cov-2 Virus (Journal of Laws of 2020, item 695).

Sejm of Poland. (2020b). Act of 10 July 2015 on Supporting the Sustainable Development of the Fisheries Sector with the Participation of the European Maritime and Fisheries Fund (Journal of Laws of YEAR, item 2140).

Sejm of Poland. (2020c). Act of 18 November 2020 on Electronic Delivery (Journal of Laws of 2022, item 569).

Sejm of Poland. (2023). Act of 8 February 2023 on the Strategic Plan for the Common Agricultural Policy for 2023–2027 (Journal of Laws of 2020, item 1741).

Sejm of Poland. (2024). Act of 19 July 2019 on Ensuring Accessibility for People with Special Needs (Journal of Laws of 2024, item 1411).

Tadeusiewicz, R. (1999). Smog informacyjny. *Polska Akademia Umiejętności, Prace Komisji Zagrożeń Cywilizacyjnych*, *2, pp. 97–107*.

Uerpmann-Wittzack, R. (2010). Principles of international internet law. *German Law Journal*, *11*, 1245–1263.

van Deursen, A., & Hellsper, E. (2015). A nuanced understanding of internet use and nonuse among the elderly. *European Journal of Communication*, *30*, 171–187.

Wegner, J. (2020). Konstrukcja subsydiarnego stosowania przepisów kodeksu postępowania administracyjnego. *Państwo i Prawo*, *6, pp. 85–101*.

Wilbrandt-Gotowicz, M. (Ed.). (2021). *Doręczenia elektroniczne. Komentarz.* Wolters Kluwer, S. A.

Wittenberg, A. (2023, 28 November). *Gigantyczny wyciek danych medycznych. Przestępcy ujawnili dane pacjentów Alabu.* Gazeta Prawna. https://www.gazetaprawna.pl/wiadomosci/kraj/artykuly/9365021, gigantyczny-wyciek-danych-medycznych-przestepcy-ujawnili-dane-pacjent.html

Bialystok Legal Studies
Białostockie Studia Prawnicze
2025 vol. 30 no. 4

sciendo

DOI: 10.15290/bsp.2025.30.04.03

Received: 15.04.2025
Accepted: 05.08.2025

Iwona Wrońska
University of Bialystok, Polska
wronska@uwb.edu.pl
ORCID ID: 0000–0002–8945–3545

Ewelina Cała-Wacinkiewicz
University of Szczecin, Polska
ewelina.cala-wacinkiewicz@usz.edu.pl
ORCID ID: 0000–0002–5439–4653

Maciej Nyka
University of Gdansk, Polska
maciej.nyka@prawo.ug.edu.pl
ORCID ID: 0000–0003–0786–7785

Prawo dostępu do Internetu, prawo do niekorzystania z Internetu i prawo do bycia offline a prawo do prywatności – czy multiplikacja praw człowieka jest remedium na ich efektywność?

The Right to Access the Internet, the Right Not to Use the Internet, the Right to Be Offline and the Right to Privacy: Is a Multiplication of Human Rights a Remedy for Their Effectiveness?

Abstract: The research objective of this study is to address the need for scientific interest in categories that are somewhat overshadowed by analyses dedicated to internet access, namely the categories of not using the internet and being offline, and their possible conceptualisation within the framework of the next human rights, in order to then refer to the longer history of human rights and the established status of the right to privacy. The leading research perspective is that of human rights, which has allowed important questions to be asked in the context of the intensifying phenomenon of the multiplication of rights. In this context, is moving towards a standardisation of the right to access the internet, the right not to use the internet and the right to be offline justified and, as such, is it confirmed in the axiologically conditioned protective function of law? Does the multiplication of rights not undermine the effective-

ness of their protection mechanisms and obliterate the values underlying them and the scope of their protection? Should the well-established right to privacy shape the content of the right to access the internet, or on the contrary the right not to use the internet or the right to be offline, even if one wants to recognise them as having a postulatory character *de lege lata*?

Key words: internet access, right to be offline, multiplication of human rights
Słowa kluczowe: dostęp do Internetu, prawo do bycia offline, multiplikacja praw człowieka

Wprowadzenie

Jeśli postulat zakodowany w łacińskiej paremii *ius sequitur vitam* – prawo podąża za życiem – chcieć zapatrzeć w naukowo determinowaną egzemplifikację, jednocześnie postrzegając Internet jako zjawisko społeczne, to nie sposób nie dostrzec, że dynamicznie zmieniające się uwarunkowania społeczno-kulturowe kształtują poszczególne dziedziny życia i obszary regulacji, w tym również – a może i przede wszystkim – przestrzeń funkcjonowania Internetu i dostępu do niego.

Współcześnie nie da się nawet zaryzykować twierdzenia, że wpływ technologii czy w innym ujęciu transformacji cyfrowej pozostaje w swoistym oderwaniu od praw człowieka, które, immanentnie sprzęgając się ze społecznym aspektem funkcjonowania jednostki w społeczeństwie, wyznaczają pewien standard w tym zakresie. Wspomniany społeczny kontekst uwidacznia się chociażby w założeniu, że „prawa społeczne domagają się aktywnego zaangażowania państwa w ich urzeczywistnianie, że realizowane są poprzez działalność państwa" (Mazurek, 1982, s. 209), co w kontekście zapewnienia dostępu do Internetu zdaje się mieć fundamentalne znaczenie. Jeśliby bowiem ów dostęp wyposażyć w walor efektywności i ująć go w normatywne ramy prawa dostępu do Internetu (czy symplifikując prawa do Internetu), to *de lege lata* pewne uzasadnienie ku temu odnaleźć można jedynie w *soft law* oraz w orzecznictwie dotyczącym praw człowieka w kontekście kategorii dostępności jako takiej, o czym dalej. I choć prawu dostępu do Internetu doktrynalnie przypisuje się niekiedy status samodzielnego prawa człowieka, które wyszło z etapu konceptualizacji i wkroczyło w etap normatywizacji (Zieliński, 2013, s. 20–21), zaś z jego istoty wywodzi się takie nowe prawa, jak chociażby prawo do niekorzystania z Internetu czy nawet prawo do bycia offline, to w kontekście praw podmiotowych warto pamiętać, że konstrukcyjnie z prawem jednego podmiotu korelatywnie sprzężony musi zostać ciążący na innym podmiocie obowiązek (Hohfeld, 1923, s. 50). Owa korelacja nadaje prawom, w tym prawom nowo powstającym, pożądaną skuteczność, osadzając je na gruncie koncepcji praw podmiotowych jako takich. Czy z taką sytuacją mamy do czynienia w kontekście tytułowych praw?

Analiza mającej za sobą liczną i wielokontekstową literaturę przedmiotu kategorii dostępu do Internetu – a niekiedy – choć rzadziej – i prawa do Internetu – nie stanowi jednak celu niniejszych analiz, mimo tego, że z pewnością jest ona swoistym *signum temporis*, swojego największego sojusznika odnajdując w transformacji cyfro-

wej. Na gruncie prawodawstwa Unii Europejskiej transformację tę odważnie ujmuje się w ramy suwerenności cyfrowej, zapewniającej poszanowanie praw podstawowych, praworządność i demokrację, ale także takie kategorie – warte podkreślenia m.in. w kontekście dostępu do Internetu – jak włączenie, równość, zrównoważony rozwój, odporność, bezpieczeństwo czy tak istotną poprawę jakości życia i dostępności usług (Parlament Europejski i Rada, 2022; Komisja Europejska, 2021). Dlatego też celem badawczym niniejszego opracowania uczyniono potrzebę dowartościowania naukowym zainteresowaniem kategorii, które niejako pozostają w cieniu analiz poświęconych dostępowi do Internetu, a mianowicie kategorii niekorzystania z Internetu i bycia offline i odpowiednio ich ewentualnej konceptualizacji w ramy kolejnych praw, po to, by następnie odnieść się do mającego dłuższą historię prawno-człowieczą i ugruntowany status prawa do prywatności. Zastrzec przy tym trzeba, że wiodącą perspektywą badań jest perspektywa prawno-człowiecza, determinująca ich zakres. Jakiekolwiek analizy poświęcone kategorii dostępu do Internetu nie powinny zatem abstrahować od kategorii niekorzystania z Internetu i bycia offline nie tylko z powodu *explicite* wpisania w nie każdorazowo świadomego wyboru jednostki, ale nade wszystko zderzenia ich z założeniami transformacji cyfrowej. Uwidaczniająca się w niej nierówność stron (tj. z jednej strony państw dążących do realizacji założeń transformacji, z drugiej jednostek, „zmuszonych" się jej poddać), ale przede wszystkim podyktowana rozwojem technologicznym ewentualna multiplikacja praw człowieka – rozumiana jako namnożenie owych praw – stanowić może formę swoistej reaktywności na ów rozwój. Spostrzeżeniu temu nadano formę hipotezy badawczej, w której zakodowano przypuszczenie, że przy nieuchronnie realizowanych przez państwa założeniach transformacji cyfrowej, bez regulacji prawnych dotyczących zarówno dostępu do Internetu, niekorzystania z Internetu, jak i bycia offline, jednostka nie będzie skutecznie chroniona. Jeśli – idąc dalej tym tokiem – przypisać słuszność temu stwierdzeniu, to czy w kontekście zauważalnego i nasilającego się zjawiska multiplikacji praw człowieka pójście w stronę normatywizacji odpowiednio prawa dostępu do Internetu, prawa do niekorzystania z Internetu i prawa do bycia offline jest uzasadnione i jako takie znajduje potwierdzenie w aksjologicznie warunkowanej funkcji ochronnej prawa? Czy zatem – będąca pewnym stanem, procesem i zjawiskiem – multiplikacja praw człowieka nie osłabia efektywności mechanizmów ich ochrony poprzez zacieranie się wartości leżących u ich podstaw, zakresowo objętych ochroną? I – zwłaszcza w kontekście roszczenia jednostki o ochronę przez państwo takowych praw – czy prawo do prywatności, mające swój ugruntowany status, nie powinno kształtować treści prawa dostępu do Internetu, *a contrario* prawa do niekorzystania z Internetu czy prawa do bycia offline, nawet jeśli chcieć uznać je za mające *de lege lata* postulatywny charakter?

Weryfikacja wskazanej hipotezy możliwa będzie poprzez zastosowanie metody analitycznej oraz formalno-dogmatycznej. Jej konfirmacja bądź falsyfikacja, ukierunkowana powyżej sformułowanymi problemami, nie tylko wyznaczy zakres analiz, ale

nade wszystko umożliwi odniesienie tytułowych kategorii do autonomicznego wyboru jednostki, ukazując, jaki skutek w tym obszarze może odnieść multiplikacja praw człowieka i czy więcej to zawsze korzystniej. Biorąc to za podstawę, celowo zaproponowano nieco prowokacyjny tytuł niniejszego opracowania, mający ukazać nasilającą się tendencję do multiplikacji praw związanych z Internetem. Czy szansą na efektywną ochronę jednostki w wyznaczonym obszarze będzie wielość nowo powstających praw?

1. Od prawa dostępu do Internetu do prawa niekorzystania z Internetu

W perspektywie prawno-naturalnej prawa człowieka przysługują każdemu człowiekowi już z samego faktu bycia człowiekiem, opierając się na jego godności osobowej. Jednak współcześnie postrzeganie praw człowieka uzależnione jest także od aspektów geograficznych, kulturowych czy religijnych, a coraz częściej także technologicznych, takich jak Internet (Brzozowski, 2023, s. 31-–32). W ujęciu tym ewolucyjny katalog praw człowieka zaprzecza prawno-naturalnej tezie o zupełnej niezależności praw człowieka od uznania zewnętrznego (Brzozowski, 2023, s. 31–32). Powszechnie przyjmuje się, że zdolność jednostki do wykonywania podstawowych codziennych zadań i korzystania z podstawowych praw człowieka zależy w dużej mierze od dostępu do Internetu (Wong, 2023, s. 1–3). Jeśli ów dostęp zamknąć w ramy prawne i stwierdzić, że jest on od dawna przedmiotem analiz doktryny praw człowieka, to wśród naukowców nadal nie ma zgody, co do tego, czy nastąpiła konceptualizacja dostępu do Internetu i jaki miałby być ewentualny status prawa dostępu do Internetu (Gosztonyi, 2020, s. 134–140; Mladenov et al., 2023, s. 205–213; Qerimi, 2017, s. 1–22; Reglitz, 2020, s. 314–331; Szoszkiewicz, 2018, s. 49–62). Czy zatem *de lege lata* uprawnione jest konstytuowanie prawa dostępu do Internetu czy raczej poszukiwanie uzasadnienia dla jego samodzielności uznać należy za przedwczesne?

W piśmiennictwie zasadniczo podkreśla się, że prawo do Internetu nie zostało wyrażone wprost w żadnym wiążącym akcie prawa międzynarodowego, a społeczność międzynarodowa nie ustaliła normatywnej treści tego nowego prawa (Pollicino, 2020, s. 263–275; Szoszkiewicz, 2018, s. 59). Rozbieżności co do statusu prawa dostępu do Internetu w piśmiennictwie ujmowane są zatem z jednej strony w argument, że jest ono podstawowym prawem człowieka, opartym na idei równych szans dla wszystkich członków społeczeństwa (Estrada, 2020, s. 15–24; Gosztonyi, 2020, s. 139; Jasmontaite & De Hert, 2020, s. 15–17; Mladenov & Staparski, 2022, s. 25–34; Stępniak, 2017, s. 65). Z drugiej zaś uznaje się, że dostęp do Internetu „nie jest prawem, ale instrumentem (czynnikiem) umożliwiającym korzystanie z praw człowieka" (Malinowski, 2020, s. 23–30; Milczarek, 2023, s. 157–159; Oyedemi, 2015, s. 2). Jeśliby chcieć dowieść prawdziwości pierwszego ze wskazanych podejść, to pamiętać należy, że każde prawo podmiotowe (jako pewien swoisty miernik możliwego zacho-

wania jednostki, uznany i zapewniony przez państwo poprzez prawnie ustanowiony system gwarancji) ma co najmniej dwa obowiązkowe atrybuty: własną treść prawną jako zbiór określonych uprawnień – dopuszczalnych działań, które mogą być wykonane przez podmiot korzystający z tego prawa, oraz własny mechanizm realizacji, czyli zbiór gwarancji zapewniających realizację prawa, pożądany rezultat wykonywania prawa przez jakikolwiek zainteresowany podmiot (Mochalov et al., 2021, s. 138). Ustalenie wskazanych atrybutów jawi się zatem jako warunek *sine qua non* jakichkolwiek analiz poświęconych ujmowaniu dostępu do Internetu w normatywne ramy.

Tymczasem prawo dostępu do Internetu nie zostało zakotwiczone w systemie międzynarodowego prawa praw człowieka. Oznacza to, że żaden wiążący państwa akt prawno-człowieczy nie wyraził *explicite* tego prawa, a brak standardów traktatowych przesuwa ciężar regulacyjny w stronę co najwyżej *soft law*. Egzemplifikując, w pracach organizacji międzynarodowych widoczny jest trend ujmowania dostępu do Internetu jako instrumentu służącego realizacji poszczególnych praw i wolności człowieka, co przekłada się na doktrynalne dość śmiałe próby ujęcia owego dostępu jako prawa człowieka. Przykładowo, dostęp do Internetu przywołał Specjalny Sprawozdawca Rady Praw Człowieka już w 2011 r. w Raporcie dotyczącym wspierania i ochrony prawa do wolności opinii i ekspresji (Human Rights Council, 2011). Podkreślił on znaczenie Internetu jako kluczowego narzędzia, poprzez które jednostki realizują prawo do swobodnego wyrażania opinii i ekspresji, zawarte w art. 19 Powszechnej Deklaracji Praw Człowieka z 1948 r. czy w art. 19 Międzynarodowego Paktu Praw Obywatelskich i Politycznych (dalej jako: MPPOiP) z 1966 r. (Zieliński, 2013, s. 17). Raport ten wywołał ożywioną dyskusję w przestrzeni publicznej, w toku której przesądzająco zaczęto twierdzić, że „ONZ ogłasza dostęp do Internetu prawem człowieka", co jednak na płaszczyźnie racjonalnej argumentacji prawniczej stanowi postulat przedwczesny (Estes, 2011, s. 1). Trudno bowiem w kontekście dostępności i konieczności jej zapewnienia skutecznie dowieść istnienia prawa dostępu do Internetu jako takiego. W 2012 r. Rada Praw Człowieka ONZ przyjęła Rezolucję w sprawie wspierania, ochrony i korzystania z praw człowieka w Internecie, podkreślając, że prawa przysługujące jednostkom poza Internetem powinny być chronione również w przypadku, gdy korzystają one z Internetu, co szczególnie dotyczy swobody ekspresji (Human Rights Council, 2012). Rola dostępu do Internetu, jeśli chodzi o korzystanie z wolności ekspresji, została już wcześniej podkreślona w pracach Komitetu Praw Człowieka ONZ, który w przyjętym w czerwcu 2011 r. komentarzu nr 34 do art. 19 MPPOiP potwierdza, że Internet oraz inne środki komunikacji audiowizualnej i elektronicznej należą do instrumentów korzystania z wolności ekspresji (Human Rights Committee, 2011; Zieliński, 2013, s. 16). Nie można zatem negować, że podkreślenie znaczenia dostępu do Internetu jako warunku korzystania z praw człowieka ma swoją doniosłość. Jednak przesunięcie wektora argumentacji w stronę konceptualizacji prawa dostępu do Internetu nie znajduje uzasadnienia ani w obowiązującym prawie z zakresu ochrony praw człowieka, ani nawet w *soft law* z tego obszaru.

Poglądu tego nie osłabia jednostkowe twierdzenie, dające się wyinterpretować z Raportu Przedstawiciela Organizacji Bezpieczeństwa i Współpracy w Europie ds. Wolności Mediów z 2011 r., który zaproponował, by w związku ze znaczeniem Internetu w zakresie swobody ekspresji oraz udziału w społeczeństwie informacyjnym dostęp do niego został uznany za podstawowe prawo człowieka (Organization for Security and Co-operation in Europe, 2010).

Podobny kontekst znaczeniowy nadaje się dostępowi do Internetu w Radzie Europy, na kanwie definiowania pojęcia mediów. W Deklaracji politycznej z 9 maja 2009 r. uznano, że z racji powszechnego wykorzystywania Internetu dostęp do niego wiąże się bezpośrednio z korzystaniem z praw człowieka i podstawowych wolności (Council of Europe, 2009). Od 2012 r. Rada Europy, konsekwentnie rozbudowując standard zarządzania Internetem w państwach członkowskich, opracowała strategie na kolejne lata 2012–2015, 2016–2019 i 2022–2025 (Committee of Ministers, 2012; Committee of Ministers, 2016; Committee of Ministers, 2022). Dokumenty te – mające charakter programowy – stanowią swoiste kompendium dotyczące istniejących praw człowieka użytkowników Internetu, zwłaszcza w kontekście ich zagrożeń (Zieliński, 2013, s. 17). M. Zieliński – analizując ich treść – wskazuje, że przy opracowywaniu pierwotnej wersji strategii proponowano stworzenie instrumentu prawnego dotyczącego dostępu do Internetu ujętego jako prawo człowieka, umożliwiające pełne wykonywanie innych praw i wolności (Zieliński, 2013, s. 17). Nie zyskało to jednak ostatecznie aprobaty i nie zostało umieszczone w finalnym tekście strategii na lata 2012–2015 ani też w nowych jej wersjach, przyjmowanych na kolejne lata, co osłabiło argumenty zwolenników konceptualizacji prawa dostępu do Internetu.

Judykatura sądów międzynarodowych również nie dostarcza podstaw, by *explicite* jednoznacznie konstytuować prawo dostępu do Internetu, przesuwając ciężar analiz w stronę kategorii dostępu do Internetu, warunkującej skuteczną realizację praw człowieka. Już tylko tytułem przykładu: w sprawie Jankovskis v. Litwa Europejski Trybunał Praw Człowieka rozstrzygał, czy odmówienie dostępu do Internetu więźniowi osadzonemu w zakładzie karnym narusza jego prawo do otrzymywania i przekazywania informacji czy też nie (Wyrok Europejskiego Trybunału Praw Człowieka, 2017; Zieliński, 2013, s. 15). Innym przykładem potwierdzającym znaczenie dostępu do Internetu w celu korzystania z praw człowieka jest orzeczenie Trybunału Sprawiedliwości Unii Europejskiej w sprawie Scarlet v. SABAM, w którym stwierdzono, że dostawcy dostępu do Internetu nie mają obowiązku filtrowania połączeń internetowych, przekazywanych za ich pośrednictwem, ze względu na ryzyko naruszenia praw podstawowych klientów dostawcy, jak np. prawo do ochrony danych osobowych oraz wolność otrzymywania i przekazywania informacji, które są chronione przez art. 8 oraz art. 11 Karty Praw Podstawowych Unii Europejskiej (Abbotts, 2012, s. 75–77; Borgesius, 2012, s. 791–793; Rizzuto, 2012, s. 69–71; Unia Europejska, 2007; Wyrok Trybunału Sprawiedliwości Unii Europejskiej, 2011; Zieliński, 2013, s. 14).

W przestrzeni debaty społecznej – w świetle powyższego – za istotną uznać należy teorię o istnieniu jedynie pewnego negatywnego zobowiązania państw do nieingerowania lub utrudniania jednostce dostępu do Internetu (Mladenov & Staparski, 2022, s. 34; Wyrok Europejskiego Trybunału Praw Człowieka, 2012, 2014, 2015, 2019, 2020). W piśmiennictwie z tego zakresu podkreśla się bowiem, że to na państwach ciąży obowiązek zarówno zapewnienia dostępu do Internetu, jak i tego, by dostęp ten spełniał wymogi bezpieczeństwa online (Dror-Shpoliansky & Yuval Shany, 2021, s. 1254). Ewolucyjnie rozwija się i wzmacnia zatem przeświadczenie, że nielegalne ograniczenia lub arbitralna odmowa dostępu do Internetu może wpływać lub stanowić naruszenie innych chronionych praw. To chyba jednak zbyt mało, by z pełnym przekonaniem – na gruncie międzynarodowego prawa człowieka – konstytuować prawo dostępu do Internetu rozumiane jako obowiązek państw jego zapewnienia, chyba że ujmować je nie jako normatywnie wykształcone prawo podmiotowe, lecz pewien postulat mówiący o potrzebie jego istnienia. Postulat ten *implicite* odwzorowuje konstatację, że w erze cyfrowej realizacja praw człowieka przenosi się także do sfery online, dając asumpt do doktrynalnego wyodrębniania „międzynarodowego prawa cyfrowych praw człowieka" (Dror-Shpoliansky & Yuval Shany, 2021, s. 1254). Nawet jeśli podejmowane próby definiowania nowych praw cyfrowych nie doprowadzą do ich normatywnego zakotwiczenia w standardach traktatowych, to sam proces ich konceptualizacji posiada wartość dodaną, bowiem wpływa na rozwój wykładni prawa i polityk państw, które obejmują wartości ujęte w koncepcji nowych praw cyfrowych (Cassel, 2001, s. 123–124).

Mimo faktu, że w zaprezentowanym ujęciu trudno odnaleźć podstawy uprawniające do ujęcia dostępu do Internetu w normatywne ramy, to z pewnością podejmowana próba w tym zakresie winna być odczytywana jako zwrócenie uwagi na zakodowaną w owym dostępie warunkowość. Od jego zapewnienia zależy bowiem to, czy i w jakim zakresie możliwe będzie efektywne korzystanie z praw człowieka. Idąc tym tropem, na co zwraca się uwagę w piśmiennictwie, wyodrębnić można dwa aspekty postrzegania tego zagadnienia. Pierwszy, w którym wąsko kładzie się nacisk na dostęp do infrastruktury internetowej oraz drugi, szerzej uwzględniający – prócz technicznych uwarunkowań – przede wszystkim dostęp do treści tworzonych lub rozpowszechnianych w Internecie lub, innymi słowy, prawo do komunikowania się w niezwykle szerokim znaczeniu obejmującym zarówno prawo do wyszukiwania i otrzymywania treści, jak i do ich tworzenia i przesyłania do określonej osoby lub do wszystkich użytkowników Internetu (Mochalov et al., 2021, s. 148–151). W każdym z tych aspektów prawo dostępu do Internetu to zdolność jednostek – nosicieli praw podmiotowych – do działania w taki czy inny sposób.

Mimo braku powszechnie akceptowanej koncepcji co do istnienia i ewentualnie charakteru prawnego prawa dostępu do Internetu, doktrynalnie prawu temu przeciwstawiane jest prawo do niekorzystania z Internetu. Uznać je można za jedną z form manifestacji indywidualnej autonomii człowieka, w której jednostka decyduje się nie

korzystać z Internetu. wiąże się to z „indywidualną decyzją o nieuczestniczeniu bezpośrednio i aktywnie w Internecie bez narażania się na negatywne konsekwencje lub dyskryminację, przy jednoczesnej swobodzie zarządzania swoją obecnością cyfrową i ochronie prywatności" (Popa Tache et al., 2024, s. 184). Motywacja do niekorzystania z Internetu może być różna i tak długo, jak decyzja ta mieści się w ramach autonomii jednostki i jest podejmowana jako przejaw jej prawa, motywacja z prawnego punktu widzenia nie odgrywa istotnej roli. Jakkolwiek dylematy socjologiczne czy etyczne mogą mieć znaczenie przy analizowaniu decyzji o niekorzystaniu z Internetu, to nadal istnieją kwestie prawne, które należy wziąć pod uwagę. Motywacja może wynikać z ryzyka związanego z ochroną prawa do prywatności lub prawa do ochrony życia prywatnego, może mieć podłoże medyczne lub psychologiczne (Kloza, 2017, s. 451–505; Wyrok Europejskiego Trybunału Praw Człowieka, 2011). Ogólną decyzję o niekorzystaniu z nowoczesnych technologii mogą warunkować motywacje religijne lub po prostu potrzeba czasowego „cyfrowego detoksu" (Kloza, 2024, s. 2). Argumentami przemawiającymi za niekorzystaniem z Internetu mogą być kwestie finansowe – koszt Internetu, mimo że zgodnie z Kodeksem Komunikacji Elektronicznej ma być w przystępnej cenie i mimo że dla osób, których na to nie stać, ma być przygotowana dodatkowa pomoc finansowa, nadal w niektórych jurysdykcjach może być źródłem wykluczenia cyfrowego. I wreszcie, by korzystać z Internetu konieczne jest posiadanie określonych umiejętności w tym zakresie, gdyż zjawisko wykluczenia cyfrowego wciąż stanowi problem starszych pokoleń lub osób nieradzących sobie z technologią.

Co intrygujące, doktryna, analizując prawo do niekorzystania z Internetu, często doszukuje się podobieństw między tym instrumentem prawnym a prawem do edukacji, może bardziej konkretnie, prawem do odmowy edukacji (Kloza, 2024, s. 2; Popa Tache et al., 2024, s. 184). Związek ten ma jednak sens, jeśli spojrzymy na zmiany, jakie zaszły w edukacji po pandemii COVID-19, podczas której korzystanie z Internetu stało się integralną częścią funkcjonowania, a usługi publiczne i prywatne okazały się bardziej zależne od Internetu. Przykłady można znaleźć w dziedzinie e-zdrowia, e-administracji, w tym administracji podatkowej, usług finansowych, edukacji i wielu innych. Prawo do niekorzystania z Internetu może być również uzasadnione instrumentami alternatywnymi względem ochrony praw człowieka. Kodeks Komunikacji Elektronicznej bezpośrednio wskazuje, że konsumenci nie powinni być zobowiązani do dostępu do usług, których nie chcą, a zatem mogą nie tylko powstrzymać się od korzystania z usług elektronicznych, lecz także ograniczyć zakres usługi powszechnej, z której korzystają, do usług komunikacji głosowej (Parlament Europejski i Rada, 2018). Podobnie rekomendacje Europejskiej Rady Społeczno-Gospodarczej dotyczące reformy ram prawnych dostępu do Internetu wspominają o konieczności utrzymania niecyfrowej formy świadczenia usług publicznych, nawet pomimo wzrostu ich popularności we współczesnym świecie (Europejski Komitet Ekonomiczno-Społeczny, 2024). Należy również podkreślić, że Kodeks Komunikacji Elektronicznej stoi na stanowisku rozróżnienia pomiędzy technicznym dostarczaniem Internetu a

jego treścią. Ryzyko związane z możliwością, że w pewnym momencie społeczeństwo zostanie „zmuszone" do korzystania z Internetu w celu uzyskania określonych usług w sytuacji braku alternatywnych sposobów ich świadczenia, wydaje się być bardziej problemem związanym z zawartością Internetu i rozwojem cyfryzacji administracji i usług publicznych. Spostrzeżenia te wiążą się jednak przede wszystkim z warunkowym charakterem dostępu do Internetu i w tym ujęciu sytuują prawo dostępu do Internetu jako narzędzie warunkujące korzystanie z innych praw i wolności, o czym wspomniano powyżej.

Rzeczone prawo do niekorzystania z Internetu wydaje się być konsekwencją faktu, że dostęp do Internetu nadal pozostaje usługą komunikacji elektronicznej, mogącej być rozpatrywaną jako usługa szczególnego rodzaju, tj. taka, której charakter zmienia się z usługi publicznej w usługę powszechną, z określonymi państwowymi gwarancjami dostępności do niej w aspekcie technicznym i finansowym. Dostępność tej usługi jest ceniona wyżej niż konkurencja rynkowa i z tego powodu różne instrumenty, które mogą ewentualnie uchylić zasady konkurencji rynkowej w zakresie usługi dostępu do Internetu, są akceptowane przez Kodeks Łączności Elektronicznej. Tak ujmowana usługa może stanowić gwarancję skutecznej realizacji praw człowieka.

2. Od prawa do niekorzystania z Internetu do prawa do bycia offline – uwagi na tle prawa do prywatności

W dyskusji na temat prawa dostępu do Internetu i prawa do niekorzystania z Internetu, mimo braku przesądzającego, normatywnego rozstrzygnięcia ich statusu, doktryna idzie dalej, wskazując na zagadnienie bezpośrednio z nimi sprzężone, tj. na prawo do bycia offline (Kloza i in., 2025). Początkowo zarówno w polskim, jak i zagranicznym piśmiennictwie widoczna była tendencja do standaryzowania prawa do bycia offline głównie na kanwie prawa pracy w zakresie dotyczącym czasu pracy, bezpieczeństwa i higieny pracy czy prawa pracownika do odpoczynku. Uwarunkowane to było pandemią COVID-19 i nasilonym w tym czasie zjawiskiem pracy zdalnej (Pachała-Szymczyk, 2022, s. 14). Ostatecznie jednak rozwój koncepcji prawa do bycia offline przybrał szerszy kontekst poprzez osadzenie go na gruncie przemian społeczno-cywilizacyjnych, wpływających na proces multiplikacji praw człowieka – co w opinii niektórych przedstawicieli nauki uzasadnia tworzenie nowych praw jednostki jako odpowiedź na współczesne wyzwania (Mowbray, 2005, s. 57–79).

Prawo do bycia offline prezentowane jest w doktrynie jako prawo jednostki do wyboru, aby nie uczestniczyć – mimo zapewnionego dostępu – bezpośrednio i aktywnie w środowisku online, bez narażania się na negatywne konsekwencje lub dyskryminację, zapewniając swobodę zarządzania własną obecnością cyfrową i chroniąc swoją prywatność (Popa Tache & Miço (Bellani), 2024, s. 18). W toczącym się dyskursie – właściwym m.in. nowo powstającym kategoriom – nie sposób znaleźć jed-

noznaczne rozstrzygnięcie w zakresie charakteru prawa do bycia offline i jego relacji do prawa do niekorzystania z Internetu. W miejsce tego powielane są – podobnie jak w kontekście prawa dostępu do Internetu – dwie zasadnicze kwestie. Pierwsza – czy prawo do bycia offline należy pośrednio wywodzić z istniejącego normatywnego katalogu praw i wolności człowieka, traktując je jako instrument ich realizacji i ochrony? Druga – czy istnieje potrzeba wyodrębnienia autonomicznego prawa do bycia offline, a zatem takiego, które, będąc niezależnym, ma charakter odrębny od ustanowionych już praw? W pierwszym aspekcie wskazać warto kilka zasadniczych uwarunkowań. Nie ulega bowiem wątpliwości, że przemiany cywilizacyjne, wśród których jednoznacznie wskazuje się na rozwój przestrzeni internetowej, określić można jako *signum temporis*. Wpływają one na wiele obszarów życia człowieka, stanowiąc pierwotną determinantę w analizach dotyczących specyfiki prawa do bycia offline na płaszczyźnie praw człowieka. Z metodologicznego punktu widzenia interpretacji norm prawno-człowieczych szczególna rola wpływu przemian cywilizacyjnych na te prawa widoczna jest w aspekcie analizy dogmatycznej norm prawnych, zawartych w tekstach aktów normatywnych.

Poszukując podstaw dla formułowania prawa do bycia offline na gruncie systemu praw człowieka, jednocześnie odnosząc ten zabieg do prawa do niekorzystania z Internetu, podnieść należy kwestię – tak ważnego – normatywnego zakotwiczenia tego prawa w prawie do prywatności. O ile nie ulega żadnej wątpliwości, że prawo do prywatności przysługuje każdej jednostce, o tyle znaczne problemy powoduje określenie zakresu tego prawa, zwłaszcza we wciąż zmieniającej się rzeczywistości, w tym rzeczywistości cyfrowej (Banaszewska, 2013, s. 127). Stan toczącej się dyskusji doktrynalnej ujawnia bogactwo i różnorodność znaczeń w kontekście pojęcia prywatności. Ich zakresy są na tyle pojemne i otwarte, że niekiedy utrudniają przez to rozpoznanie, że dotyczą one wciąż tego samego pojęcia (Bąba, 2018, s. 36–38). Prywatność jest opisywana przy wykorzystaniu wartości poprzez pryzmat ich ochrony zarówno z osobna, jak i wszystkich łącznie. Istotą kategorii prywatności jest więc konglomerat pewnych uprawnień jednostki, obejmujący m.in. wolność i tajemnicę komunikowania się, autonomię informacyjną, wolność wyrażania poglądów, wolność sumienia, wolności decydowania o życiu osobistym, prawo do ochrony danych osobowych, prawo do wolnego spędzania czasu czy prawo do niekorzystania z Internetu (Bąba, 2018, s. 36–37). Szczególną rolę odgrywa także autonomia informacyjna definiowana jako prawo do samodzielnego decydowania o ujawnianiu innym informacji dotyczących swojej osoby, a także prawo do sprawowania kontroli nad takimi informacjami, jeśli znajdują się w posiadaniu innych podmiotów (Christian, 2020, s. 63–64; Iwasiński, 2020, s. 26–27; Wyrok Trybunału Konstytucyjnego, 2002, 2008). Prywatność w sensie normatywnym zakłada uprawnienie jednostki do kształtowania sfery prywatnej życia, aby była ona wolna od ingerencji i niedostępna dla innych, opierając się więc na autonomii woli podmiotu. Jak zauważa M. Safjan, „prywatność ma podlegać ochronie właśnie dlatego i tylko dlatego, że przyznaje się każdej osobie

prawo do wyłącznej kontroli tej sfery życia, która nie dotyczy innych, a w której wolność od ciekawości innych jest swoistą *conditio sine qua non* swobodnego rozwoju jednostki" (Safjan, 2006, s. 211). Prawo do prywatności nie ma charakteru absolutnego. Koncepcja istoty praw i wolności opiera się na założeniu, że „w ramach każdego konkretnego prawa i wolności można wyodrębnić pewne elementy podstawowe (rdzeń, jądro), bez których takie prawo czy wolność w ogóle nie będzie mogła istnieć, oraz pewne elementy dodatkowe (otoczkę), które mogą być przez ustawodawcę zwykłego ujmowane i modyfikowane w różny sposób bez zniszczenia tożsamości danego prawa czy wolności" (Wyrok Trybunału Konstytucyjnego, 2020). W przypadku prawa do prywatności stopień możliwej ingerencji uzależniony jest od rodzaju dóbr chronionych oraz osoby, której dobra te dotyczą, przykładowo osoby publiczne korzystają z węższego zakresu ochrony (Grzybowski, 2020, s. 54). Istotą kategorii prywatności jest przede wszystkim konglomerat pewnych uprawnień jednostki. Jeśli uznać zatem prawo do bycia offline (czy również prawo do niekorzystania z Internetu) za formę manifestacji autonomii osobistej jednostki, to brak jest podstaw, by „uniezależniać" je od prawa do prywatności. Można uznać, że prawo do prywatności swoim zakresem obejmuje uprawnienie jednostki do niekorzystania z Internetu i bycia offline, będące elementem składowym owego konglomeratu. Mając na uwadze specyfikę prawa do prywatności, uwzględnienie pewnego kontekstu społecznego wpisanego w to prawo gwarantować ma osiąganie celu, dla realizacji jakiego prawo to zostało przyjęte w systemie międzynarodowego i krajowego prawa praw człowieka. Jest nią ochrona wartości, stanowiąca *ratio legis* standardów normatywnych, w tym przypadku sprowadzająca się do sfery prywatności jako pewnego *sacrum* człowieka. Wpisanie niekorzystania z Internetu i bycia offline w traktatowo uznane prawo do prywatności ma dodatkowy walor. Uprawnia do stwierdzenia istnienia jego normatywnego zakotwiczenia w najważniejszych aktach prawa międzynarodowego m.in. takich jak: Powszechna Deklaracja Praw Człowieka ONZ z 1948 r., Międzynarodowy Pakt Praw Obywatelskich i Politycznych z 1966 r., Europejska Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności z 1950 r. czy Karta Praw Podstawowych Unii Europejskiej z 2000 roku.

Niezbędność wpisania kategorii niekorzystania z Internetu i bycia offline w normatywną istotę prawa do prywatności nie oznacza jednak pozbawienia ich samodzielnej treści, choć trudno dowieść *de lege lata* istnienia prawa do niekorzystania z Internetu i prawa do bycia offline. Prawo do prywatności stanowi zatem formę „rekompensaty", przy braku regulacji wprost odnoszących się do aspektów niekorzystania z Internetu i bycia offline, bowiem nieustanowienie standardu normatywnego zawsze osłabia efektywność ochrony praw człowieka. Gwarancje w zakresie ochrony prawa do prywatności – posiadające charakter uniwersalny – skutkują tym, że w każdym przypadku naruszenia tego prawa – również w obszarze niekorzystania z Internetu czy bycia offline – przedmiotem ochrony jest ta sama wartość – czyli określona

sfera prywatności. Ochrona tego prawa, bez względu na to, jakiej materii dotyczy, zawsze ukierunkowana jest na ochronę jednostki *in genere*.

Podsumowanie

Kwestia istoty i charakteru prawnego prawa dostępu do Internetu (a co za tym idzie, *a contrario* praw z nim powiązanych: prawa do niekorzystania z Internetu i prawa do bycia offline) pozostaje otwarta i niedostatecznie rozstrzygnięta nie tylko w literaturze prawniczej, lecz także w praktyce stosowania prawa. Biorąc pod uwagę istniejący dorobek doktrynalny, możliwe jest uogólnienie istniejących stanowisk badaczy i podkreślenie dwóch przeciwstawnych stanowisk dotyczących prawa dostępu do Internetu. Pierwsza grupa badaczy uważa, że już teraz konieczne jest uznanie prawa dostępu do Internetu za prawo podstawowe, argumentując swoje poglądy faktem, że większość praw człowieka jest realizowana za pośrednictwem technologii internetowych (Reglitz, 2020, s. 314–331). Jednocześnie druga grupa argumentuje, że dostęp do Internetu jest instrumentem (czynnikiem) umożliwiającym realizację praw człowieka, a nie prawem jako takim, w związku z czym nie ma potrzeby nadawania mu takowego statusu, ponieważ jest ono już objęte istniejącymi prawami (Skepys, 2012, s. 15–29).

Chociaż daje się zauważyć daleko idącą doktrynalną tendencję do tworzenia nowych praw człowieka, jaką są chociażby tytułowe prawo do niekorzystania z Internetu i prawo do bycia offline, a nawet i prawo dostępu do Internetu, to pojawia się zasadnicza i problematyczna kwestia: znaczna dynamika tworzenia nowych praw bez jednoczesnego zapewnienia właściwych instrumentów ich realizacji i kontroli przestrzegania, skutkować może iluzoryczną ochroną praw jednostki. Multiplikacja praw – bez ich normatywnego zakotwiczenia – może bowiem nie tylko osłabiać tak pożądaną efektywność ochrony praw człowieka, ale i skrajnie nawet jej zagrażać. Z jednej strony bowiem, daje ona jednostkom ułudę przysługujących im wielu (licznych i rozdrobnionych treściowo praw), z drugiej zaś czyni je jedynie postulatami niemożliwymi do realizacji ze względu na brak odpowiednich narzędzi prawnych. Taki stan prawny stanowić może obciążenie nawet dla tych państw, które mają ugruntowane standardy normatywne i rozbudowaną praktykę w zakresie ochrony praw człowieka. W piśmiennictwie zauważa się, iż zasadniczą cechą decydującą o praktycznym znaczeniu praw człowieka jest możliwość skutecznego dochodzenia zawartych w nich treści przed kompetentnymi i niezawisłymi organami ochrony prawnej (Kowalski, 1988, s. 67). Zgodnie z paremią *ubi ius ibi remediuvi* warunek istnienia gwarancji prawnych koniecznych dla ochrony prawa do prywatności zawarty jest zarówno w standardach normatywnych o charakterze powszechnym, jak i w regionalnych normach prawno-człowieczych. Dlatego prawo to winno wyznaczać optykę postrzegania tytułowych praw, pozwalając pozytywnie zweryfikować postawioną na wstępie hipotezę.

Jednocześnie warte podkreślenia jest to, że postęp technologiczny, rozwój przestrzeni internetowej, sztucznej inteligencji i automatyzacji otworzył erę bezprecedensowych zmian, wymagających redefinicji uznanych na arenie międzynarodowej standardów prawno-człowieczych. Z tej perspektywy konsolidacja działań na rzecz efektywności przestrzegania, egzekwowania praw człowieka czy tworzenia mechanizmów odpowiedzialności adekwatnie do rozszerzającej się interpretacji prawa do prywatności (obejmującego również prawo do niekorzystania z Internetu czy prawo do bycia offline) to model, który zapewni właściwą realizację tytułowych praw na kanwie dorobku prawnego i instytucjonalnego wpisanego w prawo do prywatności. W systemowych regulacjach z zakresu międzynarodowego prawa praw człowieka prawo to ma ugruntowany status. W sposób szczególny kształtować ono winno zatem treść takich nowych praw, jak prawo dostępu do Internetu, *a contrario* prawo do niekorzystania z Internetu czy prawo do bycia offline, jeśli postulatywnie w piśmiennictwie dostrzegamy potrzebę ich kreacji. Ich ochrona będzie wówczas skuteczniejsza w swej istocie, aniżeli „powoływanie do życia" – w obliczu braku normatywnych, wiążących ku temu podstaw – nowych praw. Fakt ich multiplikacji, choć interesujący naukowo i wzbogacający dyskurs na temat praw cyfrowych *in genere* nie przełoży się na ich efektywność. Tu potrzebne są regulacje prawne wprost zaopatrujące jednostki w konkretne prawa. Bez tego dochodzenie roszczeń objętych ich zakresem pozostanie atrakcyjną poznawczo fikcją, choć może i przyszłość pokaże, że stanie się ona – antycypując – kształtującym prawo faktem. W tym ujęciu multiplikacja praw człowieka ma nie tylko pejoratywne znaczenie, ale i może zostać uznana za czynnik zmuszający do redefinicji postrzegania praw człowieka poprzez przedmiotowe poszerzanie ich katalogu. Przy tak sformułowanym stanowisku wydaje się, iż doktrynalna propozycja uznająca teorię instrumentalnego wynikania norm prawno-człowieczych z innych norm o tym charakterze pozwala uznać, że prawo do Internetu i powiązane z nim prawo do niekorzystania z Internetu i prawo do bycia offline są niezbędne do realizacji innych praw – zatem występuje między nimi pewien związek przyczynowy (Milczarek, 2023, s. 157–159). Zgodnie natomiast z regułą instrumentalnego nakazu państwo zobowiązane jest do podejmowania takich działań, które w adekwatny sposób do tego celu prowadzą, zaś zgodnie z regułą instrumentalnego zakazu – zakazane jest podejmowanie działań, które uniemożliwiają bądź utrudniają osiągnięcie tego celu, multiplikacja praw na tej płaszczyźnie wydaje się zbędna (Wronkowska, 2005, s. 95–96).

BIBLIOGRAFIA

Abbotts, G. (2012). Scarlet Extended Reprieve from Content Filtering. *Entertainment Law Review*, *3*, 75–77.

Banaszewska, A. (2013). Prawo do prywatności we współczesnym świecie. *Białostockie Studia Prawnicze*, *13*, 127–136.

Bąba, M. (2018). Refleksje wokół prywatności i autonomii informacyjnej w świecie Internetu (wszech) rzeczy. *Współczesne Problemy Zarządzania*, *2*, 33–52.

Brzozowski, W. (2023). Zagadnienia wstępne. w: W. Brzozowski, A. Krzywoń, & M. Wiącek (red.), *Prawa człowieka* (ss. 31–32). Wolters Kluwer.

Borgesius, F. Z. (2012). Filtering for Copyright Enforcement in Europe after Sabam Case. *European Intellectual Property Review*, *11*, 791–795

Cassel, D. (2001). Does International Human Rights Law Make a Difference. *Chicago Journal of International Law*, *2*(1), 121–135

Committee of Ministers. (2012, 15 marca). Internet Governance – Council of Europe Strategy 2012–2015 (CM(2011)175-final), pkt 9a. https://search.coe.int/cm#{%22CoEReference%22:[%22CM(2011)175-final%22],%22sort%22:[%22CoEValidationDate%20Descending%22],%22CoEIdentifier%22:[%2209000016805cad04%22]}

Committee of Ministers. (2016, 30 marca). Internet Governance – Council of Europe Strategy 2016–2019. Democracy, human rights and the rule of law in the digital world. https://edoc.coe.int/en/internet/7128-internet-governance-council-of-europe-strategy-2016–2019.html

Committee of Ministers. (2022, 4 maja). Digital Agenda 2022–2025. Protecting human rights, democracy and the rule of law in the digital environment (CM(2022)20-final). https://rm.coe.int/coe-digital-agenda-2022–2025-pro-eng-web/1680aa3e1b

Council of Europe. (2009, 28–29 maja). Political Declaration. w: 1 st Council of Europe Conference of Ministers Responsible for Media and New Communications Services. A New Notion of Media? (28 and 29 May 2009, Reykjavik, Iceland). Political Declaration and Resolutions. MCM(2009)011, § 5. https://www.coe.int/

Christian, B. (2020). *The Alignment Problem. Machine Learning and Human Values*. W.W. Norton & Company.

Dror-Shpoliansky, D., & Shany, Y. (2021). It's the End of the (Offline) World as We Know It: From Human Rights to Digital Human Rights – A Proposed Typology. *European Journal of International Law*, *32*(4), 1254.

Estes, A.C. (2011). The U.N. Declares Internet Access a Human Right. *The Atlantic Wire*, 1. https://www.theatlantic.com/technology/archive/2011/06/united-nations-wikileaks-internet-human-rights/351462/

Estrada, M. (2020). Revisiting access to internet as a fundamental right in times of COVID-19. *UNIO – EU Law Journal*, *6*(2), 15–24.

Europejski Komitet Ekonomiczno-Społeczny. (2024, 18 września). Opinia: Prawa dotyczące usługi powszechnej w dziedzinie łączności elektronicznej w Unii Europejskiej (opinia rozpoznawcza na wniosek Komisji Europejskiej) (C/2024/6864) (Dz.U. UE C, 28.11.2024).

Gosztonyi, G. (2020). The European Court of Human Rights: Internet Access as a Means of Receiving and Imparting Information and Ideas. *International Comparative Jurisprudence*, *6*(2), 134–140.

Grzybowski, K. (2020). Autonomia informacyjna jednostki a zgoda na przetwarzanie przez pracodawcę danych osobowych. *Przegląd Sejmowy*, *6*, 47–67.

Hohfeld, W.N. (1923). *Fundamental Legal Conceptions: as Applied in Judicial Reasoning and Other Legal Essays*. Yale University Press.

Human Rights Committee. (2011, 21 lipca). General comment No. 34, Article 19: Freedoms of opinion and expression (CCPR/C/GC/34).

Human Rights Council. (2011, 16 maja). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue (A/HRC/17/27).

Human Rights Council (2012, 5 lipca). Resolution: The Promotion, Protection and Enjoyment of Human Rights on the Internet (20/8) (A/HRC/20/L.13).

Iwasiński, Ł. (2020). Social Implications Of Algorithmic Bias. w: B. Sosińska-Kalata, M. Roszkowski, & Z. Wiorogórska (red.), *Nauka o informacji w okresie zmian. Rewolucja cyfrowa: infrastruktura, usługi, użytkownicy* (ss. 25–35). Miscellanea Informatologica Varsoviensia.

Jasmontaite, L. & De Hert, P. (2020). Access to the Internet in the EU: A Policy Priority, a Fundamental, a Human Right or a Concern for eGovernment? *Brussels Privacy Hub Working Paper*, *6*(19), 2–24.

Kloza, D. A. (2017). Behavioural alternative to the protection of privacy. w: D. J. B. Svantesson, D. Kloza (red.), *Trans-Atlantic data privacy relations as a challenge for democracy* (ss. 451–505). Intersentia.

Kloza, D. (2024). The right not to use the Internet. *Computer Law & Security Review: The International Journal of Technology Law and Practice*, *52*, 10590 .

Kloza, D., Kużelewska, E., Lievens, E., & Verdoodt V. (2025). *The Right Not to Use the Internet: Koncepcja, Konteksty, Konsekwencje*. Routledge.

Komisja Europejska. (2021, 9 marca). Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: Cyfrowy kompas na 2030 r.: europejska droga w cyfrowej dekadzie (52021DC0118) (COM/2021/118 final.).

Kowalski, P. (1988). Nowe prawa człowieka. Perspektywy i zagrożenia. *Ruch Prawniczy, Ekonomiczny i Socjologiczny*, *2*, 57–75.

Malinowski, S. M. (2020) Status prawny Internetu w świetle Konstytucji RP i obowiązującego prawodawstwa polskiego. *Prawo Mediów Elektronicznych*, *1*, s. 23–30.

Mazurek, F. J. (1982). Społeczne prawa człowieka. *Roczniki Nauk Społecznych*, *X*, 205–230.

Milczarek, E. (2023). Miejsce prawa do Internetu w krajowych porządkach prawnych. *Przegląd Prawa Konstytucyjnego*, *1*(71), 149–160.

Mladenov, M., & Staparski, T. (2022). Liability of online platforms for content moderation from the perspective of the European Court of Human Rights – challenges and recent developments. *Revija za evropsko pravo*, *24*(1), 25–34.

Mladenov, M., Kouroupis, K., & Serotila, I. (2023). Can we make the Internet "forget" something about us? CJEU and ECtHR Approach. *Evrigenis Yearbook of International and European Law*, *5*, 205–213.

Mochalov, A., Kolobaeva, N. E., & Nesmevanova, S. E. (2021). The Right to Access the Internet: its Legal Content and the Mechanism of Implementationin. *Antinomies*, *21*(4), 135–163.

Mowbray, A. (2005). The Creativity of the European Court of Human Rights. *Human Rights Law, Review*, *5*(1), 57–79.

Organization for Security and Co-operation in Europe. (2010, 1–2 grudnia).The Office of the Representative on Freedom of the Media Duja Mijatović, Report: Freedom of Expression on the Internet, A study of legal provisions and practices related to freedom of expression, the free flow of infor-

mation and media pluralism on the Internet in OSCE participating States (ss. 54–58). https://www.osce.org/files/f/documents/c/9/105522.pdf

Oyedemi, T. (2015). Internet access as citizen's right? Citizenship in the digital age. *Citizenship Studies*, *19*(3–4), 1–15.

Pachała – Szymczyk, E. (2022). Prawo do bycia offline odpowiedzią na upowszechnienie narzędzi cyfrowych w zatrudnieniu. *Transformacje Prawa Prywatnego*, *4*, 7–26.

Parlament Europejski i Rada. (2018, 11 grudnia). Dyrektywa ustanawiająca Europejski kodeks łączności elektronicznej (wersja przekształcona) (2018/1972) (Dz.U. L , 17.12.2018), 36–214.

Parlament Europejski i Rada. (2022, 14 grudnia). Decyzja ustanawiająca program polityki „Droga ku cyfrowej dekadzie" do 2030 r. (2022/2481) (Dz. Urz. UE L 323,19.12.2022).

Pollicino, O. (2020). The Right to Internet Access: Quid Iuris? w: A. Von Arnauld, K. Von der Decken, & M. Susi (red.), *The Cambridge Handbook of New Human Rights: Recognition, Novelty, Rhetoric* (ss. 263–275). Cambridge University Press.

Popa Tache, C. E. & Miço (Bellani), H. (2024). Some Reflections on Two of the Most Visible Developments: The Right to Refuse Internet Use and the 'Chilling Effect'. w: T. Pajuste, H. Bellani Miço (Bellani), & S. Maslo Cerkic (red.), *Legal Perspectives in the Modern Era of Technological Transformations* (ss. 17–18), ADJURIS International Academic Publisher.

Popa Tache, C.E., Săraru, C.S., & Kouroupis, K. (2024). Different perspectives concerning the right not to use the internet and some analogies with education. *European Journal of Privacy Law&Technologies*, *1*, 179–193.

Qerimi, Q. (2017). Bridge over Troubled Water: An Emerging Right to Access to the Internet. *International Review of Law*, *1*, 1–22.

Rada Europy. (1950). Europejska Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności (4 listopada 1950) (Dz.U. z 1993 r. Nr 61, poz. 284).

Reglitz, M. (2020). The Human Right to Free Internet Access. *Journal of Applied Philosophy*, *37*(2), 314–331.

Rizzuto, F. (2012). Injunctions Against Intermediate Online Service Providers. *Computer and Telecommunications Law Review*, –, 69–73.

Safjan, M. (2006). Prawo do ochrony życia prywatnego. w: *Szkoła Praw Człowieka* (ss. 211–212). Helsińska Fundacja Praw Człowieka.

Skepys, B. (2012). Is There a Human Right to the Internet? *Journal of Politics and Law*, *5*(4), 15–29.

Stępniak, K. (2017). Prawo do Internetu jako środka zapewniającego partycypację w państwie demokratycznym. *Studia Prawnicze i Administracyjne*, *21*, 65–70.

Szoszkiewicz, Ł. (2018). Internet Access as a New Human Right? State of the Art on the Threshold of 2020. *Adam Mickiewicz University Law Review*, *8*, 49–62.

Tully, S. (2014). A Human Right to Access the Internet? Problems and Prospects. *Human Rights Law Review*, *14*(2), 175–196.

Unia Europejska. (2007, 13 grudnia). Karta Praw Podstawowych Unii Europejskiej (Dz. Urz. UE C 326, 26.10.2012 r.).

Wong, W. H. (2023). *We, The Data: Human Rights in the Digital Age*. The MIT Press.

Wronkowska, S. (2005). *Podstawowe pojęcia prawa i prawoznawstwa*. Ars Boni et Aequi Przedsiębiorstwo Wydawnicze Michał Rozwadowski.

Wyrok Europejskiego Trybunału Praw Człowieka z dnia 26 maja 2011 r. w sprawie *R. i R. v. Polska*, nr skargi 27617/04. https://hudoc.echr.coe.int/

Wyrok Europejskiego Trybunału Praw Człowieka z dnia 18 grudnia 2012 r. w sprawie *Ahmet Yildirim v. Turcja*, nr skargi 311/10. https://hudoc.echr.coe.int/

Wyrok Europejskiego Trybunału Praw Człowieka z dnia 11 marca 2014 r. w sprawie *Akdeniz v. Turcja*, nr skargi nr 20877/10. https://hudoc.echr.coe.int/

Wyrok Europejskiego Trybunału Praw Człowieka z dnia 1 grudnia 2015 r. w sprawie *Cengiz i in. V. Turcja*, nr skargi 48226/10 i 14027/11. https://hudoc.echr.coe.int/

Wyrok Europejskiego Trybunału Praw Człowieka z dnia 17 stycznia 2017 r. w sprawie *Jankovskis v. Litwa*, nr skargi 21575/08. https://hudoc.echr.coe.int/

Wyrok Europejskiego Trybunału Praw Człowieka z dnia 30 kwietnia 2019 r. w sprawie *Elvira Dmitriyeva v. Rosja*, nr skargi 60921/17 i 7202/18. https://hudoc.echr.coe.int/

Wyrok Europejskiego Trybunału Praw Człowieka z dnia 23 czerwca 2020 r. w sprawie *Engels v. Rosja*, skarga nr 61919/16. https://hudoc.echr.coe.int/

Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 24 listopada 2011 r. w sprawie Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), C-70/10, ECLI:EU:C:2011:771.

Wyrok Trybunału Konstytucyjnego z dnia 12 stycznia 2000 r., P. 11/98 (OTK ZU 2000, Nr 1, poz. 3).

Wyrok Trybunału Konstytucyjnego z dnia 19 lutego 2002 r., sygn. U 3/01 (Dz.U. z 2002 r. Nr 19, poz. 197).

Wyrok Trybunału Konstytucyjnego z dnia 17 czerwca 2008 r., sygn. K 8/04, (Dz.U. z 2008 r. Nr 110, poz. 707).

Zgromadzenie Ogólne ONZ. (1948). Powszechna Deklaracja Praw Człowieka (10 grudnia 1948), http://www.un.org/ en/

Zgromadzenie Ogólne ONZ. (1966). Międzynarodowy Pakt Praw Obywatelskich i Politycznych (19 grudnia 1966) (Dz. U. z 1977 r. Nr 38, poz. 167).

Zieliński, M. (2013). Dostęp do Internetu jako prawo człowieka? W sprawie potrzeby nowej wolności w Konstytucji Rzeczypospolitej Polskiej. *Przegląd Sejmowy*, *4*(117), 14–21.

Bialystok Legal Studies
Białostockie Studia Prawnicze
2025 vol. 30 no. 4

sciendo

DOI: 10.15290/bsp.2025.30.04.04

Received: 23.09.2025
Accepted: 13.11.2025

Elżbieta Kużelewska
University of Bialystok, Poland
e.kuzelewska@uwb.edu.pl
ORCID ID: 0000–0002–6092–7284

Damian Malinowski
University of Bialystok, Poland
dmalinowski90@gmail.com
ORCID ID: 0009–0002–3193–4044

Mariusz Tomaszuk
Warsaw School of Technology, Poland
tomaszuk.m@gmail.com
ORCID ID: 0000–0003–4669–9745

Human Rights and Digital Choice: Rethinking the Right (Not) to Use the Internet[1]

Abstract: As digitalization permeates nearly all areas of life, access to the internet has become essential for the exercise of numerous human rights, including freedom of expression, access to information, and participation in public life. However, the growing expectation to engage digitally may undermine individual autonomy, especially when access to fundamental services or legal entitlements depends on being online. This article examines the underexplored concept of the right not to use the internet as a human rights issue. It argues that digital non-use – whether by choice, necessity, or circumstance – must be recognized as an aspect of informational self-determination rooted in the principles of dignity and autonomy. While access to the internet facilitates other rights, the freedom to disconnect is equally essential to prevent new forms of exclusion, coercion, and surveillance. Drawing on evolving interpretations of existing rights – particularly the rights to privacy, freedom of expression, and non-discrimination – the

1 Funded by the National Science Centre, Poland, under the OPUS call in the Weave programme (UMO-2023/51/I/HS5/01417) and the Flemish Research Foundation (FWO Funding Agreement G000325N). The article is also financially supported by the Polish Minister of Science under the 'Regional Initiative of Excellence' (RID) programme.

paper proposes that digital autonomy requires protecting both positive and negative dimensions: the right to use the internet and the right not to use it. It hypothesizes that formally recognizing a 'right to digital non-use' as a separate human right faces significant challenges in highly digitalized societies, while the existing European human rights framework is sufficiently robust to protect this right. The analysis supports both hypotheses.

Keywords: digital autonomy, right not to use the internet, human rights, digital exclusion

Introduction

Digital technology has become nearly inescapable in modern life. Governments, businesses, and social services increasingly operate under a 'digital by default' paradigm, assuming universal internet use by their constituents. While efforts to promote internet access as a human right have gained momentum (De Hert & Kloza, 2012; Frosini, 2014; Kaur, 2021; Lucchi, 2013; Passaglia, 2022; Pollicino, 2020; Reglitz, 2020, 2023, 2024; Shandler, 2019; Tomalty, 2017), the flip side of the coin – the right to remain offline – has only recently entered legal and scholarly debate (Custers, 2019; Kloza, 2024; Passaglia, 2025). The central question examined in this article is whether individuals possess a human right to digital non-use, that is, the right not to be compelled to rely on the internet or related technologies as a prerequisite for exercising their rights or conducting their everyday affairs, as well as whether the catalogue of human rights can be expanded by adding the digital non-use right (the right not to use the internet). This question arises from the observation that what began as a mere convenience has swiftly become a de facto requirement for full participation in society (International IDEA, 2023; Kloza, 2024; Susi, 2025; Terzis, 2025). As online platforms replace physical services (from e-government portals to online banking), those who abstain from digital life risk marginalization. An additional question is whether human rights law protects individuals' freedom of choice to live an analogue existence, and whether this is in any form possible in the modern world. The first hypothesis of this article is that introducing the digital non-use right as a new human right would be difficult in view of the current level of digitalization in societies. The second hypothesis is that the current European catalogue of human rights is sufficient to protect the right not to use the internet. This article uses the formal and dogmatic research method. The analysis is limited to the area of Europe; therefore, European legal acts will be taken into consideration.

As a starting point for considerations concerning human rights, reference should be made to European legislation on the human rights protection system. Such legislation includes the European Convention on Human Rights (ECHR) adopted by the Council of Europe, as well as the Charter of Fundamental Rights of the European Union (EU Charter), adopted by the EU's institutions. European human rights instruments do not explicitly articulate a 'right to offline life'; however, several fundamental rights can be interpreted to offer protection for those who choose to abstain from

ubiquitous connectivity. By examining four key rights – privacy, self-determination, freedom of expression, and equality/non-discrimination – this article explores the legal foundations for a right not to use the internet. Each of these rights provides a lens on different aspects of the issue: (a) privacy relates to personal autonomy and the desire to be 'let alone' (Warren & Brandeis, 1890, p. 193); (b) self-determination speaks to the ability to shape one's life course free from undue interference; (c) freedom of expression includes the liberty not to speak or to select the medium of communication; (d) equality demands that one's life choices (such as remaining offline) not become grounds for exclusion or discrimination.

Throughout the analysis, a guiding principle is that human rights are meant to empower individuals with choice and agency. Just as human rights law has begun to affirm the right to internet access (to ensure everyone can go online if they wish) (Wiśniewski, 2021, pp. 114–120), by analogy it should also guard against forced digitalization and confirm that life offline must remain a viable and respected choice. The same human dignity that demands bridging the digital divide for those who want connectivity also demands protection for those who, for personal, ethical, or practical reasons, decline to use digital technologies.

1. The right to privacy

Under Article 8 of the ECHR, privacy and private life provide a primary foothold for the notion of a right to remain offline. Article 8 guarantees that '[e]veryone has the right to respect for his private and family life, his home and his correspondence', subject only to necessary and proportionate limitations by law. The European Court of Human Rights (ECtHR) has interpreted 'private life' broadly to encompass personal autonomy and individual identity. In *S. and Marper v. United Kingdom* (2008), the Court famously stated that the right to privacy 'can embrace multiple aspects of the person's physical and social identity'. This jurisprudence signals that personal lifestyle choices, including how one engages with society and technology, fall within the protective scope of private life (Koops et al., 2017).

Privacy in the European human rights tradition is closely linked to human dignity and the notion of a personal sphere of freedom (Whitman, 2004). Choosing to live one's life offline – for example, preferring face-to-face interactions, analogue media, and paper correspondence – can be seen as an exercise of personal autonomy in how one develops relationships and identity. Notably, the privacy right includes the 'negative' aspect of the right to be left alone, famously articulated by Warren and Brandeis (1890) as the core of privacy. In modern terms, being 'let alone' could translate into the right to opt out of digital surveillance and data collection. Indeed, scholars have argued that 'in a world of automated data processing, being offline is the most genuine form of the right to respect for private life with regard to data protec-

tion […] the "default setting"" (Karaboga et al., 2017, p. 43), with any departure from that default requiring justification. This understanding aligns with the provisions of regulations such as Article 88 of the General Data Protection Regulation (GDPR), which empowers collective bargaining to adopt more specific rules to protect workers' rights, including consent, privacy, and data management, thereby reinforcing the practical implementation of the right to digital non-use in employment settings (Miranda Boto & Brameshuber, 2024, p. 210). Karaboga et al.'s (2017) view is reinforced by data protection principles in European law, such as data minimization and purpose limitation (Article 5 GDPR), which require that if a less invasive means exists to achieve a purpose, it should be favoured. Choosing not to engage digitally is a way to control one's personal data exposure, effectively exercising 'informational self-determination'. Thus privacy and data protection rights can support an individual's claim to an offline alternative when digital systems would otherwise compel them to disclose personal data or subject themselves to surveillance.

Crucially, privacy as protected by Article 8 also covers the 'right to personal development' and the right to establish and maintain relationships with others (Judgments of the ECtHR, 2002, 2008). This aspect has two implications for digital non-use. First, an individual may genuinely believe that abstaining from social media or online platforms is important for their personal development or mental well-being. Such a personal decision, intimately linked to one's philosophy of life or health, lies within their private sphere. Second, if everyone else moves to digital-only communication, an offline person's ability to develop contacts and relationships might be impaired, raising privacy concerns in terms of exclusion.

At the same time, it must be acknowledged that Article 8 is a qualified right; not every personal preference will be protected as a matter of fundamental rights. The ECtHR has held that there is a *de minimis* threshold of seriousness for an interference with private life to engage Article 8 (Judgment of the ECtHR, 2019); minor inconveniences or trivial choices may not suffice. For instance, in *Stevens v. UK* (1986), a case concerning a school requiring a uniform, the European Commission on Human Rights found no right 'to refuse to buy a school uniform' under Article 8. Therefore a claimant asserting a right to remain fully offline would need to show that being forced online causes more than trivial inconvenience – it must seriously affect their private life or enjoyment of other rights. The proportionality analysis under Article 8(2) will weigh the individual's interest in offline autonomy against the state's interest in digital efficiency or other aims. If a government contends that online-only systems are cost-effective or serve broader public interests (e.g. combating tax fraud or enhancing service efficiency), a court will examine whether less intrusive alternatives, such as maintaining an offline option or providing assistance, could achieve the same objectives without infringing on individual autonomy (Rossi, 2025).

The right to privacy enshrined in Article 8 of the ECHR is also guaranteed in the EU Charter (Article 7), which further underscores its significance within the Euro-

pean human rights tradition. Consequently, within the European Union there exists a dual framework of human rights protection, which reinforces the safeguarding of these rights and provides a broad basis for their observance across multiple spheres of human life.

2. The right to self-determination and autonomy

Closely intertwined with privacy, but deserving separate emphasis, is the right to self-determination. Although not codified as a distinct article in the ECHR or the EU Charter, the concept of personal self-determination underlies many human rights. It flows from the idea of individual freedom and human dignity protected in instruments like the Universal Declaration of Human Rights, and is implicit in the ECHR Article 8's protection of personal autonomy (Judgment of the ECtHR, 2002). In the context of technology, self-determination means the freedom to decide how and to what extent one engages with technological tools and digital networks. It is the freedom to define one's own relationship with technology according to one's values, be it enthusiastic adoption, cautious use, or principled refusal.

Moreover, personal autonomy is a value consistently upheld by the ECtHR across various domains. In *Pretty v. United Kingdom* (2002), while the Court ultimately did not find a right to assisted suicide, it affirmed that Article 8 encompasses the notion of personal autonomy over decisions of the utmost personal importance (the timing and manner of one's death, in that case). By extension, decisions about one's way of life, including the choice to eschew using information and communications technology (ICT), fall within that autonomous sphere. The Court of Justice of the European Union has similarly acknowledged autonomy in the digital context, for instance by empowering individuals via data protection (the rights to object to processing, to erasure, etc., under the GDPR are legal tools enabling self-determination over personal data). The EU Charter's Article 1 states that '[h]uman dignity is inviolable. It must be respected and protected.' Human dignity arguably requires that individuals are not reduced to mere cogs in a digital machine or forced to conform to a technological mode of living against their will. As one commentator puts it, a right to an 'analogue life' can be ethically justified to preserve human agency in the face of pressures to digitize everything (Terzis, 2025, p. 55). Ensuring an 'analogue option' in society is a way to respect pluralism in how people choose to live – an idea consonant with democratic principles.

In summary, the right to self-determination in a human rights sense reinforces the arguments from privacy. It holds that individuals should have a say in how technology affects their lives. No one should be deprived of the ability to function in society simply because they refuse a certain technology; self-determination would deem that outcome as fundamentally at odds with the idea of personal freedom. The concept also addresses a potential counter-argument: what about the collective benefits of everyone being on-

line (e.g. efficiency or economic growth)? While legitimate public interests exist in the promotion of digital innovation, self-determination insists that individuals are not sacrificed to a one-size-fits-all mandate, and each person's capacity for choice must be respected. It is part of the pluralism of lifestyles that liberal societies cherish.

3. Freedom of expression and information rights

Freedom of expression under Article 10 ECHR (and Article 11 of the EU Charter) is traditionally understood as the right to impart and receive information and ideas without interference. At first glance, one might associate this right with a push for greater internet access, since the internet is a powerful medium for expression. Indeed, courts have recognized that unfettered access to online information is crucial for modern free speech. In 2009, for example, the French Constitutional Council struck down a law that would have allowed a person's internet access to be cut off without judicial oversight, and held that because the internet is essential for freedom of expression and communication, such a penalty affected fundamental rights (Decision of the French Constitutional Council, 2009). Likewise, in *Ahmet Yıldırım v. Turkey* (2012), the ECtHR held that wholesale blocking of Google sites (which incidentally cut off the applicant's own website) violated Article 10, and emphasized the internet's role in facilitating expression and access to information.

However, freedom of expression also includes a negative dimension: the freedom not to speak or not to be compelled to express oneself. The ECtHR has implicitly recognized negative free speech rights in various contexts. For instance, in the context of freedom of association (Article 11), which is a sibling of expression, the Court explicitly recognized a 'negative right of association', i.e. the right not to be forced to join an association (Judgment of the ECtHR, 1993). By analogy, under Article 10, one could argue there is a 'negative freedom of expression', the right not to be compelled to communicate or to use a particular channel of communication.

Article 10 protects not only the content of information but also the means of its dissemination. The ECtHR has said that the public has the right to receive information through whatever medium they see fit, and states should not unjustifiably favour or impose one medium over another. In *Manole and Others v. Moldova* (2009), the Court noted the importance of pluralism in media and that state dominance or monopolization of a particular medium (like broadcasting) can violate Article 10. Extrapolating from this, if governments eliminate non-digital media (for example, shutting down print services or in-person forums in favour of only digital platforms), one could argue that they are limiting the pluralism of communication channels. The freedom to express oneself 'in the manner of one's choosing' is implicit in the broader freedom.

In *Kalda v. Estonia* (2016), the ECtHR held that even prison inmates have a right to access certain internet websites to exercise their freedom to receive information,

linking Article 10 with new media. Moreover, Article 10 encompasses the right to information, traditionally meaning the right to seek and receive information without interference. The question is: If a government makes information only available online, does that interfere with the right of those who are offline to receive it? The answer is potentially yes. If crucial information (say, polling station locations, public health notices, or legal regulations) is published exclusively on the internet, someone who is offline either by choice or lack of access is cut off from that information. While the state is not actively censoring, it is failing to accommodate different means of reaching the public. The broader principle of technological neutrality in freedom of expression suggests that individuals have the right to access information in a format they can use – which for some means non-digital formats. Thus a right to remain offline can be framed as an aspect of Article 10: the right to access information and to express oneself through non-digital means.

At the European level, Council of Europe bodies have started to acknowledge this balance. The Parliamentary Assembly of the Council of Europe's 2023 resolution on the digital divide (Resolution 2510) underlined that moving to fully online public services can jeopardize equal access to information and services. It called on states to ensure 'full accessibility', including by maintaining non-digital access to public services wherever necessary for equality. Although framed in terms of equality, this also ties into the populace's ability to receive information and communicate with authorities – a precondition for freedom of expression and democratic participation.

In conclusion, while freedom of expression is frequently invoked to justify the expansion of internet connectivity, it also implicitly protects against compelled connectivity. The negative dimension of free speech (the right not to speak) and the right to select one's medium of expression support recognition of a right to remain offline. States must therefore ensure that, in advancing digital innovation, they do not infringe Article 10 by coercing individuals into unwanted forms of communication or by eliminating non-digital channels of access to information.

4. Equality and non-discrimination

A critical human rights perspective on the right not to use the internet is provided by the principles of equality and non-discrimination. Digitalization has the potential to create new forms of exclusion, often along the lines of existing social cleavages such as age, disability, education, income, or geography. Article 14 ECHR guarantees that the enjoyment of the other Convention rights 'shall be secured without discrimination on any ground', while Article 21 of the EU Charter provides a broad stand-alone prohibition of discrimination (on grounds including sex, age, disability, religion, social origin, etc.) within the scope of EU law.

When governments or private actors move essential services exclusively online, they may discriminate against certain groups either directly or indirectly. Requiring internet use for accessing public services, for example, disproportionately affects older adults, who statistically have lower digital literacy, and persons with disabilities who may not be able to use standard web interfaces (Gallistl et al., 2021; Mikołajczyk, 2023; Mubarak & Suomi, 2022). It can also affect those in rural areas with poor connectivity or individuals who simply cannot afford devices or broadband. While 'technology users' versus 'non-users' is not itself a protected category, the overlap with protected characteristics is clear: the digitally excluded are often society's already disadvantaged. The Council of Europe's Parliamentary Assembly recognized in 2023 that 'over 40% of Europe's population lacks basic digital skills' and that these 'digitally vulnerable' groups include the elderly, people with low literacy, migrants, and many persons with disabilities (Kużelewska et al., 2025).

Disability rights law is particularly relevant. The EU is party to the United Nations Convention on the Rights of Persons with Disabilities, which mandates accessibility and reasonable accommodations. Under its Article 9, states must ensure equal access to information and services, including through the provision of assistive technologies or alternative formats. European courts have started to address these issues. The Conseil d'État (Supreme Administrative Court) of France in June 2022 ruled on a challenge to the Ministry of Interior's decision to make certain immigration applications online-only. The Conseil d'État held that while no absolute constitutional right mandated paper procedures in general, the administration must ensure 'normal access' to public services and the effective exercise of rights by all users. This means providing support to those without digital tools or skills, and even alternative solutions for individuals who, 'due to their circumstances and the design of the digital tool', cannot use the online procedure. Because the government had not provided such support or alternatives at the time of implementation, the online-only requirement was deemed illegal.

In the European Union context, the European Commission's 2024 'State of the digital decade' report explicitly notes that 'digital technologies increasingly permeate every aspect of people's daily lives, sometimes with no or limited offline alternatives', and it calls for actions to avoid marginalizing those who are not digitally active (European Commission, 2024). While this is policy, not law, it signals an expectation that Member States ensure digitalization leaves no one behind, which could influence how courts view Member State obligations under, for example, equality laws or the Charter's solidarity provisions. The EU's 2020–2030 Digital Compass strategy sets a target of 100% online public services by 2030, but civil society and EU institutions have noted the paradox: pushing 100% e-services while a significant portion of the population cannot use them is problematic. The solution envisioned includes both digital skills training (upskilling) and retention of multi-channel service delivery until no one is left behind. Moreover, the EU's digital inclusion policies have started to use rights language (Kużelewska et al., 2025).

For instance, Belgium's Wallonia region passed a decree in 2021 requiring that all administrative procedures must still be possible on paper if the user prefers – an explicit legal safeguard for the offline option (Kloza et al., 2025). Similarly, some Swiss cantons have amended their constitutions in 2023–2024 to guarantee a 'right to an offline life', meaning that the government can never make services 100% digital with no alternative. These regional developments, while not country-wide yet, signal a clear normative trend: digitalization should not result in discrimination or exclusion, and offline minorities must be protected (O'Sullivan, March 2025).

To summarize, equality and non-discrimination principles demand that digital innovation be inclusive. The right to remain offline can be framed as a facet of the right to equal treatment: those who do not or cannot use the internet should not suffer arbitrary detriment. States have a positive obligation to ensure that alternatives exist so that, for example, an elderly pensioner can still receive state communications and benefits without the internet, or a rural villager without broadband can access the same information as an urban e-citizen. In the human rights view, technology should be a tool for inclusion, not a basis for discrimination. Therefore any policy of 'digital only' must be scrutinized for its equality impacts and likely tempered by the provision of offline avenues to safeguard the rights of all.

5. Is there a human right to digital non-use?

The analysis above demonstrates that while existing human rights norms could provide significant support for the idea of a right to remain offline, they do so in a piecemeal and implicit fashion. Privacy, autonomy, expression, and equality each contribute pieces of a puzzle – but the question arises: Should these pieces be consolidated into a new explicit right (a right not to use the internet), or is it sufficient to rely on the interpretation of existing rights? This is both a legal-strategic question and a normative one.

Those sceptical of declaring new rights often point to the dangers of 'inflation' of rights. Creating a stand-alone 'right to offline life' could be seen as redundant if all its protections can be derived from rights like privacy and equality (De Hert & Kloza, 2012). Courts are capable of adapting old rights to new contexts; the ECHR's 'living instrument' doctrine means Articles 8 and 10 can evolve to address digital dilemmas. For example, the fact that freedom of expression now covers internet access shows this flexibility of interpretation. By this logic, one might argue that there is no need to formally enshrine a right not to use technology; judges and legislatures can ensure, through nuanced application of existing provisions, that people are not coerced into digital participation.

However, there are strong arguments on the other side – that explicitly recognizing a right to digital self-exclusion would have practical and symbolic benefits (Kloza et al., 2025). One practical benefit is clarity: it would set a clear baseline that no one

can be forced to be online against their will, guiding policy and preventing overreach. Symbolically, it would affirm that human agency and well-being are at the centre of the digital revolution, not technology for its own sake. As Alexander Barclay, a Swiss digital policy expert, noted, elevating such principles to the constitutional level can 'spark a mentality shift' and ensure they are taken seriously by all actors (O'Sullivan, April 2025). Some scholars (Faith & Hernandez, 2024; Kaun, 2021; Turkle, 2011) frame the right to be offline as a necessary counterbalance to the right to internet access, preventing a scenario where what was meant to empower individuals (connectivity) ends up enslaving or coercing them. Furthermore, as Rossi (2023) remarks, sometimes one might want to be offline without any particular reason – and that in itself is a valid exercise of freedom.

Potential objections to a broad right to offline life include concerns regarding practicality, scope, and misuse. Critics may argue that such a right could impede societal progress or governmental efficiency; for instance, if individuals were to invoke the right to rely exclusively on non-digital methods, modern systems might be paralyzed or incur substantial costs. Questions of scope also arise: Does the right permit refusal of any technology, such as electricity or essential ICT necessary for public safety? Additionally, there is the risk of misuse, for example by powerful actors such as corporations seeking to avoid transparency by going 'offline'. However, these concerns can be addressed through a nuanced understanding of the right. It would likely be waivable and context-dependent, designed not to hinder digital innovation but to ensure that alternatives or exemptions are available where fairness and human dignity require them. The right could be framed with reasonable limits, such that individuals could not refuse technologies in ways that harm others. Importantly, it is primarily a defensive right of the individual rather than a tool for corporate actors, who are subject to separate obligations.

In practice, implementing a right to offline life would mean building choice into the system. For government services, it would mean always providing an alternative mode (in person, by phone, or on paper) for those who opt out of digital channels – as advocated by the 'click–call–connect' principle, wherein citizens can choose between online, phone, or face-to-face access (Right to Offline Coalition, 2024). For the private sector, it means ensuring key services (banking, healthcare, utilities) offer non-digital access without extra fees or delay (and possibly regulating to enforce this). For employment, it means strengthening the right to disconnect and perhaps allowing employees to request non-digital workflows if feasible. None of this means halting digital advancements; it means human-centric design that preserves individual choice. In the meantime, developing the academic and doctrinal foundation remains crucial. This article, along with others of its kind, seeks to contribute by weaving disparate threads into a coherent narrative: that the right (not) to use the internet fundamentally concerns the preservation of human choice, dignity, and equality in the digital age.

In closing this discussion on the feasibility of recognizing the right not to use the internet as a distinct human right, it must be acknowledged that at present, such a development is unrealistic, even though the catalogue of human rights remains open. Considering that human rights are characterized by universality, inalienability, and indivisibility, there is currently no basis for establishing a separate human right specifically guaranteeing the right to remain offline. First, such a right can be derived from existing declarations and conventions, making the creation of an additional right unnecessary. Second, there are significant regions of the world where internet access remains limited (World Bank Group, June 2023). For example, according to statistics, only 39% of the population in Africa has internet access (Międzynarodowy Związek Telekomunikacyjny, 2024). Similarly, a joint report by the Inter-American Institute for Cooperation on Agriculture, the Inter-American Development Bank, and Microsoft (IDB, 2020) indicates that 32% of the population in Latin America and the Caribbean lacks internet access. The right not to use the internet, therefore, does not have a universal character but is rather regionally contingent. In Europe, where internet penetration is higher, it may be conceivable to consider introducing a new human right, the right to remain offline. For this reason, however, it is currently not feasible to establish a separate human right specifically guaranteeing the right not to use the internet. Nevertheless, existing human rights provisions appear sufficient to support the exercise of rights associated with remaining offline.

Conclusion

The exploration of privacy, self-determination, freedom of expression, and equality within international and European human rights law reveals a robust foundation for what may be termed a right to digital non-use – the right to remain offline. While no single treaty explicitly states that 'everyone has the right not to use the internet', the current combination of rights and case law effectively recognizes that individuals cannot be compelled to digitalize their lives at the expense of fundamental rights. The right to privacy anchors this understanding by safeguarding personal autonomy, identity, and the intimate sphere of life from unwanted intrusion, which in the contemporary context includes the choice to limit one's exposure to the digital world. The right to self-determination further enshrines personal autonomy, reinforcing that individuals should chart their own course with respect to technology, consistent with their values and needs, without state or societal coercion. Freedom of expression adds a negative dimension, the liberty not to be compelled to communicate in ways one does not choose, and underscores the necessity of pluralistic communicative channels so that offline voices are not silenced. Finally, the rights to equality and non-discrimination ensure that technological advancement does not in-

fringe upon the rights of vulnerable groups, necessitating inclusive design and offline alternatives to prevent the emergence of a digital underclass.

Therefore the research question addressed in this article can be answered affirmatively: based on current human rights regulations and case law, individuals possess a human right to digital non-use. Similarly, the question of whether human rights law protects individuals' freedom to live an analogue existence, and whether such a lifestyle is feasible in the modern world, has also been answered positively. Human rights law does protect the freedom to live offline; however, a separate issue remains as to whether this lifestyle is fully achievable in all its aspects.

In conclusion, digital choice – the freedom to say 'no' as well as 'yes' to connectivity – is emerging as a crucial dimension of human rights in the 21st century. The right not to use the internet does not entail rejecting progress; rather, it ensures that progress is measured in human terms. It asserts that, in the pursuit of a digital society, we must preserve the analogue freedoms that make us human: the freedom to be left alone, to think and live at one's own pace, and not to be involuntarily conscripted into technologies one does not wish to embrace. As this right becomes more firmly established, it will play a vital role in ensuring that the Information Age remains an era of human empowerment rather than digital compulsion.

REFERENCES

Council of Europe Parliamentary Assembly. (2023). *Resolution 2510. Closing the digital divide: Promoting equal access to digital technologies*. https://pace.coe.int/en/files/33001/html

Custers, B. (2019). Nieuwe digitale (grond)rechten. *Nederlands Juristenblad*, *44*, 3288–3295. https://doi.org/10.2139/ssrn.4014541

Decision of the Constitutional Council of France of 10 June 2009, case no. 2009–580 DC.

Decision of the Supreme Administrative Court of France of 3 June 2022, case no. 452798.

De Hert, P., & Kloza, D. (2012). Internet (access) as a new fundamental right: Inflating the current rights framework? *European Journal of Law and Technology*, *3*(3). https://ejlt.org/index.php/ejlt/article/view/123

European Commission. (2024). *State of the digital decade 2024 (Report to the European Parliament and Council)*. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=COM:2024:260:FIN

Faith, B., & Hernandez, K. (2024). Smartphone – and tablet-reliant internet users: Affordances and digital exclusion. *Media and Communication*, *12*. https://doi.org/10.17645/mac.8173

Frosini, T. E. (2014). The internet access as a fundamental right. *Studia Prawnicze*, *1*(14), 5–12.

Gallistl, V., Rohner, R., Hengl, L., & Kolland, F. (2021). Doing digital exclusion: Technology practices of older internet non-users. *Journal of Aging Studies*, *59*, 1–8.

Inter-American Development Bank. (2020, 29 October). *At least 77 million rural inhabitants have no access to high-quality internet services*. https://www.iadb.org/en/news/least-77-million-rural-inhabitants-have-no-access-high-quality-internet-services

International IDEA. (2023). *Rights in the digital age*. International Institute for Democracy and Electoral Assistance. https://www.idea.int/publications/catalogue/html/rights-digital-age

Judgment of the European Court of Human Rights of 30 June 1993 on the case of *James v. United Kingdom*, application no. 8793/79.

Judgment of the European Court of Human Rights of 30 June 1993 on the case of *Sigurður A. Sigurjónsson v. Iceland*, application no. 16130/90.

Judgment of the European Court of Human Rights of 29 April 2002 on the case of *Pretty v. United Kingdom*, application no. 2346/02.

Judgment of the European Court of Human Rights of 4 December 2008 on the case of *S. and Marper v. United Kingdom*, application nos. 30562/04 & 30566/04.

Judgment of the European Court of Human Rights of 17 September 2009 on the case of *Manole and Others v. Moldova*, application no. 13936/02.

Judgment of the European Court of Human Rights of 18 December 2012 on the case of *Ahmet Yıldırım v. Turkey*, application no. 3111/10.

Judgment of the European Court of Human Rights of 19 January 2016 on the case of *Kalda v. Estonia*, application no. 17429/10.

Judgment of the European Court of Human Rights of 24 September 2019 on the case of *Vučina v. Croatia*, application no. 58955/13.

Karaboga, M., Matzner, T., Obersteller, H., & Ochs, C. (2017). Is there a right to offline alternatives in a digital world? In: Leenes, R., van Brakel, R., Gutwirth, S., De Hert, P. (eds) *Data Protection and Privacy: (In)visibilities and Infrastructures. Law, Governance and Technology Series*, vol 36. Springer, Cham. https://doi.org/10.1007/978–3-319–50796-5_2,pp. 31–50).

Kaun, A. (2021). Ways of seeing digital disconnection: A negative sociology of digital culture. *Convergence: The International Journal of Research into New Media Technologies*, *27*(6), 1571–1583. https://doi.org/10.1177/13548565211045535

Kaur, H. (2021). Protecting internet access: A human rights treaty approach. *Brooklyn Journal of International Law*, *46*(2), 767–806.

Kloza, D. (2024). The right not to use the internet. *Computer Law & Security Review*, *52*, 105907. https://doi.org/10.1016/j.clsr.2023.105907.

Kloza, D., Kużelewska, E., Lievens, E., & Verdoodt, V. (Eds.). (2025). *The right not to use the internet: Concept, Contexts, Consequences*. Routledge.

Koops, B.-J., Newell, B. C., Timan, T., Škorvánek, I., Chokrevski, T., & Galič, M. (2017). A typology of privacy. *University of Pennsylvania Journal of International Law*, *38*(2), 483–575.

Kużelewska, E., Tomaszuk, M., & Malinowski, D. (2025). The elderly digital divide: Digital exclusion versus the right not to use the internet. *International Journal for Semiotics of Law*. https://doi.org/10.1007/s11196–025-10334–4

Lucchi, N. (2013). *The role of internet access in enabling individual's rights and freedoms*. European University Institute – RSCAS working paper, 47,1–22.

Międzynarodowy Związek Telekomunikacyjny. (2024, 10 November). *Fakty i liczby 2024 – Użycie internetu*. https://www.itu.int/itu-d/reports/statistics/2024/11/10/ff24-internet-use/

Mikołajczyk, B. (2023). Universal human rights instruments and digital literacy of older persons. *The International Journal of Human Rights*, *27*(3), 403–424.

Miranda Boto, J. M., & Brameshuber, E. (2024). The digitalisation of tools for workers' representation in Europe and Spain: A first approach. *Białostockie Studia Prawnicze*, *29*(2), 209–222.

Mubarak, F., & Suomi, R. (2022). Elderly forgotten? Digital exclusion in the information age and the rising grey digital divide. *The Journal of Health Care Organization, Provision, and Financing*, *59*, 1–7.

O'Sullivan, D. (2025, 23 March). *'It's political': Why some people refuse to have a smartphone*. SwissInfo. https://www.swissinfo.ch/eng/digital-democracy/its-political-why-some-people-refuse-to-have-a-smartphone/89012366

O'Sullivan, D. (2025, 3 April). *How Swiss federalism is helping the rise of a new digital right*. SwissInfo. https://www.swissinfo.ch/eng/digital-democracy/how-swiss-federalism-is-helping-the-rise-of-a-new-digital-right/89023201

Passaglia, P. (2022). *Behind the curtain: Questioning the right to access the internet. In search of definitions (and conditions)*. Völkerrechtsblog. https://doi.org/10.17176/20221017–110251-0

Passaglia, P. (2025). An attempt to conceptualise the right to access the internet and its impact on the right not to use it. In D. Kloza, E. Kużelewska, E. Lievens, & V. Verdoodt (Eds.), *The right not to use the internet: Concept, Contexts, Consequences* (pp. 29–43). Routledge.

Pollicino, O. (2020). The right to internet access: Quid Iuris? In von Arnauld A., von der Decken K., Susi M. (Eds.), *The Cambridge handbook of new human rights* (pp. 263–275). Cambridge University Press. https://doi.org/10.1017/9781108676106.021

Reglitz, M. (2020). The human right to free internet access. *Journal of Applied Philosophy*, *37*(2), 314–331. https://doi.org/10.1111/japp.12395

Reglitz, M. (2023). The socio-economic argument for the human right to internet access. *Politics, Philosophy & Economics*, *22*(4), 441–469. https://doi.org/10.1177/1470594X231167597

Reglitz, M. (2024). *Free internet access as a human right*. Cambridge University Press.

Right to Offline Coalition. (2024). *Essential services must be accessible, even offline: The open letter*. https://righttooffline.eu/?lang=en

Rossi, J. (2025). Is there a right to be offline "for no reason" in France?. In D. Kloza, E. Kużelewska, E. Lievens, & V. Verdoodt (Eds.), *The right not to use the internet: Concept, Contexts, Consequences* (pp. 76–91). Routledge.

Shandler, R., & Canetti, D. (2019). A reality of vulnerability and dependence: Internet access as a human right. *Israel Law Review*, *52*(1), 77–98. https://doi.org/10.1017/S0021223718000262

Susi, M. (2025). Framing the right not to use the internet. In D. Kloza, E. Kużelewska, E. Lievens, & V. Verdoodt (Eds.), *The right not to use the internet: Concept, Contexts, Consequences* (pp. 44–63). Routledge.

Terzis, G. (2025). Ethical meditations for a human right to an analogue life. In D. Kloza, E. Kużelewska, E. Lievens, & V. Verdoodt (Eds.), *The right not to use the internet: Concept, Contexts, Consequences* (pp. 7–28). Routledge.

Tomalty, J. (2017). Is there a human right to internet access? *Philosophy Now*, *118*, 8–11. https://philosophynow.org/issues/118/Is_There_A_Human_Right_To_Internet_Access

Turkle, S. (2011). *Alone together: Why we expect more from technology and less from each other*. Basic Books.

Warren, S., & Brandeis, L. (1890). The right to privacy. *Harvard Law Review*, *4*(5), 193–220.

Whitman, J. Q. (2004). The two western cultures of privacy: Dignity versus liberty. *Yale Law Journal*, *113*(6), 1151–1221.

Wiśniewski, A. (2021). The European Court of Human Rights and internet-related cases. *Białostockie Studia Prawnicze*, *26*(3), 109–133.

World Bank Group. (2023, 27 June). *From connectivity to services: Digital transformation in Africa*. https://www.worldbank.org/en/results/2023/06/27/from-connectivity-to-services-digital-transformation-in-africa

Bialystok Legal Studies
Białostockie Studia Prawnicze
2025 vol. 30 no. 4

sciendo

DOI: 10.15290/bsp.2025.30.04.05
Received: 12.07.2025
Accepted: 23.09.2025

Katarzyna Sakowska
Uniwersytet w Białymstoku, Polska
k.sakowska@uwb.edu.pl
ORCID ID: 0009–0008–7148–4731

Karolina Zapolska
Uniwersytet w Białymstoku, Polska
k.zapolska@uwb.edu.pl
ORCID ID: 0000–0003–2859–6996

Czas pracy a prawo do bycia offline – analiza w świetle koncepcji „non-use of technology" w prawie polskim i unijnym[1]

Working Time and the Right to Be Offline: Analysis in the Light of the Concept of Non-Use of Technology in Polish and EU Law

Abstract: The development of technology undoubtedly affects the way work is performed. New digital tools significantly influence the performance of work, on the one hand introducing flexibility and new opportunities, but also leading to the blurring of boundaries between the professional and private spheres. The increasingly widespread use of digital tools – including communication and monitoring applications – creates new challenges in the area of employee privacy protection and the realization of the right to rest. In this context, growing emphasis is placed on the concept of non-use of technology, which denotes the right to refrain from using technology in the name of autonomy and well-being, as well as on the right to disconnect, understood as the employee's entitlement to be unavailable outside working hours. Both concepts complement each other and may constitute an element of employee rights protection. The aim of this study is to present the essence of the right to disconnect and its connection with working time and the right to rest, as well as to indicate the extent to which EU and Polish regulations provide protection against the culture of permanent availability. The analysis encompasses legal acts, case law, and scholarly literature, which allows for an assessment of whether the right to disconnect

1 The article is financially supported by the Polish Minister of Science under the 'Regional Initiative of Excellence' (RID) programme.

should be regarded as an instrument supplementing traditional labour law provisions in the context of advancing digitalization.

Key words: employees, employers, entrepreneurs, right to be offline, not using technology, labour law
Słowa kluczowe: pracownik, pracodawca, przedsiębiorca, prawo do bycia offline, non-use of technology, prawo pracy

Wprowadzenie

Wpływ nowych technologii na sposób świadczenia pracy jest niezaprzeczalny (szerzej: Boruta, 2020, s. 3–10; Piwowarska, 2018, s. 135–155). Nowe narzędzia i rozwiązania cyfrowe w realny sposób wpływają na sposób wykonywania pracy. W tym zakresie można wskazać między innymi na szanse, jakie dają elastyczne formy zatrudnienia i regulacji czasu pracy. Niewątpliwie obie te możliwości niosą za sobą wiele korzyści, ale mogą również prowadzić do zacierania granic między sferą zawodową a prywatną (Pachała-Szymczyk, 2022, s. 9). W związku z tym wraz z dynamicznym rozwojem nowych technologii oraz coraz szerszym zakresem ich zastosowania w działalności gospodarczej i organizacji pracy pojawiły się nowe wyzwania i zagrożenia, w tym związane z utrzymaniem równowagi między życiem zawodowym a prywatnym (Kurzynoga, 2022, s. 3–4). Pracownicy w ramach świadczonej pracy coraz częściej są zależni od komunikatorów czy też aplikacji umożliwiających planowanie czy nadzorowanie pracy. Nowe technologie wpływają również na podejście do rynku pracy i samej pracy, czego wyrazem jest nowy model biznesowy określany terminami *platform economy*, *gig econo*my, *on-demand economy*, *sharing econom*', *peer-to-peer economy* lub *uber economy*, w którym przedsiębiorcy „świadczą [...] swoje usługi przy użyciu osób samozatrudnionych" (Skowron, 2019, s. 153; Zapolska & Nyka, 2024, s. 187; Todolí-Signes & Tyc, 2016, s. 197).

W tym kontekście na znaczeniu zyskują koncepcja *non-use technology*, a także prawo do bycia offline (inaczej prawo do odłączenia się, ang. *right to disconnect*) jako swoista odpowiedź na zacierającą się granicę między życiem zawodowym i prywatnym. Oba zagadnienia są stosunkowo nową problematyką w zakresie prawa pracy, niemniej ze względu na postępującą cyfryzację zyskują na znaczeniu i zaczynają być dostrzegane przez doktrynę prawa, ale także ustawodawcę zarówno unijnego, jak i polskiego. Sama koncepcja *non-use of technology* sprowadza się do zapewnienia prawa o decydowaniu, czy chcemy czy też nie korzystać z nowych technologii, a więc swoistej wolności od „przymusu technologicznego" (Satchell & Dourish, 2009, s. 11). Jest to szczególnie istotne z perspektywy dobrostanu, autonomii czy też potrzeby prywatności pracowników. Stanowi jednocześnie interesujące zagadnienie w kontekście prawa pracy i problematyki prawa do bycia offline, które wiążą się m.in. z niedostępnością poza godzinami pracy. Jest w związku z tym silnie powiązane z prawem do odpoczynku pracownika. Obie koncepcje wzajemnie się uzupełniają. Dodatkowo

wydaje się, że koncepcja *non-use of technology* może stanowić podstawę do uznania prawa do bycia offline jako elementu szerszej autonomii cyfrowej pracownika.

Celem opracowania jest zdefiniowanie istoty prawa do bycia offline i ukazanie jego ścisłego związku z czasem pracy oraz prawem do odpoczynku. Analizie poddane zostaną regulacje zarówno unijne, jak i polskie, a także orzecznictwo, aby wskazać, w jakim zakresie zapewniają one ochronę pracownika przed kulturą stałej dostępności. Dodatkowo opracowanie ma na celu przedstawienie koncepcji *non-use of technology* jako perspektywy teoretycznej oraz porównanie polskich i unijnych rozwiązań, co pozwoli wyznaczyć możliwe kierunki dalszego rozwoju prawa pracy. W konsekwencji niniejsze opracowanie posługuje się metodą dogmatyczno-prawną obejmującą przede wszystkim analizę aktów prawa, takich jak dyrektywy UE i Kodeks pracy, a także orzecznictwa TSUE oraz polskiej i zagranicznej literatury naukowej.

1. Koncepcja *non-use* of technology

Zagadnienie *non-use of technology* (inaczej ang. *technology refusal*, *digital minimalism* lub *technological non-participation*) w dobie gwałtownie rozwijających się i co więcej, w wyraźny sposób wpływających na nasze codzienne życie nowych technologii, jest niezwykle ważne. To nurt w refleksji nad społeczeństwem cyfrowym, który jest swoistym kontrapunktem, czyli przeciwieństwem czy też uzupełnieniem, w czasach dość powszechnego entuzjazmu w podejściu do nowych technologii i możliwości, jakie dają. Koncepcja *non-use of technology* sprowadza się przede wszystkim do prawa do świadomego nieużywania czy też niekorzystania z nowych technologii (Nguyen & Hargittai, 2023, s. 495). Nie chodzi zatem o brak dostępu lub c wykluczenie cyfrowe, lecz o wybór (Satchell & Dourish, 2009, s. 11), co bezpośrednio wiąże się z próbą odzyskania kontroli i autonomii w korzystaniu z narzędzi cyfrowych. Zgodnie z tym podejściem jednostka ma prawo do rezygnacji i nieuczestniczenia w cyfrowych praktykach, co wydaje się szczególnie problematyczne w erze cyfrowej (Nguyen & Hargittai, 2023, s. 495), zwłaszcza że w rzeczywistości zarówno prywatnej, jak i zawodowej bycie online staje się swoistą normą (szerzej: Vorderer et al., 2016, s. 694–695), a wiele osób odczuwa presję społeczną, aby stale funkcjonować cyfrowo (Büchi, Festic, & Latzer, 2019, s. 4). Jak zauważa E. Baumer, badanie koncepcji *non-use* pozwala zakwestionować domyślne założenie dotyczące prymatu używania i samego pojęcia „użytkownika" oraz tego, kto powinien nim być (Baumer et al., 2014, s. 66). Wydaje się, że z samą koncepcją *non-use of technology* wiąże się też konieczność zapewnienia alternatyw offline, czyli np. dostępu do usług pracowniczych bez konieczności posługiwania się aplikacją mobilną, czy też prawo do wykonywania określonych obowiązków zawodowych bez konieczności stałego bycia online (Satchell & Dourish, 2009, s. 11). E. Baumer dodatkowo podkreśla, że analiza sytuacji, w których ludzie świadomie ograniczają lub odrzucają technologię, jest równie istotna jak

badania odnoszące się do jej używania, ponieważ pokazuje realne potrzeby związane z funkcjonowaniem poza infrastrukturą cyfrową (Baumer et al., 2014, s. 65).

Powstaje w tym przypadku wątpliwość, na ile z samej koncepcji *non-use of technology* mógłby skorzystać pracownik. Wydaje się, że w tym przypadku sprowadzałaby się ona w praktyce m.in. do rezygnacji z niektórych narzędzi cyfrowych lub rozwiązań technologicznych. Wiąże się również z pytaniem, czy możemy mówić o przymusie cyfrowym również w kontekście zatrudnienia – w sytuacji, gdy korzystanie z niej staje się jednym z warunków zatrudnienia. Sama koncepcja *non-use of technology* to też sprzeciw wobec przymusu bycia stale online. Czy pracownik może przykładowo zrezygnować z aplikacji służbowej, która zbiera jego dane, również poza godzinami pracy? Czy pracownicy są zobowiązani do instalowania służbowych komunikatorów na telefonie lub komputerze, czy też mają prawo odmówić? Niewątpliwie pewne jej elementy są dostrzegalne w tzw. prawie do bycia offline.

2. Pojęcie prawa do bycia offline w Unii Europejskiej

Jak zauważają E. Kryńska i E. Kwiatkowski, rynek pracy jest miejscem, „w którym dokonują się transakcje wymiany usług pracy między pracownikami a pracodawcami oraz ustalają się rozmiary wspomnianych transakcji i ich warunki, a zwłaszcza cena tych usług, tj. płaca" (Kryńska & Kwiatkowski, 2013, s. 11). Co istotne, pracodawca w tym zakresie „nabywa" prawo do dysponowania zdolnością pracownika do świadczenia pracy w wyznaczonym czasie, a więc „kupuje" dostęp do czasu i sił pracownika (Beksiak, 2014, s. 149). Obecny rynek pracy podlega dynamicznym zmianom, na co wpływ ma szereg różnych czynników ekonomicznych, demograficznych, społecznych oraz prawnych, zarówno o charakterze globalnym, jak i lokalnym. Dostrzegalne zmiany w tym zakresie są związane m.in. z „przyśpieszeniem postępu technicznego w obszarze technologii informacyjnych i telekomunikacyjnych czy nowymi strategiami wielkich korporacji" (Kotlorz, 2011, s. 10).

Upowszechnienie się narzędzi cyfrowych w ramach rynku pracy miało oczywiście swoje konsekwencje. Pojawiły się problemy związane z nadużywaniem możliwości, jakie daje wykorzystanie nowych technologii w miejscu pracy. Jednym z takich negatywnych zjawisk jest tzw. kultura „wiecznie osiągalnego pracownika" (ang. *always-on culture*) i związane z nią zaburzenie relacji między czasem pracy a prawem do odpoczynku. E. Pachała-Szymczyk wskazuje, że „z badań wynika, iż pracownicy często wykorzystujący technologie informacyjno-komunikacyjne są bardziej skłonni do dłuższych godzin pracy i pracy w godzinach nadliczbowych; korzystają również w mniejszym zakresie z okresów odpoczynku, a także mają mniej przewidywalne, nieregularne rozkłady czasu pracy" (Pachała-Szymczyk, 2022, s. 9). W literaturze słusznie podkreśla się w tym zakresie, że jedną z konsekwencji takiego podejścia jest m.in. wypalenie zawodowe (Nowak, 2019, s. 15).

Nie zaskakuje zatem, że w orzecznictwie TSUE zaczęto interpretować takie pojęcia jak „czas pracy" i „czas odpoczynku" również w kontekście nowych technologii. W tym zakresie można wskazać m.in. na sprawę C-55/18 Federación de Servicios de Comisiones Obreras – CCOO przeciwko Deutsche Bank SAE, w której TSUE analizował kwestię prowadzenia systemu ewidencji czasu pracy (rozumianego jako pomiar dobowego czasu pracy świadczonej przez każdego pracownika), aby zagwarantować przestrzeganie limitów pracy i odpoczynku. Co charakterystyczne, w wyroku C-531/23 z 23 grudnia 2024 r. TSUE stwierdził, że pracodawcy zatrudniający pracowników domowych powinni wprowadzić system pozwalający dokonywać pomiaru czasu pracy. Jednocześnie TSUE stwierdził, że możliwe są w tym zakresie odstępstwa „stosownie do danego sektora działalności, czy to ze względu na specyfikę danego pracodawcy, a zwłaszcza na jego rozmiar, o ile takie uregulowanie zapewnia pracownikom skuteczne rozwiązania pozwalające zagwarantować poszanowanie przepisów dotyczących między innymi maksymalnego tygodniowego wymiaru czasu pracy" (Wyrok C-531/23, 2024).

Jak podkreślono w sprawie C-518/15 Ville de Nivelles przeciwko Rudy Matzak, „Trybunał wielokrotnie stwierdził bowiem, że pojęcie „czasu pracy" [...] należy definiować według obiektywnych cech, odwołując się do systematyki i celu tej dyrektywy, dążącej do poprawy warunków życia i pracy pracowników. Pojęcie to zależy od trzech przesłanek: po pierwsze, pracownik musi „pracować"; po drugie, musi on pozostawać w dyspozycji pracodawcy; oraz po trzecie, musi on wypełniać swe zadania i obowiązki". Trybunał wypowiedział się również w kwestii odpoczynku dobowego i odpoczynku tygodniowego. W tym zakresie można wskazać m.in. na sprawę C-477/21IH przeciwko MÁV-START Vasúti Személyszállító Zrt., w której TSUE stwierdził, że „odpoczynek dobowy [...] nie stanowi części okresu odpoczynku tygodniowego [...], lecz dodaje się do niego". Ponadto, TSUE podkreślił, że „po okresie pracy każdy pracownik powinien niezwłocznie korzystać z okresu odpoczynku dobowego, i to niezależnie od tego, czy po tym okresie odpoczynku nastąpi okres pracy. Ponadto, w razie gdy odpoczynek dobowy i okres odpoczynku tygodniowego są udzielane w sekwencji, okres odpoczynku tygodniowego może rozpocząć się dopiero wtedy, gdy pracownik skorzysta z odpoczynku dobowego". Kwestia „gotowości do pracy" w kontekście „prawa do odpoczynku" i „czasu pracy" była natomiast przedmiotem m.in. w sprawach C-303/98 Simap, C-151/02 Jaeger, C-518/15 Ville de Nivelles przeciwko Rudyemu Matzakowi, C-344/19, D.J. przeciwko Radiotelevizija Slovenija czy też C-585/19, Academia de Studii Economice din Bucureşti przeciwko Doru Viorel Bălăn.

Na tle wspomnianego orzecznictwa zaczęto dostrzegać znaczenie prawa do bycia offline w kontekście równowagi między życiem zawodowym a prywatnym (koncepcja *work-life balance*). Należy jednak wyraźnie zaznaczyć, że prawo do bycia offline nie jest prawem funkcjonującym w oderwaniu od innych gwarancji pracowniczych. Nie funkcjonuje zatem jako odrębna i niezależna kategoria, lecz stanowi swoiste uszczegółowienie i wzmocnienie prawa do odpoczynku. Jak podkreśla K. Moras-Olaś, instytu-

cja ta wprost wiąże się z ochroną prawa pracownika do wyłączenia narzędzi cyfrowych (Moras-Olaś, 2021, s. 305). W konsekwencji prawo do bycia offline dotyczy wyłącznie okresów poza czasem pracy. Autorka dodatkowo zauważa, że zgodnie z podejściem zaprezentowanym w dokumencie roboczym Eurofound *The Right to Disconnect in the 27 EU Member States* prawo do bycia offline można rozumieć na dwa sposoby: „jako uprawnienie pracownika do powstrzymania się od pracy poza czasem pracy za pośrednictwem narzędzi cyfrowych, albo jako obowiązek pracodawcy zapewnienia, że pracownicy nie będą pracować w czasie odpoczynku i urlopu" (Moras-Olaś, 2021, s. 311). Jego istotą jest w związku z tym zapewnienie, że w okresach poza czasem pracy pracownik nie będzie zobowiązany do pozostawania w dyspozycji pracodawcy za pomocą narzędzi cyfrowych. Warto podkreślić, że w czasie pracy pracownik co do zasady nie może odmówić pozostawania online w zakresie zgodnym z prawem oraz wyznaczonym i wymaganym przez pracodawcę. Oznacza to, że prawo do bycia offline rozpoczyna się dopiero w momencie rozpoczęcia okresu odpoczynku, gdy pracownik nie pozostaje w dyspozycji pracodawcy (Sakowska, 2025a, s. 348).

K. Naumowicz wskazuje, że brak wyraźnych regulacji prawnych może prowadzić w praktyce do świadczenia pracy poza regularnymi godzinami, co stanowi istotne zagrożenie dla realizacji prawa do odpoczynku (Naumowicz, 2021, s. 537–538). Samo prawo do bycia offline nie jest bowiem w wyraźny sposób uregulowane w prawie Unii Europejskiej. Można je jednak wywnioskować, biorąc pod uwagę art. 31 Karty praw podstawowych Unii Europejskiej, zgodnie z którym każdy pracownik ma prawo do warunków pracy zapewniających poszanowanie jego zdrowia, bezpieczeństwa i godności, do ograniczenia maksymalnego wymiaru czasu pracy, do okresów dziennego i tygodniowego odpoczynku oraz do corocznego płatnego urlopu. Ważną rolę w tym zakresie odgrywa również dyrektywa 2003/88/WE Parlamentu Europejskiego i Rady z dnia 4 listopada 2003 r. dotycząca niektórych aspektów organizacji czasu pracy[2], która reguluje kwestie czasu pracy i odpoczynku w Unii Europejskiej. Dyrektywa wprowadziła m.in. prawo do minimalnego dziennego wypoczynku (odpoczynek dobowy) – 11 nieprzerwanych godzin, w okresie 24-godzinnym (art. 3 dyrektywy 2003/88/WE), prawo do odpoczynku tygodniowego – 24 godziny (art. 5 dyrektywy 2003/88/WE) czy maksymalny tygodniowy czas pracy – przeciętny wymiar czasu pracy w okresie siedmiodniowym, łącznie z pracą w godzinach nadliczbowych, nie może przekraczać 48 godzin (art. 6 dyrektywy 2003/88/WE).

Analizując zagadnienie prawa do bycia offline w UE, warto wspomnieć o Rezolucji Parlamentu Europejskiego z dnia 21 stycznia 2021 r. zawierającej zalecenia dla Komisji w sprawie prawa do bycia offline, w której podkreślono, że „coraz częstsze wykorzystywanie narzędzi cyfrowych do celów zawodowych doprowadziło do powstania kultury „stale osiągalnego", „zawsze dostępnego" lub „będącego w ciągłej gotowości" pracownika, co może mieć szkodliwy wpływ na prawa podsta-

2 Dalej jako dyrektywa 2003/88/WE.

wowe pracowników i sprawiedliwe warunki pracy". Dodatkowo wskazano, że „prawo pracowników do bycia offline ma zasadnicze znaczenie dla ochrony ich zdrowia i samopoczucia fizycznego i psychicznego oraz ochrony przed zagrożeniami psychologicznymi" (Rezolucja, 2021). Pracownik ma zatem prawo np. do nieodbierania służbowych wiadomości poza godzinami pracy bez konsekwencji ze strony pracodawcy. W praktyce oznacza to, że pracodawca nie powinien wymagać od pracownika dyspozycyjności za pomocą środków komunikacji elektronicznej poza ustalonymi godzinami pracy (Naumowicz, 2022, s. 542). Takie oczekiwania ze strony pracodawcy mogą prowadzić do faktycznego naruszania prawa do odpoczynku, nawet jeśli formalnie normy czasu pracy nie zostały przekroczone. Oznacza to w praktyce zakaz wywierania na pracowniku presji, aby poza godzinami pracy odpowiadał na wiadomości służbowe, odbierał telefony czy posiadał status „dostępny" w ramach różnych platform i komunikatorów, np. Teams (Sakowska, 2025a, s. 344).

Sama rezolucja podchodzi do zagadnienia prawa do bycia offline jako prawa podstawowego (Pachała-Szymczyk, 2022, s. 11). Wydaje się, że samo prawo do bycia offline można rozumieć jako prawo do odpoczynku od pracy w świecie cyfrowym lub od narzędzi cyfrowych. Wiąże się zatem z zakazem ustanowienia wymogu dostępności pracownika poza godzinami pracy czy też zobowiązaniem pracodawcy do jasnego określenia godzin, w których możliwe jest skontaktowanie się z pracownikiem w sprawach służbowych. Dlatego omawiane w literaturze rozwiązania i orzecznictwo TSUE nie tworzą odrębnego reżimu prawnego, lecz stanowią element szerszej gwarancji prawa do odpoczynku, które powinno być dostosowane do wyzwań wynikających z cyfryzacji pracy. Jest to więc prawo o charakterze ochronnym, które ma służyć temu, aby przepisy dotyczące czasu pracy i odpoczynku były skuteczne i efektywne w warunkach dynamicznego rozwoju nowych technologii.

W 2019 roku dodatkowo przyjęto: 1) dyrektywę Parlamentu Europejskiego i Rady (UE) 2019/1152 z dnia 20 czerwca 2019 r. w sprawie przejrzystych i przewidywalnych warunków pracy w Unii Europejskiej[3] oraz 2) dyrektywę Parlamentu Europejskiego i Rady (UE) 2019/1158 z dnia 20 czerwca 2019 r. w sprawie równowagi między życiem zawodowym a prywatnym rodziców i opiekunów oraz uchylającą dyrektywę Rady 2010/18/UE[4]. W dyrektywie 2019/1152 wskazano m.in. na kwestię związaną z określeniem godzin pracy czy przewidywalności rozkładu czasu pracy, co pośrednio wspiera koncepcję prawa do bycia offline i może być podstawą do zakwestionowania praktyk naruszających prawo do prywatności poza godzinami pracy. Natomiast w dyrektywie 2019/1158 promuje się prawo do elastycznej organizacji pracy.

3. Polskie przepisy gwarantujące pracownikom prawo do odpoczynku

3 Dalej jako dyrektywa 2019/1152.

4 Dalej jako dyrektywa 2019/1158.

Co charakterystyczne, polski kodeks pracy[5] nie zawiera regulacji odnoszących się bezpośrednio do prawa pracownika do bycia offline (Sakowska, 2025a, s. 347), co jednak nie oznacza, że pracownicy są całkowicie pozbawieni ochrony przed nadużywaniem pozycji nadrzędnej przez pracodawcę, a tym samym nienormowanym czasem pracy. Przepisy kodeksowe o czasie pracy zapewniają maksymalne okresy, w których pracownicy mogą wykonywać obowiązki pracownicze, a także minimalne okresy odpoczynku. Zgodnie z art. 128 KP czasem pracy jest czas, w którym pracownik pozostaje w dyspozycji pracodawcy w zakładzie pracy lub w innym miejscu wyznaczonym do wykonywania pracy. Pozostawanie w dyspozycji oznacza więc nie tylko czas faktycznego wykonywania pracy, lecz także okres, w którym pracownik nie świadczy pracy, jednak pozostaje w faktycznej gotowości do jej świadczenia w miejscu pracy (Sobczyk, 2005, s. 116–117; postanowienie Sądu Najwyższego, 2019). W literaturze podkreśla się, że pracownik pozostaje w dyspozycji pracodawcy również wtedy, gdy nie świadczy pracy, ale znajduje się we właściwym stanie psychofizycznym pozwalającym na realizację obowiązków oraz ma zamiar i możliwość ich wykonywania (Pisarczyk, 2017, s. 781).

Wymiar czasu pracy w podstawowym systemie czasu pracy określa art. 129 KP, zgodnie z którym czas pracy nie może przekraczać 8 godzin na dobę i przeciętnie 40 godzin w przeciętnie pięciodniowym tygodniu pracy w przyjętym okresie rozliczeniowym nieprzekraczającym 4 miesięcy. Ponadto, art. 131 KP wprowadza kolejne ograniczenie, na podstawie którego tygodniowy czas pracy łącznie z godzinami nadliczbowymi nie może przekraczać przeciętnie 48 godzin w przyjętym okresie rozliczeniowym. Z drugiej zaś strony, art. 132 i 133 KP wprowadzają minimalne i nieprzekraczalne okresy odpoczynku od pracy – w każdej dobie pracownikowi przysługuje prawo do co najmniej 11 godzin nieprzerwanego odpoczynku, natomiast w każdym tygodniu – prawo do co najmniej 35 godzin nieprzerwanego odpoczynku, obejmującego co najmniej 11 godzin nieprzerwanego odpoczynku dobowego.

Choć polskie przepisy regulują czas pracy i odpoczynku, nie da się ukryć, że nie zawsze odpowiadają w wystarczający sposób na wyzwania związane z cyfryzacją pracy. W polskim porządku prawnym prawo do bycia offline nie zostało wyodrębnione jako samodzielna instytucja prawa pracy – wynika ono pośrednio z regulacji dotyczących minimalnych okresów odpoczynku dobowego i tygodniowego. W praktyce sprowadza się ono do zagwarantowania pracownikom realizacji prawa do odpoczynku. W konsekwencji pracownik powinien być chroniony przed wymogiem stałej dostępności elektronicznej poza czasem pracy (Pachała-Szymczyk, 2022, s. 9). Ingerencja pracodawcy w tym okresie może być traktowana jako naruszenie przepisów o minimalnych okresach odpoczynku. Oczekiwanie pracodawcy, aby pracownik pozostawał dostępny cyfrowo poza czasem pracy, ogranicza faktyczną możliwość korzystania z prawa do odpoczynku. Prawo do bycia offline można zatem rozumieć

5 Dalej KP.

jako instrument realizujący lub wspomagający już istniejące rozwiązania i uprawnienia pracownika, w szczególności prawo do nieprzerwanego odpoczynku dobowego i tygodniowego (szerzej: Moras-Olaś, 2021, s. 311). Prawo do bycia offline w tym ujęciu pełniłoby funkcję gwaranta realizacji prawa do odpoczynku. Należy jednak podkreślić, że prawo do bycia offline nie oznacza możliwości odmowy korzystania z technologii w czasie pracy – kiedy pracownik pozostaje w dyspozycji pracodawcy – lecz odnosi się wyłącznie do okresów, w których pracownik nie świadczy pracy i nie ma obowiązku pozostawania w gotowości (Sakowska, 2025a, s. 347–348).

Biorąc pod uwagę powyższe, należy stwierdzić, że regulacje ograniczające czas pracy pracownika są rozbudowane i kompleksowe, jednak niezbędne jest dostosowanie powyższych reguł do aktualnych realiów społeczno-gospodarczych. Mowa tu w szczególności o postępującym rozwoju nowych technologii, który wywiera niewątpliwy wpływ na stosunki pracy. Zacieranie się granicy między czasem pracy a czasem wolnym, wynikające z cyfryzacji, sprawia bowiem, że formalne limity czasu pracy mogą być w praktyce obchodzone przez oczekiwanie od pracowników stałej dyspozycyjności (szerzej: Pachała-Szymczyk, 2022, s. 9; Chesalina, 2021, s. 37). W tym sensie brak wyraźnego uregulowania prawa do bycia offline należy uznać za lukę w systemie ochrony pracownika (Naumowicz, 2021, s. 537–538). Dlatego konieczne staje się wypracowanie rozwiązań prawnych, które zapewnią pracownikowi realne korzystanie z prawa do odpoczynku w warunkach rozwoju technologii cyfrowych.

Można zaryzykować stwierdzenie, że obecnie stosunek pracy uległ swoistej transformacji, biorąc pod uwagę trzy podstawowe kwestie, które decydowały o szczególnym charakterze stosunku pracy: podporządkowanie pracownika pracodawcy, miejsce i czas wykonywania pracy. W tych nowych realiach pojawia się pytanie, jak zagwarantować pracownikowi realne korzystanie z prawa do odpoczynku bez zakłóceń wynikających z nadużywania przez pracodawcę nowych technologii. Wydaje się, że w tym zakresie prawo do bycia offline może być instrumentem uzupełniającym tradycyjne przepisy o czasie pracy, stając się tym samym dodatkową ochroną przed nadmierną ingerencją pracodawcy w sferę życia prywatnego pracownika.

4. Wybrane wyzwania związane ze stosowaniem prawa do bycia offline

Pandemia COVID-19 miała niewątpliwy wpływ na zmianę zasad wykonywania pracy. Rozwój nowych technologii, w tym cyfryzacja, automatyzacja oraz powszechne wykorzystanie Internetu, znacząco przekształciły krajobraz rynku pracy, stawiając przed prawem pracy wiele wyzwań. Praca może być wykonywana w innym miejscu niż zakład pracy oraz poza zwyczajowymi godzinami pracy obowiązującymi u danego pracodawcy. Cyfrowe narzędzia pracy umożliwiają pracę w zasadzie z dowolnego miejsca, co zwiększa elastyczność zatrudnienia i pozwala pracownikom na efektywniejsze zarządzanie czasem (Sakowska, 2025b, s. 116–117). Z drugiej jednak strony, możliwość

wykonywania pracy z każdego miejsca i w każdym czasie za pomocą nowoczesnych technologii może prowadzić do ciągłej dostępności pracownika dla pracodawcy.

Jeżeli mowa o zmianie paradygmatu stosunku pracy w zakresie miejsca pracy (Spytek-Bandurska, 2024), największym jej przejawem jest zdecydowanie praca zdalna, która pojawiła się w KP w 2023 roku. Zgodnie z art. 67^{18} KP praca zdalna może być wykonywana całkowicie lub częściowo w miejscu wskazanym przez pracownika i każdorazowo uzgodnionym z pracodawcą, w tym pod adresem zamieszkania pracownika, w szczególności z wykorzystaniem środków bezpośredniego porozumiewania się na odległość. W przypadku pracy zdalnej doszło do ingerencji ustawodawcy w kompetencje kierownicze pracodawcy – zmianie uległy zarówno czas, jak i miejsce świadczenia pracy, a także związane z tym możliwości sprawowania kontroli przez pracodawcę (Krysiak, 2024, s. 83). Najważniejszym aspektem pracy zdalnej jest natomiast możliwość jej świadczenia poza zakładem pracy przy użyciu cyfrowych narzędzi pracy.

Aby pracownik mógł wykonywać pracę w formie zdalnej, konieczne jest uprzednie jej uzgodnienie pomiędzy pracodawcą i pracownikiem – wyjątkowo ustawodawca dopuszcza możliwość polecenia pracownikowi wykonywania pracy zdalnej przez pracodawcę: w okresie obowiązywania stanu nadzwyczajnego, stanu zagrożenia epidemicznego albo stanu epidemii oraz w okresie 3 miesięcy po ich odwołaniu lub w okresie, w którym zapewnienie przez pracodawcę bezpiecznych i higienicznych warunków pracy w dotychczasowym miejscu pracy pracownika nie jest czasowo możliwe z powodu działania siły wyższej (art. 67^{19} § 3 KP). Jednocześnie w kodeksowej definicji pracy zdalnej jednym z podstawowych elementów jest „wykorzystanie środków bezpośredniego porozumiewania się na odległość". KP nie ustanawia natomiast wymogu, aby pracownik wykonujący pracę zdalną znajdował się w ciągłym kontakcie z pracodawcą. Korzystanie ze środków bezpośredniego porozumiewania się na odległość stanowi wyłącznie przykład sposobu wykonywania pracy zdalnej, o czym przesądza sformułowanie „w szczególności". W odniesieniu do poprzedniczki pracy zdalnej w KP, czyli telepracy, nie ustanowiono także wymogu przekazywania wyników pracy w sposób zdalny (Sobczyk, 2023, komentarz do art. 67^{18} KP), co oznaczałoby, że pracownik może uzgodnić z pracodawcą cotygodniowe dostarczenie wyników wykonanej pracy przykładowo w formie pisemnej.

W opinii autorek immanentną cechą pracy zdalnej jest możliwość zdalnego komunikowania się z pracodawcą i, biorąc pod uwagę podstawowe cechy pracy zdalnej, rezygnacji z szeroko rozumianych narzędzi cyfrowych opartych na nowych technologiach, przy założeniu, że większość działań pracodawcy nie opiera się na rozwiązaniach cyfrowych, co będzie jednak stanowić margines przypadków. Aktualny rynek pracy uległ znaczącym zmianom technologicznym – pracodawca jest uprawniony do prowadzenia dokumentacji pracowniczej w formie elektronicznej, zazwyczaj dostarcza on również pracownikom odpowiednie narzędzia do pracy, takie jak laptop czy monitor, wszelkie listy obecności zostały zastąpione przez karty magnetyczne lub aplikacje. Jeżeli więc działalność pracodawcy odbywa się wyłącznie elektronicznie

lub „w chmurze", przekazywanie wyników wykonanej pracy w formie innej niż elektroniczna może być utrudnione, jednak nie niemożliwe. Należy mieć jednak na uwadze fakt, że w większości przypadków pracownik, który ma zamiar wykonywać pracę zdalną, godzi się na używanie rozwiązań cyfrowych. Niejednokrotnie pracownik podejmuje decyzję o pracy zdalnej z uwagi na uprawnienie do wykonywania pracy zdalnej poza zakładem pracy i jednocześnie kontakt z pracodawcą i udostępnianie wyników swojej pracy przy użyciu rozwiązań nowych technologii.

Praca zdalna umożliwia efektywniejsze zarządzanie czasem pracownika, a także wpisuje się w koncepcję *work-life balance* (szerzej: Latos-Miłkowska, 2008, s. 8 –12), czyli możliwość łączenia pracy z życiem prywatnym. W systemie pracy zdalnej należy zauważyć zmianę w zakresie cech właściwych stosunkowi pracy, gdzie podstawowe cechy stanowią ciągłość i powtarzalność, natomiast w przypadku pracy zdalnej większy nacisk zostaje położony na wynik czy efekt wykonywanej pracy. Praca zdalna zdecydowanie ułatwia godzenie życia zawodowego z życiem prywatnym, jednak może też prowadzić do sytuacji, w której pracownik pozostaje w dyspozycji pracodawcy przez cały dzień (*work*), natomiast z przerwami (na *life*). W efekcie może dojść do sytuacji, w której nie będzie możliwe zapewnienie odpowiedniego okresu odpoczynku dobowego, ponieważ pracownik wykonywał pracę w określonych odstępach czasu.

Biorąc pod uwagę uprawnienia kierownicze pracodawcy, posiada on również uprawnienie do polecenia pracownikowi pozostawania na dyżurze. Na podstawie art. 151^5 § 1 KP pracodawca może zobowiązać pracownika do pozostawania poza normalnymi godzinami pracy w gotowości do wykonywania pracy wynikającej z umowy o pracę w zakładzie pracy lub w innym miejscu wyznaczonym przez pracodawcę. Dyżur w zakładzie pracy nie powoduje wielu wątpliwości – czas dyżuru nie jest wliczany do czasu pracy, jeżeli pracownik nie wykonywał podczas dyżuru pracy, natomiast za czas takiego dyżuru pracownikowi przysługuje czas wolny od pracy w wymiarze odpowiadającym długości dyżuru, a w razie braku możliwości udzielenia czasu wolnego – wynagrodzenie wynikające z jego osobistego zaszeregowania, określonego stawką godzinową lub miesięczną, a jeżeli taki składnik wynagrodzenia nie został wyodrębniony przy określaniu warunków wynagradzania – 60% wynagrodzenia.

Problematyczną kwestię stanowi natomiast tzw. dyżur domowy, kiedy powyższa zasada nie ma zastosowania i wynika to bezpośrednio z art. 151^5 § 3 KP. Dyżur domowy pracownik pełni zazwyczaj w miejscu swojego zamieszkania i jest w tym czasie pod telefonem. W doktrynie podkreśla się, że w ramach takiego dyżuru pracownik ma dużą swobodę w rozporządzaniu swoim czasem i może go wykorzystywać w zasadzie dowolnie (Świątkowski, 2018). Z powyższym nie sposób się jednak zgodzić, ponieważ pracownik jest zobowiązany do stworzenia warunków, które umożliwią pracodawcy wezwanie go do świadczenia pracy, a tym samym musi być dla pracodawcy dostępny i osiągalny, a najprostszym rozwiązaniem jest posiadanie przy sobie telefonu komórkowego. Co więcej, jeżeli pracodawca wezwie pracownika, jest on zobowiązany do stawienia się w stanie psychofizycznym pozwalającym na wy-

konywanie pracy (Stefański, 2022, komentarz do art. 151(5)). Takie ukształtowanie zasad dotyczących tzw. dyżuru domowego stanowi, zdaniem autorek, poważną ingerencję w swobodę podejmowanych działań i w życie prywatne pracownika. Należy przy tym podkreślić, że w przypadku dyżuru domowego pracownik nie może odmówić używania narzędzi cyfrowych, pozwalających na możliwość komunikowania się na odległość. Zgodnie z poglądem utrwalonym w orzecznictwie dyżur pracownika pod telefonem w gotowości do podjęcia obowiązków pracowniczych (pełniony poza miejscem wykonywania pracy) nie jest czasem pracy, ale nie jest też czasem odpoczynku, o którym mowa w art. 132 § 1 KP i art. 133 § 1 KP (Wyrok Sądu Apelacyjnego w Łodzi, 2016).

Rozwój nowych technologii przyczynił się do powstania pojęcia pracownika „ciągle dostępnego". KP przewiduje środki ochrony, zwłaszcza w zakresie limitowania czasu pracy oraz wprowadzenia odpoczynków dobowych i tygodniowych. Z drugiej jednak strony każdy pracownik jest aktualnie wyposażony w telefon komórkowy, co ułatwia stały kontakt ze współpracownikami i pracodawcą. Biorąc pod uwagę możliwość wykonywania pracy w różnych godzinach, najważniejsze jest ustalenie, czy pracodawca zobowiązuje pracownika do pozostawania w ciągłej gotowości (przykładowo weryfikowania powiadomień w aplikacjach pracodawcy), czy to pracownik sam decyduje o „nieodłączeniu się" od aplikacji pracodawcy również po godzinach pracy, co w większości przypadków jest podyktowane chęcią bycia na bieżąco. Pracodawca będzie zobowiązany do postępowania zgodnie z przepisami prawa pracy, natomiast nie ma rozwiązań prawnych pozwalających wymusić na pracownikach odłączenie się.

Wnioski

Ustawodawstwo i orzecznictwo zarówno polskie, jak i europejskie przewidują szereg rozwiązań pozwalających na limitowanie czasu pracy pracowników. Niewątpliwie nowe technologie przyczyniły się do uelastycznienia prawa pracy, a jednocześnie do zmian w tradycyjnym rozumieniu podporządkowania pracownika pracodawcy w procesie pracy. Najpoważniejszą przyczyną takiego stanu rzeczy jest wszechobecny rozwój technologii, który ma również wpływ na sposób prowadzenia działalności przez pracodawców i wykonywania pracy przez pracowników. Celem jest ograniczenie kosztów działalności, co najczęściej jest możliwe poprzez przeniesienie zasobów do sfery cyfrowej. W tym zakresie niezwykle istotne jest prawo do bycia offline, które za rozumieniem przyjętym przez E. Pachała-Szymczyk „można traktować jako składową prawa do należytych i sprawiedliwych warunków pracy odpowiadającą na wyzwania obecnych czasów" (Pachała-Szymczyk, 2022, s. 23). Podkreślenia wymaga, że prawo do bycia offline co do zasady dotyczy wyłącznie okresu poza świadczeniem pracy, w którym pracownik powinien korzystać z gwarantowanego prawem odpoczynku (Moras-Olaś, 2021, s. 311). W tym sensie prawo do bycia

offline pełni funkcję ochronną i uzupełniającą względem istniejących już regulacji o czasie pracy i odpoczynku.

Aktualnie istniejące rozwiązania nie uniemożliwiają pracownikowi rezygnacji z wykorzystywania narzędzi cyfrowych czy też odmowy ich używania. Takiego stanu rzeczy należy upatrywać w początkowym procesie transformacji cyfrowej – nie jest wykluczone, że za 15 czy 20 lat takie regulacje okażą się niezbędne. Już dziś jednak dostrzegalne są negatywne rezultaty zanikania granicy między czasem pracy a czasem wolnym, związanie z wystąpieniem wypalenia zawodowego, stresu oraz poważnych chorób. Dlatego dyskusja o prawie do bycia offline powinna uwzględniać to, w jaki sposób można usprawnić istniejące już mechanizmy egzekwowania prawa do odpoczynku.

Oczywiście na odrębną refleksję zasługuje zagadnienie, na ile wykorzystanie nowych technologii jest wolą przedsiębiorcy czy też pracodawcy, a na ile przymuszają go do tego obecne realia prowadzenia biznesu. Pojawia się bowiem wątpliwość, czy decyzje o wdrażaniu narzędzi cyfrowych lub zdalnych form komunikacji są związane z potrzebą innowacyjności, czy też tak naprawdę są konieczne, aby utrzymać się na rynku. Niezależnie jednak od tego pracodawcy nie mogą zapominać o pracowniku i jego ochronie przed zagrożeniami wynikającymi z wykorzystania nowych technologii na rynku pracy.

Powiązanie koncepcji *non-use technology* z prawem do bycia offline mogłoby w przyszłości wiązać się z wprowadzeniem regulacji dotyczących m.in. obowiązków informacyjnych pracodawcy np. w zakresie informowania, jakie technologie, w jaki sposób i w jakim zakresie są stosowane w odniesieniu do pracownika. Jednym z rozwiązań mogłoby być również zagwarantowanie pracownikom możliwości wyboru lub odmowy korzystania z wybranych narzędzi cyfrowych. Wydaje się, że byłoby to szczególnie istotne w przypadku aplikacji naruszających prywatność pracownika (np. aplikacji monitorujących efektywność lub geolokalizację). Jednocześnie należy pamiętać, że praktyczna realizacja prawa do bycia offline nie zależy wyłącznie od ustawodawcy. Jak słusznie zauważa się w literaturze przedmiotu, „przepisy prawa, nawet najbardziej szczegółowe, nie pozwolą na w pełni efektywne korzystanie przez zatrudnionych z omawianego uprawnienia, jeżeli równolegle z legislacją nie będzie kształtowana odpowiednia kultura pracy, bez przyzwolenia na ciągłą dostępność pracowników" (Pachała-Szymczyk, 2022, s. 24). Tylko wówczas można mówić o realnym prawie do bycia offline czy też możliwości podjęcia decyzji w ramach koncepcji *non-use of technology*.

BIBLIOGRAFIA

Baumer, E. P. S., Ames, M. G., Burrell, J., Brubaker, J. R., Dourish, P. (2014). Refusing, limiting, departing: Why we should study technology non-use. CHI '14 Extended Abstracts on Human Factors in Computing Systems, 65–68. ACM. https://doi.org/10.1145/2559206.2559224

Beksiak, J. (2014). *Ekonomia. Kurs podstawowy*. C.H. Beck.

Büchi, M., Festic, N., & Latzer, M. (2019). Digital overuse and subjective well-being in a digitized society. Social Media Society, *5*(4), 1–12. https://doi.org/10.1177/2056305119886031

Boruta, I. (2020). O przyszłości pracy. *Praca i Zabezpieczenie Społeczne*, *1*, 3–12.

Chesalina, O. (2021). The legal nature and the place of the right to disconnect in European and in Russian labour law. *Russian Law Journal*, *9*(3), 37–63.

Dyrektywa Parlamentu Europejskiego i Rady 2003/88/WE z dnia 4 listopada 2003 r. dotycząca niektórych aspektów organizacji czasu pracy, Dz. U. L 299, 18.11.2003, 9–19.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1152 z dnia 20 czerwca 2019 r. w sprawie przejrzystych i przewidywalnych warunków pracy w Unii Europejskiej, Dz.U. L 186, 11.07.2019, 105–121.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1158 z dnia 20 czerwca 2019 r. w sprawie równowagi między życiem zawodowym a prywatnym rodziców i opiekunów, uchylająca dyrektywę Rady 2010/18/UE, Dz.U. L 188, 12.07.2019, 79–93.

Eurofound. (2020a). Right to disconnect in the 27 EU Member States. In: Telework and ICT-based mobile work: Flexible working in the digital age (Working Paper, Industrial Relations series). Luxembourg: Publications Office of the European Union. https://www.eurofound.europa.eu/en/publications/all/right-disconnect-27-eu-member-states#authors

Pisarczyk, Ł. (2017). w: Florek, L. (red.). *Kodeks pracy. Komentarz*. Wolters Kluwer. LEX.

Karta Praw Podstawowych Unii Europejskiej, Dz. U. C 202, 07.06.2016, 389–405.

Kotlorz, D. (2011). Współczesny rynek pracy – wybrane problemy. w: D. Kotlorz (red.), *Współczesny rynek pracy. Wybrane problemy* (ss. 9–35). Wydawnictwo Uniwersytetu Ekonomicznego w Katowicach.

Kryńska, E., & Kwiatkowski, E. (2013). *Podstawy wiedzy o rynku pracy*. Wydawnictwo Uniwersytetu Łódzkiego.

Krysiak, K. (2024). O prawnym pojęciu pracy zdalnej. *Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury*, *3*(55), 75–91.

Kurzynoga, M. (2022). Propozycje Parlamentu Europejskiego unormowania prawa pracowników „do odłączenia" (*the right to disconnect*). *Praca i Zabezpieczenie Społeczne*, *LXIII*(5), 3–13.

Latos-Miłkowska, M. (2008). Godzenie pracy zawodowej z życiem rodzinnym w przepisach o czasie pracy (*work-life balance*). *Praca i Zabezpieczenie Społeczne*, *7*, 14–21.

Moras-Olaś, K. (2021). Prawo do bycia offline jako podstawowe prawo pracownika. *Studia z Zakresu Prawa Pracy i Polityki Społecznej*, *28*(4), 305–323. https://doi.org/10.4467/25444654SPP.21.024.14266

Naumowicz, K. (2021). Prawo pracowników zdalnych do bycia offline – rozważania prawnoporównawcze. *Roczniki Administracji i Prawa*, *XXI*(z. specjalny), 535–544. https://doi.org/10.5604/01.3001.0015.6195

Nowak, M. (2019). Wypalenie zawodowe a prawo do odpoczynku – wybrane zagadnienia. *Monitor Prawa Pracy*, *1*, 15–20. https://doi.org/10.1093/joc/jqad021

Nguyen, M. H., & Hargittai, E. (2023). Digital inequality in disconnection practices: Voluntary nonuse during COVID-19. *Journal of Communication*, *73*(5), 494–510.

Pachała-Szymczyk, E. (2022). Prawo do bycia offline odpowiedzią na upowszechnienie narzędzi cyfrowych w zatrudnieniu. *Transformacje Prawa Prywatnego*, *4*, 5–23.

Piwowarska, K. (2018). Czy nowe technologie zrewolucjonizują rynek pracy? *Studia Prawnicze. Rozprawy i Materiały*, *2*, 135–155.

Postanowienie Sądu Najwyższego z dnia 28 marca 2019 r., sygn. I PK 89/18.

Rezolucja Parlamentu Europejskiego z dnia 21 stycznia 2021 r. zawierająca zalecenia dla Komisji w sprawie prawa do bycia offline (2019/2181(INL)), Dz. U. C 456, 10.11.2021, 161–176.

Sakowska, K. (2025a). Prawo do bycia offline z perspektywy obowiązków pracodawcy. *Studia Prawnoustrojowe*, *67*, 341–352.

Sakowska, K. (2025b). Elastyczne formy zatrudnienia w erze cyfrowej – zarys problematyki. *Palestra*, *1*, 116–5.

Satchell, C., & Dourish, P. (2009). Beyond the user: Use and non-use in HCI. Proceedings of the 21st Annual Conference of the Australian Computer-Human Interaction Special Interest Group (OZCHI '09), 9–16. https://doi.org/10.1145/1738826.1738829

Skowron, R. T. (2019). Cybertariat – prawo pracy a nowe formy zatrudnienia w ramach ekonomii współpracy. *Przegląd Prawno-Ekonomiczny*, *49*(4), 152–173. https://doi.org/10.31743/ppe.9948

Sobczyk, A. (2005). *Zasady prawnej regulacji czasu pracy*. Dom Wydawniczy ABC.

Sobczyk, A. (red.). (2023). *Kodeks pracy. Komentarz*. Legalis.

Spytek-Bandurska, G. (2024). Komentarz do art. 67(18). w: W. Muszalski & K. Walczak (red.), *Kodeks pracy. Komentarz* Legalis.

Stefański, K. (2022). Komentarz do art. 94–304(5). w: K. W. Baran (red.), *Kodeks pracy. Komentarz*. Tom II (ss. 501–560). WKP LEX.

Świątkowski, A. M. (2018). Dyżur pracowniczy. Zagadnienia prawne dotyczące relacji pojęć „czas pracy" i „okres wypoczynku" w świetle orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej. *Przegląd Sądowy*, *11*, 45–61.

Sejm Rzeczypospolitej Polskiej. (1974). Ustawa z dnia 26 czerwca 1974 r. – Kodeks pracy (t.j. Dz.U. z 2023 r., poz. 1465).

Todolí-Signes, A., & Tyc, A. (2016). The need for a platform-specific employment contract in the Uber economy. *Gdańsko-Łódzkie Roczniki Prawa Pracy i Prawa Socjalnego*, *6*, 197–210.

Wyrok Sądu Apelacyjnego w Łodzi z dnia 18 kwietnia 2016 r., sygn. III APa 3/16.

Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 14 maja 2019 r., Federación de Servicios de Comisiones Obreras (CCOO) przeciwko Deutsche Bank SAE, C-55/18.

Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 2 marca 2023 r., IH przeciwko MÁV-START Vasúti Személyszállító Zrt., C-477/21.

Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 21 lutego 2018 r., Ville de Nivelles przeciwko Rudy Matzak, C-518/15.

Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 23 grudnia 2024 r., Loredas, C-531/23.

Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 3 października 2000 r., Simap, C-303/98.

Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 9 marca 2021 r., D.J. przeciwko Radiotelevizija Slovenija, C-344/19.

Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 17 marca 2021 r., Academia de Studii Economice din Bucureşti przeciwko Doru Viorel Bălăn, C-585/19.

Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 9 września 2003 r., Jaeger, C-151/02.

Vorderer, P., Krömer, N., & Schneider, F. M. (2016). Permanently online – Permanently connected: Explorations into university students' use of social media and mobile smart devices. *Computers in Human Behavior*, *63*, 694–703. https://doi.org/10.1016/j.chb.2016.05.085

Zapolska, K., & Nyka, M. (2024). The impact of DAC7 Directive on functioning of platforms and platform operators from the perspective of legal model of their collaboration with individuals. *Białostockie Studia Prawnicze, 29*(2), 177–193.

Bialystok Legal Studies
Białostockie Studia Prawnicze
2025 vol. 30 no. 4

sciendo

DOI: 10.15290/bsp.2025.30.04.06

Received: 22.02.2025
Accepted: 10.09.2025

Edyta Bielak-Jomaa
Uniwersytet Łódzki, Polska
ejomaa@wpia.uni.lodz.pl
ORCID ID: 0000–0002–9217–7959

(Nie)dopuszczalność stosowania neurotechnologii w miejscu pracy

The (In)Admissibility of the Use of Neurotechnology in the Workplace

Abstract: Neurotechnology, together with the rapid development of artificial intelligence, opens up a world of almost infinite possibilities. It is also finding applications in the work environment. Despite the undoubtedly positive effects of the use of neural tools in the workplace (the possibility of improving work efficiency, enhancing the health and safety system, or risk management), they bring obvious threats to the dignity, privacy, psychological privacy, and other personal assets of the worker. There is no doubt that technological progress will redefine human life, may significantly affect social relations as we have known them so far, and will give rise to unprecedented consequences for human rights. It is therefore legitimate to ask whether the existing legal regulations are a sufficient response to these challenges, or whether it is nevertheless necessary to amend the regulations or enact a new law.

Keywords: neuroscience, employment law, neurotechnology, employee rights, privacy, neurodata
Słowa kluczowe: neuronauka, prawo pracy, neurotechnologia, prawa pracownika, ochrona prywatności, neurodane

Wprowadzenie

Rozwój technologii przybrał niespotykane dotąd tempo i wyraźnie zwiększył swój zasięg. Telefony komórkowe, laptopy, tablety, smartfony stały się powszechnie używanymi narzędziami komunikacji i pracy. Wykorzystywanie smartwatchy, elektroniki noszonej na ciele (*wearable technology*) i aplikacji mierzących rytm serca, puls czy liczbę spalanych kalorii zaczynają być stosowane masowo. Pojawiają się wciąż nowe technologie i systemy sztucznej inteligencji pomagające ratować życie i zdrowie, ułatwiające pracę, wprowadzające nowe modele komunikowania się wewnątrz

i na zewnątrz organizacji, wspierające naukę. Technologia staje się coraz bardziej zaawansowana. Algorytmy sztucznej inteligencji, *blockchain*, Internet Rzeczy (IoT), biochipy, rzeczywistość wirtualna i rozszerzona (VR/AR) oraz neurotechnologia mogą w najbliższym czasie przyczynić się do wprowadzenia przełomowych zmian rzeczywistości, również w zakresie prawa pracy, które „wchłania" w naturalny sposób technologie służące zwiększeniu efektywności i produktywności, umożliwiając obniżenie kosztów i wzmacniając potencjał rynkowy pracodawcy.

Celem prezentowanego artykułu jest wskazanie obszarów prawa pracy, w których neurotechnologia mogłaby znaleźć zastosowanie, określenie zagrożeń dla pracownika w związku z jej stosowaniem oraz próba odpowiedzi na pytanie, czy istniejące regulacje prawne pozwalają na jej stosowanie i jakie przewidują ograniczenia z punktu widzenia ochrony pracowników i ich praw w miejscu pracy.

1. Wykorzystanie neurotechnologii w środowisku pracy

Neurotechnologia jest definiowana jako wszelkie narzędzia, które pozwalają na monitorowanie lub modyfikowanie funkcji mózgu (Eaton & Illes, 2007, s. 393–397) i są wykorzystywane do uzyskiwania dostępu, badania, oceny, manipulowania oraz zmiany struktury i funkcji układu nerwowego (OECD, 2019).

Metodami neurtechnologii i neurobiologii są: tomografia komputerowa (*computed tomography*, CT), pozytronowa tomografia komputerowa (*positron emission tomography*, PET), obrazowanie strukturalnym rezonansem magnetyczny (*magnetic resonance imaging,* MRI) lub funkcjonalnym rezonansem magnetycznym (*functional magnetic resonace imaging*, fMRI), pozwalające tworzyć wielowymiarowy obraz mózgu. Powszechne zastosowania neurotechnologii obejmują także interfejsy mózg–komputer (*Brain-Computer Interface*, BCI), służące do sterowania urządzeniami lub neuromonitorowania w czasie rzeczywistym, systemy oparte na neuroczujnikach, narzędzia do treningu poznawczego, do noszenia dla dobrego samopoczucia psychicznego i systemy rzeczywistości wirtualnej (Ienca & Andorno, 2017, s. 4).

Szybki rozwój neurotechnologii generuje szereg pytań o możliwości korzystania z dorobku tej nauki w prawie pracy. Może ona znaleźć zastosowanie w obszarze rekrutacji, do oceny pracowników i monitorowania ich pracy czy podniesienia poziomu bezpieczeństwa w zakładzie pracy. Pracodawcy mogą być zainteresowani używaniem fMRI do sondowania umysłów kandydatów do pracy i pracowników, np. w celu pomiaru ich uczciwości, gustów i nawyków, co umożliwiałoby im wybór najbardziej odpowiedniego kandydata z punktu widzenia jego przydatności i zdolności adaptacji w organizacji (Jalan & Punj, 2025, s. 215–216). Neurotechnologia może pomóc w ocenie zdolności osoby do generowania pewnego stanu psychicznego (Ienca & Andorno, 2017, s. 5) i zostać wykorzystana do oceny prawdopodobieństwa, że dana osoba np. popełniła lub popełni przestępstwo seksualne. Badania z wykorzy-

staniem neurotechnologii mogą ujawnić świadome lub nieświadome uprzedzenia rasowe, orientację seksualną i preferencje seksualne (Tovino, 2007, s. 48–49).

Badania łączące pomiary biometryczne i psychologię mogą być wykorzystywane jako nowe narzędzia, których celem jest monitorowanie uwagi pracowników w pracy, po to, aby zwiększyć ich wydajność i produktywność (Appel, 2008, s. 616; ICO, 2023, s. 14), identyfikować stany neuropoznawcze, takie jak błądzenie myśli (Dehais i in., 2020, s. 2; Sela i in., 2020). Nowe urządzenia mogą nie tylko monitorować koncentrację, lecz także zwiększać jej poziom za pomocą stymulacji prądem stałym – tDCS (Karthikeyan i in., 2021). Technologia może więc pomóc pracownikom w walce ze zmęczeniem czy ułatwić kontrolowanie presji i zarządzania nią (Surdykowska, 2025, s. 318). Może mieć to ogromne znaczenie dla pracowników, którzy są zobowiązani do zapewnienia bezpieczeństwa innym ludziom: strażaków, medyków pracujących w pogotowiu ratunkowym, osób wykonujących prace wysokiego ryzyka, np. maszynistów pociągów dużych prędkości, czy podejmujących się szczególnie niebezpiecznych prac wymagające dużego i ciągłego skupienia uwagi (Cofas, 2022 Muhl & Andorno, 2023, s. 3–4).

Technologie w miejscu pracy mogą być wykorzystywane do wykrywania niewygodnych pozycji podczas pracy, wysiłku fizycznego, wibracji, związku powtarzalności zadań ze zmęczeniem fizycznym, mierzenia ostrości umysłu, oceny zgodności zachowań pracowników z przepisami bezpieczeństwa i wpływu przerw na odpoczynek (ICO, 2023, s. 14; Patel i in., 2022, s. 1; Wilson, 2013). Elektroniczne czujniki i algorytmy sztucznej inteligencji do monitorowania fal mózgowych i wykrywania skoków emocji, takich jak lęk i depresja, montowane w czapkach, noszone w postaci opasek czy słuchawek mogłyby ułatwić pracodawcom tworzenie i dostosowanie harmonogramów zmian i przerw w pracy w celu zwiększenia poprawy warunków życia załogi (Appel, 2008, s. 616; Muhl & Andorno, 2023, s. 2).

Dzięki identyfikowaniu reakcji poznawczych narzędzia i badania neurologiczne mogą dostarczyć dowodów na „niewidoczne" obrażenia, narażenie na działanie toksyn oraz ból i cierpienie emocjonalne (Rosenthal, 2019, s. 307). Zdolność technologii do ujawniania reakcji bólowej w mózgu może pomóc w zrozumieniu, diagnozowaniu i weryfikacji chorób i urazów, które wpływają na strukturę i funkcjonowanie mózgu i przekładają się na schorzenia fizyczne (Fox & Stein, 2015, s. 975). Choroby neurodegeneracyjne oraz ból i cierpienie, wywołane warunkami pracy, stresem i przemocą w miejscu pracy, dzięki obrazowaniu mózgu mogłyby być uznane za przyczynę utraty zdrowia pracownika (Appel, 2008, s. 618; Eisenberger, 2021 s. 45–47; Rosenthal, 2019 s. 295). Neurotechnologia może przyczynić się do zanikania granic państwowych dla świata pracy dzięki temu, że będzie możliwe połączenie mózgu człowieka z sieciami przekazywania danych (Adamczyk & Surdykowska, 2021, s. 8). Zastosowanie neuronarzędzi oraz technologii neurobiologii daje prawie nieograniczone możliwości obrazowania, analizy i kontroli mózgu. Osiągnięcia neuronauk mogą przysłużyć się poprawie warunków pracy. Wiedza pracodawców o tym, jak reaguje organizm pra-

cownika na określone działania podejmowane wobec niego, okoliczności i warunki pracy, sposób zarządzania, kultura kontroli mogą ułatwiać dostosowanie organizacji do oczekiwań pracowników i zwiększyć wpływ załogi na funkcjonowanie zakładu pracy. Neurotechnologia budzi jednocześnie wyjątkowe obawy etyczne, ponieważ w przeciwieństwie do innych technologii bezpośrednio oddziałuje na mózg, emocje, uczucia i myśli człowieka (Yuste i in., 2021). Jej inwazyjność wymaga istnienia takich rozwiązań prawnych, które pozwolą człowiekowi z jednej strony w bezpieczny sposób korzystać z dobrodziejstw technologii, a z drugiej chronić przed nieuprawnioną ingerencją w tożsamość psychiczną.

2. Zagrożenia dla pracowników wynikające z neurotechnologii

Pomimo stałego rozwoju i ulepszania technik obrazowania mózgu, co pozwala na uznanie ich za wysoce użyteczne, ich wykorzystywanie wywołuje wiele kontrowersji (Krupa, 2020, s. 89). Mózg nie jest bowiem po prostu kolejnym organem, ale tym, który generuje całą aktywność umysłową i poznawczą i po raz pierwszy w historii, dzięki neurotechnologii, istnieje realna możliwość dekodowania ludzkich myśli lub manipulowania nimi za pomocą technologii (Yuste i in., 2021).

W literaturze wskazuje się, że neurotechnologia ma potencjał dostępu nie tylko do świadomych procesów mózgowych, lecz także do przetwarzania podświadomego, nad którym człowiek ma ograniczoną kontrolę lub wręcz nie ma żadnej (Bonaci i in., 2015, s. 35; Muhl & Andorno, 2023, s. 4). Dzięki zastosowaniu neurourządzeń pracodawcy mogliby, przynajmniej w pewnym stopniu, stać się świadomi uczuć, emocji i obciążenia psychicznego pracowników. Neurotechnologia umożliwia również podejmowanie ważnych decyzji na podstawie przewidywania lub subiektywnych opinii, które mogą nie być wiarygodne lub dokładne. W szczególności posiadanie takich informacji mogłoby skłonić pracodawców do wykorzystania danych np. do porównywania i oceny wyników pracy czy podejmowania decyzji o możliwych premiach i awansach (Goodenough & Tucker, 2010, s. 89–90).

Stosowanie technologii, w tym neurotechnologii w miejscu pracy może negatywnie wpłynąć na poczucie wartości pracowników. Dehumanizacja i uprzedmiotowienie tworzą toksyczne warunki, które zmniejszają zaangażowanie w pracę i życie organizacji (Arico i in., 2020, s. 2; Bastian & Haslam, 2011), powodują emocjonalne odrętwienie, zmniejszenie motywacji i satysfakcji z pracy (Twenge i in., 2003, s. 420–422). Świadomość, że aktywność mózgu jest monitorowana lub analizowana, może wywoływać u pracowników presję na dokonywanie autocenzury lub modyfikowanie zachowań, aby dostosować je do określonych oczekiwań lub standardów uznawanych przez pracodawcę za jedynie prawidłowe (Wilson, 2013; Muhl & Andorno, 2023, s. 4). Monitoring w miejscu pracy i kontrola prowadzona zwłaszcza przy zastosowaniu neuronarzędzi może naruszać godność pracownika i jest kontrprodukt-

tywna, ponieważ pracownicy bardziej skupieni są na tym, jak ominąć system, niż jak prawidłowo i efektywnie wykonywać swoje zadania (Holman i in., 2022, s. 61; Siegel i in., 2022, s. 2–3).

Pojawiające się technologie, szczególnie te oparte na sztucznej inteligencji, stawiają nowe wyzwania dla ochrony przed dyskryminacją (Kolber, 2014 s. 835–841). Wykorzystanie sztucznej inteligencji może prowadzić do dyskryminacyjnych wyników, nawet jeśli algorytmy są zaprojektowane z myślą o szanowaniu różnorodności i integracji (Drage & Mackereth, 2022, s. 9–12). Pracodawcy mogą analizować statystyki dotyczące poziomu zmęczenia i koncentracji konkretnych pracowników i nagradzać tych, którzy są mniej skłonni do robienia przerw w ciągu dnia pracy i potrafią utrzymać wyższy poziom koncentracji. Taka „neurodyskryminacja" (Ienca i in., 2022, s. 2) może skutkować zmniejszeniem szans osób o niższych zdolnościach poznawczych i mniejszej stabilności emocjonalnej (Ienca & Ignatiadis, 2020, s. 79–82; Müller i in. 2021, s. 594–597).

Poza wszystkim należy zaznaczyć, że neurotechnologia nie jest nieomylna. Skany mózgu często nie potwierdzają związku przyczynowo – skutkowego między np. stanem zdrowia pracownika a warunkami pracy, a jedynie wskazują korelacje, przez co stają się nieprzydatne do udowodnienia przyczyny oraz wpływu warunków pracy na stan zdrowia pracownika (Goodenough & Tucker, 2010, s. 89–91). Istotnym problemem w wykorzystaniu dowodów z neuroobrazowania jest bowiem ustalenie wyjściowego stanu funkcji mózgu. Trudno ocenić, czy konkretny incydent faktycznie spowodował u człowieka określoną szkodę czy krzywdę psychiczną (Appel, 2008, s. 617).

3. Neurodane jako dane osobowe

Środowisko pracy stale się zmienia, ale najcenniejszymi aktywami organizacji nadal pozostają informacje i dane, w tym dane osobowe (Wood, 2021). Neurotechnologiczna przyszłość będzie wymagała zagwarantowania ochrony nie tylko informacji, które rejestrujemy i udostępniamy, lecz także źródła tych informacji, ponieważ w przypadku neurodanych mogą być one nierozłączne (Palaniappan & Mandic, 2007, s. 249).

Pojawia się zatem pytanie, czy tradycyjne prawo do prywatności obejmuje dane zawarte w ludzkich umysłach i przez nie generowane. Dylemat ten jest poważny nie tylko dlatego, że w żadnym akcie prawnym nie zawarto legalnej definicji prywatności, zaś w literaturze brak zgody co do treści tego pojęcia, lecz także ze względu na szczególny charakter danych mózgowych. Obejmują one dwie kategorie danych. *Brain data* powstają na etapie zbierania impulsów mózgowych przez elektrody i dotyczą pomiaru struktury, aktywności i funkcji ludzkiego mózgu. Dane te wymagają przetworzenia (odkodowania przez AI) w celu dostarczenia wartościowych informacji. Informacje odkodowane przez AI to tzw. *mental information*. Mogą one za-

wierać informacje objęte katalogiem danych szczególnej kategorii – dotyczących zdrowia (Słocka, 2021, s. 82). Każdy pomiar aktywności mózgu może być traktowany jako informacja o stanie zdrowia osoby poddanej badaniu, ponieważ urządzenia lub usługi związane z neurotechnologią są w stanie wnioskować o zdrowiu fizycznym lub sprawności fizycznej osób i ich stanie psychicznym, np. umiejętności rozwiązywania problemów, szybkości podejmowania decyzji, wyszukiwaniu w pamięci, percepcji, emocjach (EDPS, 2024, s. 15).

Skany mózgu mogą być porównywalne z unikalnymi odciskami palców. Zapewniają odrębny obraz mózgu danej osoby, a zatem można je uznać za dane biometryczne, jeżeli służą jednoznacznej identyfikacji osoby fizycznej (Palaniappan & Mandic, 2007, s. 243–244; Finn i in., 2015, s. 1668–1669; Article 29 Data Protection Working Party, 2003, s. 3). Biometria mózgu wprowadza dodatkowe elementy inwazyjności. Wynika to z możliwości wnioskowania informacji związanych z doświadczeniami osób, których dane dotyczą, bez ich wyraźnego przekazywania lub z możliwości profilowania osób, których dane dotyczą, na podstawie wzorców fal mózgowych.

Bez względu na to, czy badania mózgu polegają tylko na jego pomiarze, czy będą one polegały na gromadzeniu danych dodatkowo odkodowywanych i interpretowanych celem uzyskania dalszych informacji, otrzymujemy informację o prawidłowej neuroaktywności mózgu, czyli o odpowiedniej chemii mózgu czy funkcjonowaniu neuroprzekaźników (Głuchowska, 2024). Jest to zatem najbardziej inwazyjne przetwarzanie, naruszające prywatność psychiczną i potencjalnie integralność psychiczną danej osoby.

Już zatem na etapie samego badania, neurodane stanowią dane osobowe szczególnej kategorii w rozumieniu RODO i jako takie podlegają ochronie zagwarantowanej przez art. 9 ust. 1 RODO. Co do zasady takie dane nie mogą być przetwarzane. Wyjątki dopuszczające przetwarzanie danych szczególnie chronionych wskazane są w ust. 2 art. 9 i w nim można poszukiwać potencjalnych podstaw przetwarzania danych neuronowych.

4. Polskie regulacje prawne a stosowanie neurotechnologii

Narzędzia neurotechnologiczne ściśle powiązane są z systemami cyfrowymi, szczególnie systemami sztucznej inteligencji. Korzystanie z rozwiązań sztucznej inteligencji jest wyzwaniem dla współczesnego prawa pracy, wymaga bowiem nowego spojrzenia na warunki w miejscu pracy, obowiązki i odpowiedzialność stron stosunku pracy. Kontrowersyjna jest już kontrola pracowników przy wykorzystaniu mechanizmów sztucznej inteligencji (Latos-Miłkowska, Kibil, 2024, s. 157). Tym bardziej niebezpieczne w stosunkach pracy jest wykorzystywanie danych mózgowych i ich analiza przez systemy AI.

Polski ustawodawca nie uregulował w żaden sposób dopuszczalności i zasad korzystania z neurotechnologii w prawie pracy, ale także nie zakazał wprost stosowania tej technologii. Nie oznacza to, rzecz jasna, że użytkowanie cyfrowych technologii monitorujących ludzki mózg i przetwarzających dane z niego nie podlega ograniczeniom. Ramy regulacyjne określające stosowanie nowych technologii w środowisku pracy aktualnie w dużej mierze opierają się na systemie standardów i zasad wypracowanych przez przepisy o ochronie danych osobowych, głównie RODO (Parlament Europejski i Rada UE, 2016). Oceny dopuszczalności korzystania z narzędzi neurotechnologii i neurobiologii w środowisku pracy należy jednak poszukiwać i analizować ich przydatność także w przepisach AI Aktu (Parlament Europejski i Rada UE, 2024).

Przetwarzanie szczególnych kategorii danych osobowych – dotyczących zdrowia, biometrycznych, genetycznych oraz innych , ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz seksualność lub orientację seksualną osoby fizycznej – musi opierać się na jednej z przesłanek wskazanych w art. 9 ust. 2 RODO. Znajduje to podstawę w wielu przepisach prawa pracy, dotyczących m.in. przetwarzania danych osobowych kandydatów do pracy, profilaktycznych badań lekarskich czy obowiązków pracodawcy z zakresu bhp.

Wydaje się, jednak że na podstawie obecnie obowiązujących przepisów prawa pracy w stosunku do danych neuronowych teoretycznie można rozpatrywać wyłącznie trzy przesłanki ich przetwarzania: zgodę (art. 9 ust. 2 lit. a), niezbędność przetwarzania do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego (art. 9 ust. 2 lit. h RODO) oraz niezbędność do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej (art. 9 ust. 2 lit. b RODO).

Jeżeli przesłanką przetwarzania danych należących do szczególnej kategorii miałaby być zgoda osoby fizycznej, to zgodnie z art. 9 ust. 2 lit a RODO zgoda musi być wyraźna i spełniać warunki wskazane w art. 4 pkt 11 RODO. Zgoda oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych. Zgoda musi precyzyjnie określać zakres i cel przetwarzania danych. W stosunkach pracy obwarowane jest to dodatkowym wymogiem wynikającym z art. 22^{1b} § 1 i 2 kodeksu pracy. W świetle tego przepisu pracodawca może przetwarzać dane na podstawie zgody wyłącznie w przypadku, gdy ich przekazanie następuje z inicjatywy pracownika. Pracodawca nie może więc korzystać z neurodanych, bo oznaczałoby to, że zgoda pracownika ma charakter następczy wobec przetwarzania. Ponieważ sygnały mózgowe i aktywność neuronowa mózgu pozwalają określić tożsamość osoby i mogą być z nią powiązane, trudno byłoby także

uznać, że zgoda na zbieranie i wykorzystywanie danych neuronowych miałaby charakter konkretny i świadomy, gdyż pracownik nie wiedziałby, na gromadzenie jakich konkretnie danych wyraził zgodę (Ienca & Andorno, 2017).

Artykuł. 9 ust. 2 lit. h RODO wskazuje na legalność przetwarzania danych m.in. w razie oceny zdolności pracownika do pracy. W art. 229 § 1^3 k.p. ustawodawca określił, że celem pozyskiwania danych o stanie zdrowia pracownika jest ustalenie zdolności zdrowotnej do wykonywania określonej pracy. Zgodnie z tą normą pracodawca żąda od kandydata do pracy albo pracownika aktualnego orzeczenia lekarskiego stwierdzającego brak przeciwwskazań do pracy na danym stanowisku. Nie ma on prawa gromadzić i przetwarzać innych danych dotyczących zdrowia. Oznacza to, że nie może przetwarzać danych neuronowych w celu określenia stanu zdrowia pracownika albo wnioskowania o nim w kontekście jego zdolności do pracy.

Przesłanka, którą warto zbadać, jest również niezbędność do wypełniania obowiązków i wykonywania szczególnych praw przez administratora danych osobowych (pracodawcę) w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jednak jest to dozwolone prawem unijnym lub krajowym bądź porozumieniami zbiorowymi, jeżeli wprowadzają one odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą (art. 9 ust. 2 pkt b RODO). Obowiązek lub prawo, o jakich mowa, muszą zostać wyartykułowane przez ustawodawcę wprost w przepisie ustawy, np. niezbędność przetwarzania wynikająca z obowiązku zapewnienia bezpiecznych i higienicznych warunków pracy w miejscu jej wykonywania (art. 207§1k.p.). Z obowiązkiem ochrony zdrowia pracowników immanentnie związane jest prawo pracodawcy do pozyskiwania informacji o ich stanie zdrowia. Niewątpliwie zapewnieniu bezpiecznych warunków pracy mogą służyć neuronarzędzia wykorzystywane do wykrywania niewygodnych pozycji podczas pracy, wysiłku fizycznego, stresu, lęku, depresji czy innych emocji. Przepisy dotyczące obowiązków pracodawcy w dziedzinie bhp mają jednak charakter zbyt ogólny, żeby można było uznać je za wystarczające do stosowania przez pracodawcę technologii opartej na analizie neurodanych, zwłaszcza w kontekście zasad przetwarzania danych określonych w RODO.

Kwestie związane z bezpieczeństwem pracowników w miejscu pracy regulowane są także w przepisach AI Aktu. W art. 5 ust. 1 lit. f wprowadza on zakaz stosowania systemów sztucznej inteligencji dla algorytmicznego wyciągania wniosków na temat emocji osoby fizycznej w miejscu pracy. Rozpoznawanie czy identyfikacja emocji ma miejsce, gdy przetwarzanie danych biometrycznych osoby fizycznej pozwala na bezpośrednie porównanie i zidentyfikowanie z emocją, która została wcześniej zaprogramowana w systemie rozpoznawania emocji. Wnioskowanie natomiast odbywa się poprzez dedukowanie informacji generowanych przez procesy analityczne i inne procesy dokonywane przez sam system. W takim przypadku informacje na temat emocji nie opierają się wyłącznie na danych zebranych na temat osoby fizycznej,

ale są wnioskowane na podstawie innych danych dotyczących tej osoby (European Commission, 2025, s. 82).

AI Akt zasadniczo zakazuje stosowanie systemów AI dla algorytmicznego wyciągania wniosków na temat emocji osoby fizycznej w miejscu pracy. Jednocześnie wprowadza wyjątek w tym zakresie: przepisy dopuszczają bowiem możliwość wprowadzania do obrotu i wykorzystywania systemów w miejscu pracy ze względów medycznych lub bezpieczeństwa. Jednak w celu zapewnienia wysokiego poziomu ochrony praw podstawowych wyjątek ten należy jednak interpretować wąsko. Pojęcie względów bezpieczeństwa w ramach tego wyjątku należy rozumieć jako mające zastosowanie wyłącznie w odniesieniu do ochrony życia i zdrowia, a nie do ochrony innych interesów, na przykład mienia przed kradzieżą lub oszustwem. Wynika z tego, że każde użycie systemów do wykrywania emocji pracowników ze względów bezpieczeństwa powinno zawsze być ograniczone do tego, co jest absolutnie konieczne i proporcjonalne, z uwzględnieniem ograniczeń czasowych, kontekstu i skali przetwarzania informacji oraz bezpieczeństwa danych. Konieczność powinna być obiektywie oceniana w odniesieniu do celu (bezpieczeństwa pracowników), a nie odnosić się do potrzeb pracodawcy. Ocena proporcjonalności powinna dotyczyć analizy tego, czy nie istnieją mniej inwazyjne środki alternatywne, które zapewniałyby bezpieczeństwo pracownikom w miejscu pracy (European Commission, 2025, s. 87–88).

Trzeba także zauważyć, że zgodnie z motywem 18 AI Aktu system rozpoznawania emocji nie obejmuje stanów fizycznych, takich jak ból lub zmęczenie, co oznacza, że szereg systemów sztucznej inteligencji może być wykorzystywanych ze względów bezpieczeństwa pracowników, w tym na przykład systemy wykorzystywane do wykrywania stanu zmęczenia zawodowych pilotów lub kierowców.

AI Akt, dopuszczając stosowanie systemów sztucznej inteligencji przez badających emocje, może otworzyć drogę dla neurotechnologii w prawie pracy, jeżeli może być ona przydatna do podniesienia bezpieczeństwa życia i zdrowia pracowników w miejscu pracy.

5. Uwagi *de lege ferenda*

Artykuł 2 ust. 11 AI Aktu stanowi, że Unia lub państwa członkowskie mogą wprowadzać przepisy ustawowe, wykonawcze lub administracyjne, które są korzystniejsze dla pracowników w zakresie ochrony ich praw w odniesieniu do stosowania systemów AI przez pracodawców niż AI Akt. Powinny także określić zasady korzystania z systemów sztucznej inteligencji.

Ustawodawca krajowy może zatem w ogólne zakazać stosowania systemów sztucznej inteligencji do rozpoznawania emocji pracowników lub reglamentować zasady jej stosowania. Poprzedzone to powinno zostać rzetelną analizą obowiązujących przepisów bhp oraz praktyk w kontekście ich efektywności. Konsultacje ze środowi-

skiem pracy – pracodawcami i przedstawicielami pracowników oraz reprezentantami świata akademickiego, ekspertami od systemów sztucznej inteligencji oraz osobami zajmującymi się neuronaukami, zwłaszcza neurotechnologią i neurobiologią, pozwoli na miarodajne określenie ewentualnych potrzeb i oczekiwań stron stosunku pracy, wskaże możliwości technologiczne i prawne oraz etyczne granice ewentualnego korzystania z tej technologii w środowisku pracy.

Jeżeli ustawodawca zdecyduje się jednak dopuścić stosowanie systemów AI służących rozpoznawaniu emocji w miejscu pracy, powinien określić szczegółowe warunki korzystania z technologii informatycznych przetwarzających neurodane. Po pierwsze, konieczne byłoby wskazanie podstawy gromadzenia i przetwarzania tego typu danych. Ze względu na szczególny charakter danych i sposoby ich przetwarzania należałoby rozstrzygnąć, czy określenie zasad i reguł korzystania z systemów AI nie powinno zostać uregulowane w odrębnej ustawie. Po drugie, przepisy powinny wskazywać wyraźny, konkretny cel przetwarzania („bezpieczeństwo" czy „względy medyczne" są pojęciami zbyt szerokimi), należałoby także dokładnie określić, w jakich okolicznościach pracodawca mógłby korzystać z systemów (np. w odniesieniu do konkretnych zawodów, stanowisk czy rodzajów pracy). Bezwzględnie przepisy powinny również wskazywać cechy systemu sztucznej inteligencji, żeby mógł być dopuszczony do użytku. Wreszcie, niezbędne byłoby wskazanie zasad wdrażania takiego systemu, określenia roli przedstawicieli pracowników w ustalaniu jego założeń i działania, przejrzystości korzystania, określenie praw pracowników do odmowy bycia obiektem neurotechnologii oraz uprawnień osób, wobec których system taki ma być stosowany. W przepisach krajowych należałoby także przewidzieć zasady odpowiedzialności pracodawcy za nielegalne albo nieprawidłowe korzystanie z neurotechnologii. Przetwarzania neurodanych w systemach AI musi, poza powyższym, nadal spełniać wszystkie warunki i zasady ochrony danych osobowych, takie jak wymogi minimalizacji, proporcjonalności, celowości, adekwatności, przejrzystości i bezpieczeństwa danych, określone w RODO.

Wnioski

Nie podważając potencjału nowych technologii i ich przydatności, np. do poprawy stanu zdrowia i ratowania życia, trzeba zauważyć, że w stosunkach pracy zastosowanie technologii wykorzystujących sztuczną inteligencję i opartych na analizie danych z mózgu budzi co najmniej obawy dotyczące niezawodności tej technologii oraz obawy etyczne i prawne. Otwarta do dyskusji pozostaje również kwestia ustanowienia katalogu neuropraw w środowisku pracy. Tylko pogłębiona refleksja pozwoli zdecydować, czy tworzyć nowe prawa chroniące ludzki umysł przed ingerencją czy też wystarczy inaczej (szerzej) interpretować istniejące.

Zaprezentowane wyżej rozważania nie wyczerpują w żaden sposób tematyki zasygnalizowanej w prezentowanym artykule. Ze względu na ograniczone ramy opracowania zawiera ono jedynie wskazanie obszarów, które powinny być przedmiotem szerszej i pogłębionej analizy. Środowisko pracy nie uniknie zmian technologicznych, które być może wymagać będą nowego spojrzenia na stosunki pracy i relacje między stronami tych stosunków prawnych. Niezwykle inwazyjny charakter neurotechnologii z jednej strony oraz z drugiej potencjalne korzyści wynikające z niej domagają się rzetelnych i odpowiedzialnych reakcji ustawodawcy. Konieczne jest podjęcie działań, które mogą zapobiegać wkraczaniu technologii nie tylko w rozpoznaną i prawnie regulowaną sferę prywatności pracowników w miejscu pracy, lecz także w sferę intymności ich myśli, uczuć i emocji, ale jednocześnie dadzą jasne wytyczne pracodawcom, czy i jak z tych rozwiązań mogą korzystać dla dobra pracowników.

BIBLIOGRAFIA

Adamczyk, S. & Surdykowska, B. (2021). Cyborgizacja człowieka pracy. Czy godność pracy ludzkiej przetrwa. W stulecie urodzin Stanisława Lema. *Praca i Zabezpieczenie Społeczne*, *12*, 3–11.

Appel, J. M. (2008, lipiec). When the boss turns pusher: a proposal for employee protections in the age of cosmetic neurology. *Journal of Medical Ethics*, *34*, 616–618. DOI:10.1136/jme.2007.022723

Arico, P., Sciaraffa, N. & Babiloni, F. (2020). Brain–computer interfaces: toward a daily life employment. *Brain Science*, *10*(3), 2–4. DOI: 10.3390/brainsci10030157

Article 29 Data Protection Working Party. (2003, 1 sierpnia). *Working document on biometrics*. WP 80. www.ec.europa.eu

Bastian, B. & Haslam, N. (2011). Experiencing dehumanization: Cognitive and emotional effects of everyday dehumanization. *Basic and Applied Social Psychology*, *33*(4), 295–303. DOI: 10.1080/01973533.201.614132

Bonaci, T., Calo, R. & Chizeck, H. J. (2015). App Stores for the Brain: Privacy & Security in Brain-Computer Interfaces. IEEE International Symposium on Ethics in Science, Technology and Engineering. *IEEE Technology & Society Magazine, 34*(2), 32–39. https://ssrn.com/abstract=2788104

Cofas, A. (2022, 19 stycznia). Energizing the Brain: Combating Worker Fatigue Using Wearable Neurotechnology. *Texas A&M Today*. https://engineering.tamu.edu/news/2022/01/energizing-the-brain-combating-worker-fatigue-using-wearable-neurotechnology.html

Dehais, F., Lafont, A., Roy, R. & Fairclough, S. (2020). A Neuroergonomics Approach to Mental Workload, Engagement and Human Performance. *Frontiers in Neuroscience*, *14*, 73–89. DOI: 103389/fnins.2020.00268

Drage, E. & Mackereth, K. (2022). Does AI Debias Recruitment? Race, Gender, and AI's "Eradication of Diference". *Philosophy & Technology*, *35*, 9–12. https://link.springer.com/article/10.1007/s13347–022-00543–1

Eaton, M. L. & Illes, J. (2007). Commercialising cognitive neurotechnology – the ethical terrain. *Nature Biotechnology*, *25*(4), 393–397, DOI: 10.1038/nbt0407–393

Eisenberger, N. I. (2021). Broken Hearts and Broken Bones: A Neural Perspective on the Similarities Between Social and Physical Pain. *Current Directions Psychology Sciente*, *21*, 42–45. DOI: 10.1177/0963721411429455

European Commission. (2025, 4 lutego). Annex to the Communication to the Commission Approval of the content of the draft Communication from the Commission – *Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)*. https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act

EDPS, European Data Protection Supervisor (2024). *TechDispatch, Neurodata*. DOI: 10.2804/770800

Finn, E. S., Shen, X., Scheinost, D., Rosenberg, M. D., Huang, J., Chun, M. M., Papademetris, X. & Constable, R.T. (2015). Functional connectome fingerprinting: identifying individuals using patterns of brain connectivity. *Nature Neuroscience, 18*, 1664–1671. DOI: 10.1038/nn.4135

Fox, D. & Stein, A. (2015). Dualism and Doctrin. *Indiana Law Journal*, *90*, 975–1010. https://www.repository.law.indiana.edu/ilj/vol90/iss3/2

Głuchowska, J. (2024, 9 maja). Neurodane – dane neuronowe i ochrona prywatności – nowa regulacja w Stanach Zjednoczonych, czy przepisy unijne (UE) nadążają za rozwojem nowych technologii? https://auraco.pl/blog/neurodane-dane-neuronowe-i-ochrona-prywatnosci-nowa-regulacja-w-usa-czy-przepisy-ue-nadazaja-za-rozwojem-nowych-technologii/

Goodenough, O. R. & Tucker, M. (2010). Law and Cognitive Neuroscience . *Annual Review of Law and Social Sci*ence*, 6*, 61–92. DOI: 10.1146/annurev.lawsocsci.093008.131523

Holman, D., Chissick, C. & Totterdell, P. (2002, marzec). The Effects of Performance Monitoring Emotional Labor and Well-Being in Call Centers. *Motivation and Emotion*, *26*(1), 57–81. https://www.researchgate.net/profile/David-Holman-6/publication/225615265_The_Effects_of_Performance_Monitoring_on_Emotional_Labor_and_Well-Being_in_Call_Centers/links/02e7e53295dffc30db000000/The-Effects-of-Performance-Monitoring-on-Emotional-Labor-and-Well-Being-in-Call-Centers.pdf

Ienca, M. & Andorno, R. (2017). Towards new human rights in the age of neuroscience and neurotechnology. *Life Sciences, Society and Policy*, *13*(5), 1–27. DOI: 10.1186/s40504–017-0050–1

Ienca, M. & Ignatiadis, K. (2020). Artificial intelligence in clinical neuroscience: methodological and ethical challenges. *AJOB Neuroscience, 11*, 77–87. DOI: 10.1080/21507740.2020.1740352

Ienca, M., Fins, J. J., Jox, R. J., Jotterand, F., Voeneky, S., Andorno, R., Ball, T., Castelluccia, C., Chavarriaga, R., Chneiweiss, H., Ferretti, A., Friedrich, O., Hurst, S., Merkel, G., MolnárGábor, F., Rickli, J., Scheibner, J., Vayena, E., Yuste, R. & Kellmeyer, P. (2022). Towards a Governance Framework for Brain Data. *Neuroethics*, *15*, 1–14. DOI: 10.1007/s12152–022-09498–8

ICO, Information Commissioner´s Office. (2023). *Tech futures: neurotechnology*. https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/technology-and-innovation/ico-tech-futures-neurotechnology/

Jalan, S., Punj, N. (2025) Leveraging Neurotechnology for Revolutionizing HR Practices, in: Kaur, J. (ed.) *Technological Enhancements for Improving Employee Performance, Safety, and Well-Being*. (pp.211–228). IGI Global Scientific Publishing. https://doi.org/10.4018/979–8-3693–9631-5

Karthikeyan, R., Smoot, M. R. & Mehta, R. K. (2021). Anodal tDCS augments and preserves working memory beyond time-on-task deficits. *Scientific Reports, 11*, 19134. DOI: 10.1038/s41598–021-98636-y

Kolber, A. J. (2014, 19 marca). Will There Be a Neurolaw Revolution? *Indiana Law Journal*, *89*, 807–845. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2398071

Krupa, M. (2020). Neuroprawo: próba zaklasyfikowania dowodu w postaci obrazowania mózgu z badania fMRI w polskim procesie karnym. *Czasopismo Prawa Karnego i Nauk Penalnych*, *4*, 87–116.

Latos-Miłkowska, M. & Kibil, M. (2024). Czy jesteśmy gotowi na sztuczną inteligencję w zatrudnieniu? *Studia z Zakresu Prawa Pracy i Polityki Społecznej*, *3*, 153–166. DOI:10.4467/25444654 SPP.24.013.19925

Muhl, E. & Andorno, R. (2023). Neurosurveillance in the Workplace: Do Employers Protecting Cognition: Background Paper on Human Rights and Neurotechnology have the Right to Monitor Employees' Minds? *Frontiers in Human Dynamics, 5*, 1245619. DOI:10.3389/fhumd.2023.1245619

Müller, S. M., Schiebener, J. & Brand, M. (2021). Liebherr Magnus, Decisionmaking, cognitive functions, impulsivity, and media multitasking expectancies in high versus low media multitaskers. *Cognitive Processing*, *22*, 593–607. DOI:10.1007/s10339–021-01029–2

OECD. (2019, 11 grudnia). Rekomendacja Rady ds. Odpowiedzialnej Innowacji w Neurotechnologii. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0457

Palaniappan, R. & D. Mandic, D.(2007). EEG Based Biometric Framework for Automatic Identity Verification. *Journal of VLSI Signal Processing*, *49*(2), 243–250. DOI:10.1007/s11265–007-0078–1

Parlament Europejski i Rada UE. (2016, 27 kwietnia). Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE. L. 2016.119).

Parlament Europejski i Rada UE. (2024, 13 czerwca). Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) (Dz. Urz. UE. L.2024.1689).

Patel, V., Chesmore, A., Legner, C.M. & Pandey, S. (2022). Trends in Workplace Wearable Technologies and Connected-Worker Solutions for Next-Generation Occupational Safety, Health, and Productivity. *Advanced Intelligent System– 4*. DOI:10.1002/aisy.202100099

Rosen, J. (2007, 11 marca). The Brain on the Stand. *N.Y. TIMES MAGAZINE*. http://www.nytimes.com/2007/03/11/ magazine/11Neurolaw.t.html

Rosenthal, H. (2019). Scanning for Justice: using neuroscience to create a more inclusive legal system. *Columbia Human Rights Law Review, 50.3,* 290–337. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3413213#

Sejm Rzeczypospolitej Polskiej. (1974). Ustawa z dnia 26 czerwca 1974 r., Kodeks pracy (t.j. Dz.U. 2023, poz. 1465).

Sela, Y., Santamaria, L., Amichai-Hamburge, Y. & Leong, V. (2020). Towards a Personalized Multi-Domain Digital Neurophenotyping Model for the Detection and Treatment of Mood Trajectories. *Sensors, 20*, 5781. DOI: 10.3390/s20205781

Siegel, R., König, C. J. & Lazar, V. (2022). The impact of electronic monitoring on employees' job satisfaction, stress, performance, and counterproductive work behavior: A meta-analysis. *Computers in Human Behavior Reports*, *8*, 2–3. DOI:10.1016/j.chbr.2022.100227

Słocka, L. (2021). Aktualność unijnego systemu ochrony danych osobowych w świetle przetwarzania neurodanych. *Przegląd Prawa Medycznego*, *3–4*(8), 79–97.

Surdykowska, B. (2025). Jak długo nasze ciała pozostaną nasze? Kilka uwag o udoskonalaniu człowieka w kontekście wykonywania pracy. w: M. Gersdorf, & E. Maniewska (red.), *Prawo pracy wobec nowych technologii* (ss. 308–319*)*. Wolters Kluwer.

Twenge, J. M., Catanese, K. R. & Baumeister, R. F. (2003). Social Exclusion and the Deconstructed State: Time Perception, Meaninglessness, Lethargy, Lack of Emotion, and Self-Awareness. *Journal of Personality and Social Psychology*, *85*(3), 409–423. DOI: 10.1037/0022–3514.85.3.409

Tovino, S. (2007). Functional Neuroimaging and the Law: Trends and Directions for Future Scholarship, *The American Journal of Bioethics7*(9), 44–56. DOI 10.1080/1526516070158714

Wood, A. J., *Algorithmic Management: Consequences for Work Organisation and Working Conditions,* Seville: European Commission, 2021, JRC124874.

Yuste, R., Genser, J. S. & Herrmann, S. (2021). It's time for neuro-rights. *Horizons*, *18*, 154–164.

Wilson, J. H. (2013, wrzesień). Wearables in the Workplace. *Harvard Business Review*. https://hbr.org/2013/09/wearables-in-the-workplace

Bialystok Legal Studies
Białostockie Studia Prawnicze
2025 vol. 30 no. 4

sciendo

DOI: 10.15290/bsp.2025.30.04.07

Received: 31.03.2025
Accepted: 10.09.2025

Michał Jacuński
University of Wroclaw, Poland
michal.jacunski@uwr.edu.pl
ORCID ID: 0000–0002–6492–4945

The Limited Use and Non-Use of Digital Tools and Technologies in the Activities of Political Parties in Poland

Abstract: This article examines selected causes and manifestations of a limited use or outright non-use of digital technologies and tools by political parties in Poland. The analysis focuses on key areas of party activity within the digital ecosystem, particularly internal dimensions such as membership, party financing, internal e-voting, and decision-making processes. The research design combines a review of the existing literature, critical analysis of primary sources (including party websites and statutes), and original data derived from an expert survey.

Keywords: digitalisation, political parties, digital abstention, Polish politics

Introduction

Political parties operate in a digital environment and have been doing so for at least two decades. To better describe the conceptual framework for studying digitalisation, Dommett et al. (2020) termed this the 'party-centred digital ecosystem'. A substantial corpus of literature exists in the domain of political science and the study of political parties that addresses the processes of these organisations' transitions to the digital realm (see Correa et al., 2021; Deseriis, 2020; Gerbaudo, 2019; González-Cacheda & Cancela Outeda, 2024; Klimowicz, 2018). There is a broad consensus that digital technology is becoming an increasingly significant component of political parties' internal and external activity in contemporary liberal and competitive democracies. Digital technology has had a profound impact on the manner in which political parties conduct their internal operations and engage with the public. Internally, the implementation of

digital tools such as party management software, online communication platforms, and e-voting systems has led to significant improvements in organisational processes, decision-making, and enhanced transparency among members. These technologies enable parties to manage membership data more efficiently, coordinate activities across diverse geographic locations, and foster real-time communication through platforms like Slack or dedicated intranets. Externally, digital technology has revolutionised political campaigning by providing platforms for targeted communication, social mobilisation, and rapid dissemination of political messages. Social media networks and mobile applications empower political parties to access wider audiences, engage with voters in interactive ways, and personalise outreach efforts, which may potentially increase voter participation and political efficacy.

While it is relatively straightforward to identify papers and research on the use and development of digital technologies and tools, it is more challenging to locate work or complex studies on the non-use of technology. This article will address a significant research gap in this domain by analysing the non-use or limited use of digital tools and technologies (hereafter referred to as DTT) by political parties in Poland. Its objective is to identify manifestations and the underlying causes of the non-use or limited use of DTT. Based on the problems introduced and the state of the art, the article poses several research questions: What are the areas of activity in which political parties in Poland refrain from or limit the use of DTT? What are the underlying causes of this digital abstention? The investigation goes on to consider whether these phenomena might be attributed to technological barriers or other limitations. In order to achieve the research objectives and answer the questions posed, I use the following research methods: analysis of literature on party organisation and digitalisation, critical analysis of party statutes and other party-related documents, content analysis of parties' websites, and the expert survey method. The article is divided into three sections: a theoretical section conceptualising the limited use of technology, empirical sections related to Polish political parties and analysis of digital tools and their application, followed by expert perceptions of DTT use. The last section discusses the limitations of the study and summarises the research findings.

1. Conceptualising the limited use of technology among political parties

The issue of the non-use of DTT necessitates an elucidation of their definition within the context of political activity. Moreover, it is imperative to delineate the concept of the non-use of technology in an era of advancing technologisation and digitalisation. For the purposes of this article, I employ the terms 'digitalisation' and 'digital tools and technologies', which are understood as follows: digital technology is generally defined as the set of tools, systems, and devices that encode, store, process, and trans-

mit information using digital signals represented in binary form. Digital technology is distinguished from other technologies that rely on analogue signals by its use of digital representations of information; this encompasses computers, software applications, digital communication networks, and associated devices and infrastructures. International organisations such as the OECD (OECD, 2025) acknowledge digital technology within the context of information and communication technologies (ICT) and digital data, emphasising its role in enabling automation, improving efficiency, and fostering global communication to shape a positive digital future. The scientific understanding of digital technology emphasises its capability to transform data into actionable information, thus driving innovation and influencing nearly every aspect of modern life.

Digitalisation in the context of political parties pertains to the utilisation of digital instruments and technologies in the internal and external dimensions of party operations. The term 'digital tools' refers to specific web applications, computer programs, or platforms that use online communication to enable specific functions in a digital environment, whereas a lack of digital implementations often centres around concepts such as 'digital non-use', 'digital abstention', or 'digital exclusion'. I will briefly explain these and link them with political parties.

Digital non-use is defined as a state in which individuals either never adopt or actively disengage from digital technologies. This concept is closely tied to the idea of the digital divide, where non-use may further entrench existing social inequalities. Digital abstention, as defined in several academic studies, pertains to a deliberate rejection of digital technology. This phenomenon can be attributed to various factors, including personal values, concerns regarding privacy, or resistance to technological change. Digital exclusion is a broader concept that encompasses both non-use and forced non-use, mainly due to socio-economic factors and low digital literacy. It is defined as the outcome of systemic barriers, such as limited access to digital technologies, insufficient digital literacy, or economic constraints, that prevent individuals from participating fully in the digital society. These definitions typically distinguish between individuals who lack access to digital tools due to structural barriers and those who deliberately refrain from using technology.

Existing academic work has significantly advanced our understanding of digital non-use, digital abstention, and digital exclusion by revealing their multifaceted nature, but they do not explain technology non-use among political organisations. A growing body of research (Boulianne, 2015; Norris, 2001; Vaccari & Valeriani, 2015) has examined the surprisingly low uptake of digital technologies in political engagement, revealing that technological access alone does not guarantee political participation. The collective analysis of this work underscores that the underutilisation of technology in politics is not merely a consequence of inadequate access but rather reflects a complex interplay of cognitive, cultural, and structural factors that must be addressed to fully harness the potential of digital innovations in democratic processes.

One of the consequences for parties and their members of technological transformations, observed across society, is the digital divide triggered by digital exclusion. The competencies required to leverage digital media to its fullest extent are not distributed uniformly among rank-and-file party members, nor do they align among political activists or representatives. This phenomenon can be conceptualised as a group of 'losers of digitalisation', or those who deliberately oppose modernity (Jacuński, 2018, p. 7).

Table 1 outlines the distinctions between digital non-use, digital abstention, and digital exclusion, and their respective implications for party members and organisational dynamics. Digital non-use refers to a state where parties or members either never adopt or actively disengage from digital technologies, often relying on traditional tools and exhibiting strong organisational inertia rooted in institutional norms. Digital abstention represents a deliberate resistance to digital innovation, where party elites may suppress technological change to retain control, offering members conventional modes of participation and adopting digital tools only sporadically or in hybrid forms. In contrast, digital exclusion highlights the unintended consequences of digitally native parties that, while technologically advanced, fail to accommodate members with low digital literacy or limited access – thereby reinforcing socio-economic divides.

Table 1. The relation between concepts and their impact on party members and party organisation.

Concept	Digital non-use	Digital abstention	Digital exclusion
Meaning	A state in which individuals or organisations either never adopt or actively disengage from digital technologies.	A deliberate rejection of digital technology; resistance to technological change.	Non-use and forced non-use due to low digital literacy or socio-economic factors.
Impact on party members and sympathisers	Party members and sympathisers choose not to use many ICT tools and rely on traditional solutions. They can deliberately refrain from use or stay connected via grassroots digital tools.	Party members are offered traditional forms of engagement. Party leaders may also deliberately prevent technological change to better control members' behaviour.	Digital-native parties may be technologically savvy and digitally advanced. They contribute to the digital divide and exclusion due to not offering, or having a limited offer, for offline engagement.
Impact on party organisation	ICT and digital tools have limited impact on party functioning and institutionalisation. Party structures ignore changes due to embedded rules, norms, and reputations. Organisational inertia is observed.	Technology and digital solutions are sporadically used. Hybrid solutions can be introduced, which is typical for late adopters. Party structures resist change due to embedded rules, norms, and reputations.	Party organisation neglects chances to remain open to less affluent and digitally literate individuals; its digital nature limits inclusion and accessibility.

Source: own elaboration

A limited use of technology can also be theoretically explained by broader historical and sociological institutionalism and path-dependency frameworks, which help us understand how party structures resist change due to embedded rules, norms, and reputations. The face-to-face foundations of party organisations created norms and procedures that parties are incentivised to maintain, even as new tech arises, which may be reflected in a historical reliance on local party networks or a central party office for legitimacy and control. Institutions reinforce internal legitimacy through long-standing procedures, so that informal hierarchies may view digital systems as threats to vertical authority and elite control. Path dependency in party organisational developments assumes that early institutional choices, which were often contingent or pragmatic at the time, produce self-reinforcing mechanisms. In such a loop, a lack of member pressure results in low innovation levels, which brings few digital users and returns to a state of no pressure.

Having addressed the limited use of technology, we move beyond the theoretical framework to assess how Polish political parties operationally employ DTT or not. The following sections of the article empirically examine the existence or non-existence of digital tools.

2. Empirical analysis

The first empirical section is based on the content and a functional analysis of nine official political party websites, supplemented by analysis of party statutes and historical analysis of selected digital practices. The sample was selected using the criterion of representation: all the parties are represented in the lower house of parliament (the Polish Sejm). Based on the matrix of digital instruments proposed by González-Cacheda et al. (2022), an extended list of nine digital features was proposed to analyse several aspects of digital party functioning: e-participation (online membership, e-voting, participatory programmes), funding (micro-donations, micro-credits), deliberation (discussion forums), and contact (mailboxes). Social media icons were also taken into account, as they enable participation, deliberation, and contact across the board.

2.1. E-participation

The use of technology in the context of applying for membership of political parties has been widely discussed in the literature. Sobolewska-Myślik et al. (2007, p. 439) cite the thesis of Seyd and Whiteley (2004) that the decline in interest in membership of political parties is not only the result of structural changes in society, and therefore not only that citizens have lost interest in party membership, but also because parties are not as interested in recruiting members as they once were. This prompts the question of the efficacy of contemporary technologies and digital tools for remote registration and verification of membership in various social and civic

initiatives, in the absence of any interest in their implementation. A thorough examination of party statutes and relevant websites reveals that parties solely permit the initiation of the recruitment procedure online. Statutory eligibility rules (age, citizenship, acceptance of the party code or programme) are common across parties that have published statutes. The application process for membership is reduced to two online steps: downloading the membership declaration and searching for information about membership structures and further procedures without the use of digital tools. Full membership generally requires additional steps, such as personal meetings or submitting signed documents. To analyse the parties more closely: Poland 2050 (Polska 2050), the Left (Nowa Lewica), and Civic Platform (Platforma Obywatelska, PO) provide robust digital onboarding for new members, including online forms and automated follow-up consistent with their statutes. The Polish Peasants' Party (Polskie Stronnictwo Ludowe, PSL) offers membership through downloadable documentation, but lacks an end-to-end web-based process. Law and Justice (Prawo i Sprawiedliwość, PiS), the Confederation (Konfederacja), the Greens (Zieloni), and Polish Initiative (Inicjatywa Polska, IPl) either do not support online member applications or keep membership processes largely offline or internal. The Together Party (Partia Razem) offers a 'Join' feature on its official site but links it to volunteering or supporting, not a formal membership registration.

According to the PiS party statutes (article 5(3)), membership of the organisation is granted upon resolution by the PiS district board, regional board, political committee, or by a decision of the PiS Secretary General, subsequent to the submission of a written declaration and relevant documentation. Article 38 stipulates that individuals aged between 16 and 30 are eligible to join the Youth Forum; the procedure for admission to this is not specified in the statute.

The Civic Platform party has adopted a more streamlined approach to membership, with an online application and confirmation of registration via a link in an email constituting the entire procedure. The subsequent steps are completed in accordance with conventional methods, namely by liaising with a regional office employee, submitting a membership declaration, and participating in a local chapter meeting. The Polish Peasants' Party asserts that the process of becoming a member is streamlined to a mere three steps: firstly, downloading the membership form from the party's official website, then locating a local branch within one's municipality, and finally submitting the completed form (the method of submission remains ambiguous). A similar approach is adopted by the National Movement party, part of the right-wing coalition Confederation Liberty and Independence (Konfederacja Wolność i Niepodległość), frequently shortened to just Confederation (Konfederacja). Interested individuals may join the National Movement via the Confederation's website. This conservative approach to the acceptance of new members, and the lack of digital tools that allow for single-step registration of new members, may be due, for example, to a fear that members with an established position in the organisational

structure may lose the party authorities' control over the membership structure before new members are accepted.

No major Polish political party currently offers a publicly visible internal electronic voting platform, such as Zeus, used by the Together Party. While PSL supports the concept in principle, there is no evidence that it is implemented internally, and Civic Platform only refers to a historical 2013 online vote. None of the parties provide participatory platforms enabling cocreation or policy engagement; they are virtually absent, with The Left being the sole exception, inviting member input via email consultations. Participatory platforms, whether digital or hybrid, can foster more inclusive, responsive, and dynamic modes of political engagement; they encourage party members and sympathisers to contribute directly to the development of political programmes, policy proposals, and strategic priorities. Unlike traditional top-down models, participatory infrastructures create horizontal communication channels, where grassroots actors are not merely recipients of party leaders' messaging but active agents in shaping it. Such platforms advance intra-party democracy by institutionalising deliberation and feedback loops between the leadership and rank-and-file members. Their absence may mean that the parties analysed, no matter their size, age, or political leaning, refrain from creating a digital participatory environment. This does not mean that parties are against using participatory pathways, but it is merely visible in an online form.

2.2. Funding

Micro-donations, usually small contributions made by individual supporters, represent one component of party finance. Their function is to diversify sources of party income, making parties less reliant on public subsidies. In many campaigns micro-donations are often seen as a mechanism for grassroots mobilisation and empowerment. They allow engagement through material support, fostering a sense of political belonging. For newer parties without institutional funding, or for those outside the mainstream, this form of financing can be a vital resource for survival. Micro-donation infrastructures are often digitally mediated, using low – barrier tools such as recurring payments, crowdfunding, or in-app contribution buttons. Political marketers understand that simplified transfers can also provide valuable data on supporters' behaviour, geographic distribution, etc.

The use of technological systems to facilitate political party financing leads us to Confederation and Poland 2050, the only parties that offer the functionality of donations using an efficient and uncomplicated payment mechanism. In the case of Confederation it is the Paybynet system, which has been implemented by the National Clearing House (Krajowa Izba Rozliczeniowa S. A.). This mechanism, which is well known and commonly used in e-commerce solutions, has been implemented on the Confederation's website: there is a 'Support' page with preset donation tiers (e.g. PLN 25, 50, 100), suggesting small donations, but lacking recurring micro-credits. Poland

2050 enables small individual donations (even starting at PLN 10) and allows electronic recurring payments via PayU. Donors can set small amounts and automate monthly contributions.

In contrast, the other major political parties in Poland use conventional bank transfers as the primary means of financial collection. The Together Party has a 'Support' section for contributions, but this appears to be standard donation amounts, without micro-payment flexibility or recurring support. The Left provides a public register of donations, and regional pages list bank transfer donation options; no user-oriented interactive micro-donation features are accessible. PiS, PSL, and the Greens offer donation via a standard bank transfer form, with legal disclaimers and limits; there are no visible micro-donation interfaces or widgets, nor recurring options. The requirement for the payer to provide their full details is a mandatory prerequisite, whereas the use of instant payment mechanisms or alternative methods such as the mobile payment system BLIK is not a possibility. The Civic Platform, on the other hand, offers the possibility to support various causes, such as a party or an election fund for a presidential campaign.

While the technological possibilities for fundraising exist, political parties evince a marked conservatism with regard to the methods by which they raise funds from supporters. This conservatism may be attributed to various factors, including the stringent donor oversight requirements, the stipulations for a public register of donations, and the reliance on public funding, which provides the majority of financial resources for major political parties. In terms of technological innovation, the potential implementation of digital reporting tools for political party finance, with the aim of introducing traceability mechanisms at all stages of the process, is also indicated.

While parties could ensure greater transparency in terms of financing, the system is imperfect in Poland. Article 11(2) of the Polish Constitution stipulates the requirement for transparency in the financing of political parties. Digital technologies have the capacity to facilitate the online publication of financial statements, thereby enhancing citizens' access to information regarding the sources of parties' income and expenditure. For instance, the National Electoral Commission has a website that publishes the financial statements of political parties, thereby allowing public scrutiny of them. Digital technologies facilitate the process of collecting contributions through online payment systems, which increases convenience for donors and efficiency in financial management. However, it should be noted that the Political Parties Act stipulates that political parties are only permitted to accept funds from Polish citizens permanently residing within the country's borders. This necessitates the implementation of robust mechanisms to verify the identity of donors within online systems. As of 1 July 2022, political parties are obligated to disclose information regarding donations received, with the stipulation that these donations exceed PLN 10,000 annually.

It is notable that certain parties have adopted a more comprehensive approach by publishing data on all donations, including smaller ones. The Civic Platform has

made available on its website a downloadable PDF file containing a register of approximately 1,700 individuals who have donated, including both minor and substantial contributions (the smallest donation was PLN 50, and the largest over PLN 50,000). A comparable approach is adopted by the PSL. Poland 2050 offers online access to the document via the party's website at the Polish Public Information Bulletin (BIP). It is noteworthy that certain political parties opt not to disclose donations below PLN 10,000, opt for the anonymisation of individual data within contractual agreements, and refrain from disclosing the specific value or details of these contracts.

2.3. Deliberation and contact

Earlier empirical research on party members in Poland (Jacuński, 2023) indicated that party members perceive traditional and direct forms of interaction and deliberation as attractive. However, new parties with younger members clearly expected and practised more online activities. For instance the Together Party used communication and decision-making software, such as Zeus or Slack, to better perform and streamline administrative tasks, enabling efficient member registration, financial tracking, and event organisation. Internal communication platforms, dedicated forums, and integrated solutions facilitated real-time dialogue among Together Party members, thereby fostering a more collaborative environment. The significance of these tools extends beyond mere operational efficiency, as they also play a crucial role in cultivating a culture of transparency and accountability within the organisation. Is this also the case in the analysed sample of parties? In the case of other parties, it was not recognisable that they offered avenues for deliberation or any other specific solutions. Party websites do not offer discussion forums or members-only areas. The Left's website contains historical thematic regional and policy forums; it can be assumed that their existence and the links to social media compensate for the lack of discussion and deliberation features on websites.

Poland 2050, Confederation, the Together Party, the Left, PO, the Greens, and PSL offer clear public email contacts, including general offices and media/press addresses. IPl uses an online contact form instead of listing a direct email. PiS does not disclose a central party email publicly, though certain individual MP offices provide email contacts. The above-mentioned features are similar across all parties, and one can assume that their standardisation dates back to the early development of websites.

Table 2 presents a comparative overview of selected digital instruments across major parties in Poland, ranging from online membership and micro-donations to participatory programmes and social media integration. These tools are indicative of each party's approach to internal democratisation, technological adoption, and member accessibility. The table highlights both the presence and the absence of mechanisms such as electronic voting, member mailboxes, and discussion forums, offering insight into whether parties merely communicate digitally or also enable participatory engagement

through digital channels. This empirical mapping serves as the basis for analysis of the broader digital infrastructure and democratic inclusivity of party organisations.

Table 2. Selected digital tools and their application among Polish political parties' official websites.

Party name	Online membership	Micro-donations	Micro-credits	E-voting	Discussion forum	Participatory programme	Mailbox	Social media icons
IPI	No	No	No	No	No	No	Contact form	Yes
Confederation	No	Yes (donation form with fixed amounts)	No	No	No	No	Party units and press contact	Yes
Left	Online contact form + PDF package	No (bank transfers only)	No	No	Historical thematic forums (regional/policy)	Encourages consultations via email	General email and press contact	Yes
Together Party	Only volunteer/support options	Yes (Donation via micropayment interface)	No	Not mentioned (however, use of open-source Zeus platform)	No	No	General email and press contact	Yes
PiS	No	No (bank transfers only)	No	No	No	No	General email	No
PL 2050	Form + declaration + regional follow-up	Yes (small online donations via payment widgets)	No	No	No	No	Contact form + email	Yes
PO	Email form, confirmation + regional follow-up	No (bank transfers only)	No	No	No	No	General email	Yes
PSL	PDF form + offline submission	No (bank transfers only)	No	No	No	No	Executive committee and press contact	Yes

Greens	Online contact form for members and sympathisers	No (bank transfers only)	No	No	No	No	General email and press contact	Yes

Note: IPl: Inicjatywa Polska (Polish Initiative); Konfederacja (Confederation); Lewica: Nowa Lewica (New Left); Partia Razem (Together Party); PiS: Prawo i Sprawiedliwość (Law and Justice); PL 2050: Polska 2050 (Poland 2050); PO: Platforma Obywatelska (The Civic Platform); PSL: Polskie Stronnictwo Ludowe (The Polish Peasants' Party); Zieloni (Greens).

Source: own elaboration based on matrix by González-Cacheda et al. (2022, p. 341).

3. The use of DTT by political parties according to an expert survey

I conducted an expert survey among Polish scholars dealing with political parties in order to validate their own research findings and to possibly expand the field of research on the use or non-use of DTT by political parties in Poland.[1] The invitation was extended to participate in the survey, which employed an online structured questionnaire with the objective of enhancing the identification and evaluation of the tools utilised by political parties in Poland. The final sample of respondents numbered 25. The tools that were primarily mentioned mostly included communication tools, such as websites, social media, vlogs, and blogs. When asked about the existence of any digital tools used by political parties, respondents again indicated that parties primarily use social media, including social networking sites, blogs, and similar platforms. The most frequently cited social media platforms included Facebook, YouTube, Instagram, X, and TikTok. Concurrently, a significant proportion of experts expressed the opinion that digital tools are not being utilised to their full potential by political parties in Poland. Specifically, they are not employed in the areas of internal democratisation (52% of responses), decision-making and deliberative processes (44%), the creation of political/election programmes (44%), and the selection of candidates in elections or leadership processes (40%).

The participants in the expert survey identified two main barriers to the digitalisation of political parties in Poland: firstly, the leaders' fear of destabilising established procedures and hierarchies (56% of responses), and secondly, a lack of expertise and human resources, including experts in the field of new technologies (48%). Additionally, in the context of digital democratic innovations, respondents highlighted the presence of varying degrees of internal democracy within Polish political parties.

1 The survey, 'The digitisation process in Polish political parties', was conducted in February 2025. Party researchers were directly invited to participate in the study based on their membership in the research section of the Polish Political Science Association and/or their scholarly achievements. The survey is part of the research project 'Political actors and the digitalisation of internal and external environments'.

Utilising a scale of 1–5, where 1 signifies a low level of internal democracy and 5 signifies a high level, the least democratic parties were identified as Law and Justice and Confederation, while the most democratic parties are considered to be the Greens, the Left, and the Together Party. Opinions are ambivalent towards some parties, especially from the current ruling coalition (including Confederation and PSL): some consider them democratic, others do not. This suggests that organisational culture and internal decision-making processes, which are sometimes not very democratic, may be hindering digital democratic innovations.

The experts identified several instances of democratic innovation within Polish political parties, primarily focused on universal internet voting, which allows rank-and-file party members to participate; however, these are few and far between. They include an online vote on the Democratic Left Alliance (Sojusz Lewicy Demokratycznej, SLD) programme (entitled Constitution for SLD) and primaries for the election of the party leader (e.g. PO in 2013) or the presidential candidate (e.g. PO in 2010, 2020, 2024; KORWiN: the Coalition for the Republic's Renewal, Freedom and Hope in 2020). Jasmine, a project introduced by the Poland 2050 party, is regarded as the sole unsuccessful endeavour to date in implementing such an application. In contrast, the Together Party has opted for a different approach, whereby decisions are made by party members through internal votes on the Zeus open-source platform, an independent voting system developed by GRNET and widely used in academic and organisational elections, especially in Greece. In the Civic Platform, the initiative to co-create and consult on the election programme with voters, alongside online programme discussions, was initiated in 2015; the marketing idea was not developed after the party lost the election.

The results of the expert survey also proved that limited use of DTT, as described in previous sections, is a combination of deliberate omissions and reinforcement of existing patterns and norms. It is apparent that at present, no external pressure from (new) participants in political rivalries would force modernisation and elevate party organisations to a higher level of development.

Conclusions

Academic research on the use of digital technologies by political parties is constrained by several limitations that prevent a comprehensive understanding of the phenomenon. Primarily, a significant proportion of the existing literature and empirical studies focuses exclusively on the members and the changing nature of party membership (Gauja et al., 2024; Gibson et al., 2016; Vittori, 2020; Ziegler et al., 2024).

Secondly, a persistent lack of transparency in parties' internal digital practices hinders researchers from accessing reliable data, leading to incomplete analyses. Moreover, there is limited demand for innovations and modernisation in the structures of many front-running political parties, until they are pushed to perform their digital transformation by the emergence of digitally native parties. This was presumably the case for Partido Socialista Obrero Español (PSOE) and Podemos in Spain and Parti Socialiste and La France Insoumise in France (Mompó et al., 2025, p. 10), but it has not yet materialised in Poland. Therefore digital advancements are frequently viewed as secondary concerns, compared to more pressing political issues.

The limitation of expert research is that it reduces answers to the perception of the characteristics of the objects under study, rather than necessarily confirming the actual state of affairs (e.g. whether a feature is present or not). Nevertheless, the collective knowledge of experts is a strong point; it confirms the limited implementation of advanced digital tools in Polish political parties. It does not invoke the existence of digital democratic innovations, and it confirms the barriers to the digitalisation of political parties. The latter seems to attach greater importance to internal causes than to external ones, such as legal or technological barriers.

The analysis of digital practices across Polish political parties reveals a persistent disconnection between the technological potential for democratisation or improvements and the organisational realities of party life. Despite the widespread availability of digital tools for participation and transparency, most parties continue to offer minimal opportunities for member input or deliberation. This suggests that even a limited use of digital tools does not automatically translate into the democratisation of outcomes and that in many cases, elite control and organisational routine often outweigh the participatory affordances of technology.

In comparison with many of their western European counterparts, some of which have adopted online primaries, member consultations, or policy co-creation, Polish political parties appear to be undergoing a limited internal transformation in terms of adopting digital innovations to enhance intra-party democracy, facilitate candidate selection procedures, conduct online consultations, or co-decide policy development and implementation. In the context of the formation and organisation of political parties in Poland, it is therefore inaccurate to mention an entire non-use of technology; rather, the focus should be on the limited use of technology in the establishment and in party governance.

The hesitancy or restraint exhibited by mainstream political parties in Poland towards using solutions that are available and practised in other countries or sectors is rather due to the specific organisational model of parties, described in the literature (cf. Bennett et al., 2018; Bolleyer, 2012) as hierarchical, stratarchic, and connective. In Poland, parties with a typically hierarchical structure do not allow solutions that disrupt control over the party. Conversely, those with a stratarchical organisational model, predominantly left-wing and green parties, have been observed to resort to

consultation mechanisms such as referendums, albeit infrequently. The Together Party, which is similar to the connective model, is notable for the fact that it is easier to use digital tools in an organisation with several thousand members than in one with many times that number. The absence of an offer for light members or sympathisers, compounded by the failure to sustain Poland 2050's Jasmine application, and the absence of pressure from rank-and-file members to adopt new technological solutions collectively indicate that a breakthrough in this area is improbable. Consequently, the relevant parties in Poland can continue to exercise digital abstention, limiting the use of technology to communication and external purposes related to the conduct of election marketing campaigns.

The divergence among parties is related to their age and size. Newer and smaller parties like Poland 2050, the Together Party, and Confederation exhibit relatively more openness to digital innovation, albeit often in symbolic or limited ways. In contrast, mature and bigger parties, such as PiS, PSL, and the Civic Platform, reflect the characteristics of organisations that are hierarchical, less open, and less responsive to bottom-up input. Abstention from DTT aligns with principles of historical institutionalism and risk aversion. Once parties have invested in face-to-face engagement, offline membership procedures, and hierarchical leadership and management, the organisational, cultural, and strategic costs of transitioning to a digital ecosystem possibly become too high.

In nearly all cases, there is a visible reliance on a symbolic rather than a substantive development of digital tools. While most parties prominently display social media favicons or accept online donations, they avoid providing integrated platforms for policy co-creation, e-voting, or interactive dialogue. This limited use or non-use symbolises instrumental digitalisation, where ICT does not transform internal governance.

Finally, it is important to note that this article is deliberately focused on a single-country case study. Nevertheless, I am keen to acknowledge several potential avenues for future research, such as comparative studies covering parties in Central and Eastern Europe as well as those beyond. It would be an interesting area of research for scholars to investigate how party members themselves perceive digital engagement options and how they assess limited use of DTT. In addition, it would be equally interesting to identify what external factors could drive innovations from outside traditional party hierarchies. Furthermore, research agendas exploring the conditions under which symbolic digitalisation shifts into structural transformation appear to remain open.

REFERENCES

Bennett, W. L., Segerberg, A., & Knüpfer, C. B. (2018). The democratic interface: Technology, political organisation, and diverging patterns of electoral representation. *Information, Communication & Society*, *21*(11), 1655–1680. https://doi.org/10.1080/1369118X.2017.1348533

Bolleyer, N. (2012). New party organization in Western Europe: Of party hierarchies, stratarchies and federations. *Party Politics*, 18(3), 315–336. https://doi.org/10.1177/1354068810382939

Boulianne, S. (2015). Social media use and participation: A meta-analysis of current research. *Information, Communication & Society*, *18*(5), 524–538. https://doi.org/10.1080/1369118X.2015.1008542

Correa, P., Barberà, O., Rodríguez-Teruel, J., & Sandri, G. (2021). The digitalisation of political parties in comparative perspective. In O. Barberà, G. Sandri, P. Correa, & J. Rodríguez-Teruel (Eds.), *Digital Parties. The Challenges of Online Organisation and Participation.* (pp. 287–304). Springer.

Deseriis, M. (2020). Two variants of the digital party: The platform party and the networked party. *Partecipazione e Conflitto*, *13*(1), 896–917.

Dommett, K., Kefford, G., & Power, S. (2020). The digital ecosystem: The new politics of party organization in parliamentary democracies. *Party Politics*, *27*, 847–857.

Gauja, A., Kosiara-Pedersen, K., & Weissenbach, K. (2024). Party membership and affiliation: Realizing party linkage and community in the twenty-first century. Party Politics, 31(2), 207–216. https://doi.org/10.1177/13540688241306730 (Original work published 2025)

Gerbaudo, P. (2019). *The digital party: Political organisation and online democracy*. Pluto Press.

Gibson, R., Greffet, F., & Cantijoch, M. (2016). Friend or Foe? Digital Technologies and the Changing Nature of Party Membership. *Political Communication*, *34*(1), 89–111. https://doi.org/10.1080/10584609.2016.1221011

González-Cacheda, B., & Cancela Outeda, C. (2024). Digitalisation and political parties in Europe. *Party Politics*, *31*(3), 488–498. https://doi.org/10.1177/13540688231225639 (Original work published 2025)

González-Cacheda, B., Cancela Outeda, C., & Cordal, C. (2022). Factors for the digitalisation of political parties in Portugal and Spain: A comparative perspective. *Partecipazione e Conflitto*, *15*(2), 330–350. https://doi.org/10.1285/i20356609v15i2p330

Inicjatywa Polska. (n.d.) *Strona główna*. Retrieved 16 September 2025, from ipl.org.pl

Jacuński, M. (2018). Digitalization and political party life in Poland: A study of selected communication habits of party members and elective representatives. *Polish Political Science Review*, *6*(2), 6–25.

Jacuński, M. (2023). Proces digitalizacji partii politycznych: W kierunku interdyscyplinarności badań. *Wrocławskie Studia Politologiczne*, 107–116. https://doi.org/10.19195/1643–0328.31.7

Klimowicz, D., 2018. *Network Parties: A Model for Democratizing and Digitalizing Party Politics*, Progressive Zentrum. Germany. Retrieved from https://coilink.org/20.500.12592/bwct33 on 15 Oct 2025.

Konfederacja. (n.d.) *Strona główna*. Retrieved 16 September 2025, from konfederacja.pl

Lewica (n.d.) *Strona główna*. Retrieved 16 September 2025, from lewica.org.pl

Mompó, A., Meloni, M., Barberà, O., Lupato, F., Sandri, G., & von Nostitz, F. (2025). When do parties go digital? Examining the drivers of internal and external party digitalisation. *Party Politics*, *0*(0). https://doi.org/10.1177/13540688251339977

Norris, P. (2001). *Digital divide: Civic engagement, information poverty, and the internet worldwide*. Cambridge University Press.

OECD. (2025). *Going digital*. https://www.oecd.org/en/about/projects/going-digital.html

Partii Prawo i Sprawiedliwość. (n.d.) *Strona główna*. Retrieved 16 September 2025, from bip.pis.org.pl

Platforma Obywatelska. (n.d.) *Strona główna*. Retrieved 16 September 2025, from platforma.org

Polska 2050. (n.d.) *Strona główna*. Retrieved 16 September 2025, from polska2050.pl.

Polskie Stronnictwo Ludowe. (n.d.) *Strona główna*. Retrieved 16 September 2025, from psl.pl

Razem. (n.d.) *Strona główna*. Retrieved 16 September 2025, from partiarazem.pl.

SobolewskaMyślik, K., KosowskaGąstoł, B., & Borowiec, P. (2007). Członkostwo w polskich partiach politycznych. *Politeja*, *8*, 437–460.

Vaccari, C., & Valeriani, A. (2015). Accidental exposure to politics on social media as online participation equalizer in Germany, Italy, and the United Kingdom. *New Media & Society*, *18*(9), 1857–1874. https://doi.org/10.1177/1461444815616223

Vittori, D. (2020). Membership and members' participation in new digital parties: Bring back the people? *Comparative European Politics*, *18*, 609–629. https://doi.org/10.1057/s41295–019-00201–5

Ziegler, S., Borucki, I., & Weissenbach, K. (2024). The digital transformation of party membership: How party members perceive online participation and adapt to it under pandemic circumstances. *Party Politics*, *31*(2), 251–264. https://doi.org/10.1177/13540688241306726

Zieloni. (n.d.) *Strona główna*. Retrieved 16 September 2025, from partiazieloni.pl

Bialystok Legal Studies
Białostockie Studia Prawnicze
2025 vol. 30 no. 4

sciendo

DOI: 10.15290/bsp.2025.30.04.08
Received: 18.07.2025
Accepted: 24.09.2025

Tomasz Nieborak
Adam Mickiewicz University, Poznań, Poland
tomasz.nieborak@amu.edu.pl
ORCID ID: 0000–0002–5499–9353

Digital Coercion? The Financial Market and the Right to Digital Opt-Out between Fiction and Reality

Abstract: This article examines the challenges that digitalisation poses for the regulation of contemporary financial markets and the implications for individual freedom. The financial sector demonstrates how 'digital coercion' can threaten the right not to use technology, raising questions about the balance between protecting citizens' rights and enabling participation in a digitalised economy. The focus is on how technological development, especially artificial intelligence (AI), affects everyday interactions with financial systems and whether individuals still have a genuine choice to remain outside digital frameworks. The analysis relies primarily on the dogmatic-legal method, complemented by axiological reflection and critical legal perspectives, to reveal tensions between existing regulations, constitutional values and human rights. Digital coercion occurs when opting out of technology is no longer practically possible, particularly in finance where alternatives diminish as digital tools dominate. While it may be theoretically possible to avoid financial technology, doing so risks exclusion from essential functions such as accessing credit or managing finances. EU regulations like the AI Act, MiCA and DORA reinforce this process, promoting and effectively enforcing digitalisation while limiting the right to digital opt-out. Although these frameworks aim to safeguard privacy and freedom, in practice technologies and algorithms increasingly shape financial markets, often in opaque ways. In line with Lawrence Lessig's notion that 'code is law', algorithms become de facto lawmakers, establishing norms that constrain free consumer choice. Consequently, the right not to use technology becomes largely illusory when access to fundamental services depends on technological infrastructure.

Keywords: financial market regulation, right to digital opt-out, financial exclusion, human rights, European Union, FinTech, Decentralised Finance, human beings

Introduction

It will soon be 100 years since the publication of the novel *Brave new world* by Aldous Huxley (1946). The novel combines elements of both prophetic vision and warning. Reading it today, in the age of technological revolution and ongoing debates about the future role of artificial intelligence (AI) in our daily lives, it takes on a completely different dimension (Boden, 2020, pp. 96–113). For we are now facing the emergence of a new world – Huxley's World State – which is linked through complex IT systems that operate on the basis of increasingly sophisticated and self-learning computer technologies. These systems affect all the major spheres of our everyday lives. Although this reality is a human creation, there is growing concern about the potential for these technologies to take control of our lives and, as it were, create a social destiny which will be accepted by society, much like in the Brave New World – a society where most men and women will grow up to love their servitude and will never dream of revolution (Huxley, 1946, pp. xvi–xvii), in exchange for comfort and everyday stability. Today, nearly a century later, Huxley's warning seems uncannily relevant, particularly in the context of digital coercion, which is no longer optional but rather the default mode of operation for the human being in the realm of services, including financial services. At times it may even seem that the individual, a consumer in the financial market, although seemingly aware and informed (Cyman, 2023, pp. 55–56), has become just another cog in the financial system, a system in which AI increasingly plays, and will continue to play, a pivotal role. But will this lead to a situation where autonomous IT systems effectively take over the governance of our reality, including the financial one? A reality of Huxley's World State, structured to ensure that 'when the individual feels, the community reels' (Huxley, 1946, p. 110)?

While this dystopian vision of society is terrifying, it is not entirely unrealistic. It prompts us to ask questions about possible alternatives, such as, for instance, a world in which humans can control the extent to which technology interferes in their daily lives (Stacewicz, 2023). This would be a world akin to Huxley's 'Savage Reservation', governed by old, 'natural' rules, rejecting the new order. One must then ask: Is the right not to use digital technologies, and its protection by law or other regulatory means, still possible – or has it already become an anachronism in the digital dogma of modernity? Or is it already becoming an anachronism in the digital dogma of modernity, even more so when the subject of study is the financial market and its legal regulation, the identification of which, it turns out, presents another research problem? Another question that arises in view of the above is whether the technological revolution has led to a situation in which new, self-creating sources of financial market law are hidden in algorithms created by hidden lawmakers who use self-learning algorithms to adjust relevant systems and rules on an ongoing basis, based on changing market conditions.

In view of this, is it true that, as Lawrence Lessig wrote, 'code is law' (1999, p. 3)? The search for an answer to this question is the central theme of this article, contained in this issue of *Bialystok Legal Studies* devoted to the non-use of digital technologies and the protection of such non-use by law as well as by other means of regulation. As editor Elżbieta Kużelewska rightly observes: 'As the contemporary ubiquity of new technologies leaves little if no choice for individuals whether to use them, our interest in legal and other regulatory means to protect their non-use merits both academic and professional attention' (Kużelewska, 2025).

One of the key areas requiring attention in this regard is the financial market, the rules and operational architecture of which have undergone revolutionary changes in recent years. This is largely due to the widespread adoption of AI by FinTech players, who have successfully challenged traditional market operators – particularly banks – by offering consumers attractive, affordable financial solutions based on modern technology. However, embedded in the 'genotype' of these products is a coercion to use new technologies. While opting out is theoretically possible, in the long term it results in exclusion from access to the one resource crucial for life which is money (Kowalewska & Musiał, 2025). Money is essential for securing daily needs as well as for personal self-realisation, such as acquiring material goods or achieving a certain level of prosperity.

One could argue at this point that certain areas of financial market participation are becoming spaces where formal individual freedom (including human rights) does not translate into actual freedom of choice. Moreover, even though lawmakers strive to protect this freedom, the rules of the virtual reality system cause individuals to remain largely unaware of the mechanisms (algorithms) that track and then analyse their behaviour, and in certain situations influence their choices (Szoszkiewicz & Świergiel, 2018).

Naturally, no one is forced to use particular technological solutions. However, the modalities described by Lessig (law, markets, social norms or code) effectively eliminate the option of not using them. Who, then, is the true creator of our reality: the lawmaker or the code (algorithm)? Can this brave new world of modern financial markets be controlled in such a way that consumers have a genuine right of non-use, and will it be a right to choose an alternative, to enjoy transparency of operations and to exercise the choice of a non-algorithmic service, for example? And will such regulation, if adopted, be effective and efficient?

Even without prejudging the answers to these questions, it is already apparent at this point that it would be hard to imagine a contemporary financial market functioning without access to technology. This is also due to the actions of lawmakers (e.g. the EU), who, while trying to regulate this reality, in practice confirm the thesis of the actual absence of the possibility of guaranteeing a formal right to not use technology. As a result, current EU financial market regulations structurally exclude individuals who wish to function outside the digital infrastructure.

There are at least a few examples of this, and they include the fundamental EU financial market regulations such as the AI Act (2024), DORA (2022), MiCA (2023), PSD 2 (2015) and FIDA (2023). These legislative acts are too specialised and extensive to analyse in detail within the scope of this article, although selected examples will be used to support the main arguments formulated here. These include the assertions that 'digital coercion' exists in the EU financial market today and that the role of AI in creating and enforcing law is growing. This law may increasingly be a technical implementation of an algorithm. But who will write this algorithm: a human being or AI?

1. The financial market in the face of a new regulatory paradigm in the age of FinTech

For decades, financial markets have been based on the principle of stability and predictability. The traditional structures and divisions of the financial markets, the roles ascribed to them and, last but not least, the actors operating within them, banks in particular (commonly perceived as institutions of public trust), have remained constant. But 2008 brought the financial crisis that has been permanently etched into the pages of history as exceptional, not least because of its global nature and above all because of the underlying causes that led to it. Among these was the widespread use of financial derivatives as an investment strategy designed to generate additional profits, especially for banks (Jurkowska-Zeidler, 2008, p. 72). These profits were obtained through risk-trading mechanisms and the use for this purpose of funds entrusted to the financial sector by trusting clients. The outcome of this experiment is well known; one of its effects was the loss of that public trust and the consequent search for alternatives (Jurkowska-Zeidler, 2011). Although the conditions for the provision of new alternatives had been developing for years, this was precisely the moment for them to materialise in the form of the growth of the FinTech sector, supported by the dynamic development of AI.

Drawing on the ideas of Zygmunt Bauman (2006), one could argue that after 2008 the world witnessed the true face of 'liquid modernity', in which social structures, relationships, or values and identities are no longer stable or unchangeable, and a sense of security is eroding. Volatility and unpredictability are also features that characterise modern technology; it is evolving at a tremendous pace and in a direction that is nowadays difficult to foresee (Armour et al., 2016). This is an even greater challenge for lawmakers today, who are guided by the essence of the law and seek to frame this new reality within a legal framework, given the nature of modern technology, especially AI, and its ability to adapt and self-learn. But is this really possible? Or should lawmakers today not aim at fully controlling and shaping reality with the aid of traditional sources of law, as well as with the use of soft forms of regulation? Such soft law approaches are already being successfully used in the European Union's fi-

nancial market regulation, one example being the Binding Technical Standards (Fedorowicz, 2021b).

Another challenge for modern legislatures in this context is the speed of change and the process of economisation of the law (Nieborak, 2016, pp. 75–94). Just as money has evolved from gold coins to virtual cryptocurrencies, AI will also evolve in ways that will affect our lives in a manner that we cannot fully foresee today. Yet the evolution of money spanned centuries, and the development of AI is measured in years. It can certainly be argued that it began as early as the 1950s with the publication of Alan Turing's essay 'Computing machinery and intelligence', but it was only in 2012 that the introduction of the AlexNet model demonstrated the power and potential of the new technologies (Krizhevsky et al., 2017). Around the same time, start-ups that today are icons of the FinTech sector, such as PayPal, Revolut and Square, began operating. Without their pioneering efforts, further progress in the areas of cryptocurrencies, neobanks like Monzo, InsureTech like Lemonade, or more recently RegTech (Nowakowski, 2020, pp. 13–56) would likely not have been possible. All of these innovations fall under the FinTech category. They are also a perfect example of the progressive process of financialisation, i.e. the penetration of the financial sphere into the real world and its impact on everyday life, through technological innovations (including AI) whose rules of operation are often only understood by a narrow group of specialists (so-called rocket scientists).

Among other things legislatures and supervisors are concerned about the significance of this area of the financial market for the socio-political situation, particularly with regard to protecting the interests of weaker actors (financial market consumers). Having previously fallen victim to the unethical actions of financial market players so far, in the new world they may now be subjected to forces created by a virtual reality based on algorithms used to analyse data and automate processes, as well as to assess their creditworthiness or examine their purchasing habits (Rutkowska-Tomaszewska, 2020). Consequently, in order to obtain a loan, authenticate personal data or confirm a transfer order, it becomes necessary to use digital technologies. This may be termed 'digital coercion', i.e. a situation in which the consumer is compelled to use digital solutions, even unwillingly, which clearly contradicts the idea of the non-use of digital services (Rutkowska-Tomaszewska & Gałązka, 2024). As a result, new technologies, especially those based on AI, are beginning to shape social norms significantly. These norms, alongside law, constitute a fundamental instrument for creating the reality around us.

The confrontation of these two entities, namely AI and the law, triggers a series of questions and doubts, the analysis of which, in my view, requires going back to the sources, i.e. answering the question about the essence of law. Relevant in this respect are the questions posed by Marek Smolak: How does law connect with the world? Is the legal system autonomous from its surrounding reality? Should it be understood merely instrumentally, as a means of achieving important non-legal objectives, including so-

cial, political and economic ones? (Smolak, 2001). However, given the complexity and speed of change in the world around us, as well as the impact on our daily lives, one has to agree with Włodzimierz Gromski's (2007, p. 51) thesis that it is also necessary to look at the law in its real aspect, as a factor shaping the attitudes and behaviours of members of society in accordance with models established or recognised by the state (the legislature). Law as a social phenomenon, therefore combining both the real and the formal aspects, is desirable, as it allows a holistic view of the reality around us. This becomes particularly relevant today, in the age of modern technology, when humanity's challenge is to find the right legal framework to ensure technological development on the one hand and human control over it on the other. This is particularly true of AI, the progress of which will surely only continue to move towards previously unknown forms (such as neural networks), transforming all aspects of our daily lives and work, as well as the functioning of the financial market, the essence of which lies primarily in the role it plays in the creation of what has always been the most important commodity – money. Money is the building block of capital, without which it would be difficult to imagine the functioning of the world and its development.

The birthplace of money is the financial market, where the revolution mentioned earlier, of which AI is one of the protagonists, is taking place. The sources of this revolution should be sought in the change in the approach of lawmakers, including EU legislatures, and their attempts to regulate this segment of the market. This new approach manifests itself in disintermediation and the growing role of new types of financial intermediaries,, among other things, for which legislatures alone are opening the door. One example is the EU regulation of the payment services market; crucial in this respect is the Payment Services Directive 2 (Zalcewicz, 2016), which in the name of increasing market competitiveness allowed so-called Third Party Providers (TPPs) access to the market, seen as an example of the open banking concept (Masłowski, 2024, pp. 20–50). Using cutting-edge technological solutions, TPPs often sense upcoming trends in advance and offer a range of innovative instruments that are often faster and easier to operate. This has obviously contributed to their appeal to customers, even though consumers are not always aware of how these mechanisms work. Depending on the type of TPP in question, i.e. an Account Information Service Provider or a Payment Initiation Service Provider, and with the consumer's consent, opportunities then arise for the provider of a given service to access valuable data, such as the user's account information (transaction history, balance) or personal finance management behaviour, or the ability of the provider to initiate certain transactions directly from the user's bank account, which always require the user's authorisation (Szpringer & Szpringer, 2014).

As can be seen, although the specific role of the human being is taken into account in these processes, the secondary nature of the situation, related to the process of collecting and processing huge amounts of data – Big Data – is concealed (Szoszkiewicz, 2021, pp. 33–46). Properly processed, structured and analysed in a spe-

cific context, these data constitute an excellent source of information, which, as Jean Baudrillard has rightly observed, is a form of control (Ziętek, 2013). Whoever has access to data has power over information and how it is used (Kusak, 2022). In the case of the data collected and processed in the financial markets, this power is immense and must be controlled. And yet as the nature of AI evolves towards more rapid self-learning and AI adaptation, are we not going to be faced with a situation where any attempt to regulate this entity becomes merely an illusion of control? Exercising the right not to use digital technology may constitute a guarantee of individual freedom from digital coercion.

However, one must also be aware of the other side of this right, related to the potential exclusion and social marginalisation of people who refuse to accept algorithmic interference in their lives. Is it therefore possible to design an optimal system based on the values that are accepted and upheld in a given society? The debate on regulating AI is essentially a debate about values, not legal rules, and the ultimate shape of legal regulation depends on which values the lawmakers choose to prioritise (Jędrzejczak, 2024). But does the choice of values allow a situation where people are coerced to use the internet to exercise their rights or fulfil their duties (Kloza et al., 2025, p. 1)? What happens when the algorithm code becomes the actual, albeit hidden, legislation? The conditions currently created by the 'traditional' EU legislation to regulate the financial market actually aimed at supporting the development of the digital sector, and may soon, in my view, necessitate a redefinition of the paradigm of financial market regulation. The existing assumptions, theories, methods and values behind it either will be blurred or will require redefinition in the face of the emergence of a 'new' legislature and the acceptance of a new paradigm, namely that code is law, while the rules enshrined in this code will become a real regulatory force, a fourth modality of regulation, shaping entire societies whose spheres of activity will also be determined by it (Lessig, 1999, pp. 85–99). And all this in the age of a culture of immediacy and risk.

2. Is code law? Do new self-creating sources of financial market law already exist?

The answer to the question of whether code is law should begin with a brief description of the financial market, undoubtedly one of the most important spheres in which societies exist and function today (Bybee, 2016, pp. 21–23). The phenomenon of financialisation, whereby the financial sphere penetrates the real sphere and thus everyday life, aptly captures its importance (Engelen, 2008). To define financialisation we only need to reflect on our daily activities. The financial market permeates our lives in a number of ways: when we withdraw cash from an ATM, pay for purchases, buy insurance, go on holiday or take out a loan to finance the purchase of a house. These ac-

tivities are accompanied by a world that exists in parallel but is practically unknown to those who use services such as clearing and settling payments, credit and risk assessments, scoring or new financial instruments that are frequently based on the principle of freedom of contract between the parties (over-the-counter instruments). All of this poses a real challenge to market regulators, and the relevant processes are supported by modern technologies developed by sectors such as FinTech and significantly influence consumer behaviour, particularly in terms of capital management and interaction with financial institutions (Nowakowski, 2023, pp. 161–169). Mobile applications, the use of AI and the introduction of virtual trading platforms result on the one hand in growing automation that allows business transactions to be conducted from anywhere across the globe, but on the other hand they bring about digital coercion. This is naturally followed by a re-evaluation of traditional social norms related to privacy and transparency. Indeed, one might get the impression that consumers are willing to sacrifice their privacy, hitherto considered to be an absolute value, for convenience, speed and personalisation of services. The value of privacy is protected by the Universal Declaration of Human Rights, Article 12, which states that 'no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks' (United Nations, 1948). Does this new reality of the way financial markets operate pose a threat to this right? Can algorithms arbitrarily violate it? These questions must be asked by their creators, who, we assume, are always humans, who construct solutions based on a controlled version of AI, otherwise known as narrow AI (Footer, 2020).

While artificial general intelligence, considered to be the highest potential level of AI development, is currently only hypothetical, one might wonder whether it may become another 'black swan', a species that we are breeding which will eventually outperform us and which will, at some point, begin to compete with humans in terms of general reasoning, learning, problem-solving and the use of consciousness (Chłopecki, 2018, pp. 5–6). It might, for example, aim to control the financial system of which the financial market and its various components are a part. The financial market must be viewed in the broader context of the economic system, which is in turn part of the social system. While this may seem an obvious point, it is nevertheless of great importance and should serve as a guideline for lawmakers and those who apply their legislation. This interdependence means that any turbulence in the financial system will have specific consequences for the economy and consequently for society.

The EU legislature seems to understand this interdependence, as it successively includes new spheres of financial market operations within digital finance in its legal framework, simultaneously examining potentially necessary measures to be undertaken in areas such as crypto-assets, cyber-resilience, financial data access and the digital euro. The definition of 'digital finance' that may be found on one of the websites of the European Commission dedicated to this issue reads that it is 'the term

used to describe the impact of new technologies on the financial services industry, which includes a variety of products, applications, processes and business models that have transformed the traditional way of providing banking and financial services'. We read further that:

> while technological innovation in finance is not new, investment in new technologies has substantially increased in recent years and the pace of innovation is exponential. We now interact with our bank using mobile technology. We make payments, transfer money and make investments using a variety of new tools that were not there a few years ago. Artificial intelligence, social networks, machine learning, mobile applications, distributed ledger technology, cloud computing and big data analytics have given rise to new services and business models by established financial institutions and new market entrants. All these technologies can benefit both consumers and companies by enabling greater access to financial services, offering wider choice and increasing efficiency of operations. They can also contribute to bringing down national barriers and spurring competition in areas such as: online banking, online payment and transfer services, peer-to-peer lending, personal investment advice and services. The financial services industry has been influenced by innovative technology, which can benefit both consumers and companies by giving a greater access to financial services, offering wider choice and increasing efficiency of operations. Numerous opportunities involve also risks and challenges, which require monitoring and regulation. Therefore, the Commission has put further many initiatives to embrace the innovations, preserve market stability and integrity, and protect financial investors as well as consumers (European Commission, *Overview of digital finance*).

Aware of the changes taking place and the growing importance of AI in the financial market, on 24 June 2024 the European Union launched a targeted consultation on artificial intelligence in the financial sector. For that purpose, the Commission drew up a consultation document entitled 'Artificial intelligence in the financial sector' (European Commission, 2024), which contains numerous questions broken down by specific sectors of the financial market. It also highlighted that the targeted consultation will answer the questions posed in the document, divided into three parts: one with general questions on the development of AI, one consisting of questions related to specific use cases in finance and one on the AI Act as related to the financial sector. At the same time it was agreed that in the description of the purpose of the targeted consultation, the concept of AI corresponds to the definition of an AI system established in Article 3(1) of the AI Act 2024 and covers 'any machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it

receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments'.

The consultation period is now closed, and a summary, expected in the near future, will provide a valuable insight into the perception of AI by market participants in a broad sense, who have already been covered by regulations directly or indirectly applied pursuant to the AI Act. This Act, an extremely detailed and extensive regulation, introduces four types of AI and identifies them according to the degree of risk associated with their application:

– minimal-risk systems, which pose no significant security or human rights risks (e.g. spam filters),
– limited-risk systems, which affect the user, but create no serious risks (e.g. recommendations on e-commerce platforms),
– high-risk systems, the AI systems that pose a risk of harm to health and safety or an adverse impact on fundamental rights, which includes, among other things, credit risk assessments,
– unacceptable-risk systems, which are banned in the EU (with some exceptions related to the threat of terrorism) and which are regarded as contrary to the EU's values, infringing fundamental rights. Among them are the ability to recognise emotions in a specific context and the social scoring system already in use in some countries to assess citizens, based on their behaviour, actions or characteristics.

The first two types of AI can be implemented without any additional compliance requirements. In contrast, high-risk systems must comply with certain requirements, including a compliance assessment prior to implementation. AI systems that pose an unacceptable risk or that constitute a threat to EU fundamental rights have been prohibited, with some exceptions. As explained in Annex III to the AI Act, using AI in the financial market will typically involve high-risk systems, giving rise to certain obligations for financial institutions. They will have to register these systems in a special EU register, making them subject to relevant testing, compliance assessments and audits. AI decisions must also be subject to human oversight (the 'human-in-the-loop' rule). Proper management of risks and the quality of data is also necessary to limit discrimination and bias among users of financial services.

Table 1. Summary of AI Act compliance requirements (for high-risk systems).

Requirement	Description	AI Act reference
Risk classification	Must determine if the system falls into unacceptable, high-risk, etc.	Arts. 6–9, Annex III
Conformity assessment	Technical and documentation checks for high-risk AI	Arts. 19–24

Human oversight	Human-in-the-loop must monitor, override or validate AI decisions	Art. 14
Data governance	Training data must be relevant, representative, free of bias	Art. 10
Transparency obligations	Users must be informed of AI use, especially if interacting with it	Art. 50
Post-market monitoring	AI providers must track performance, report issues	Art. 72

While the AI Act acknowledges the importance of the financial market as an integral part of the EU's internal market, as outlined in Article 26 of the Treaty on the Functioning of the European Union (European Union, 2012), it should be considered supplementary to the current EU financial market regulations. This is particularly relevant for market segments that use AI. Financial institutions will be required to fulfil obligations arising from the use of AI in their activities, while also complying with sector-specific requirements. While this will arguably give rise to extra costs, the overriding objective is to ensure safety and trust among clients using specific solutions. This also implies that AI will not impact the lives of those not using the services; in other words, it will not affect those who do not need to use them, nor will it prevent them from exercising their right to opt out of digital technology. While the latter is certainly possible, the significance of these services in daily life may well coerce consumers into using digital technology. Examples of EU legislation where the paths of AI and the financial market converge include the following acts, which cover the FinTech sector:

- Digital Operational Resilience Act (DORA) (European Parliament and European Council, 2022) on cybersecurity and the operational resilience of financial institutions (Zalcewicz, 2023),
- Payment Services Directive (PSD2), standardising electronic payments, security and open banking (Dybiński, 2025, pp. xiii–xiv),
- Markets in Crypto-Assets Regulation (MiCA) (European Parliament and European Council, May 2023) a regulation of the crypto-asset market (Fedorowicz, 2021a; Mariański, 2024),
- Anti-Money Laundering / Countering the Financing of Terrorism (AML/CFT) (European Parliament and European Council, May 2024), a system of regulations and obligations designed to prevent money laundering and terrorist financing,
- selected European Banking Authority (EBA) guidelines, formulating requirements concerning, for example, risk management, transparency and use of data. Examples of these include the EBA guidelines on loan origination and monitoring (EBA, 2020), on internal governance (EBA, 2021), and on ICT and security risk management (EBA, 2025).

One cannot ignore two other important EU initiatives currently being worked on by European Union institutions, which are the:

- Financial Data Access Regulation (FIDA) (European Parliament and European Council, 2023c), intended, among other things, to enforce transparency on algorithms that use financial data,
- Payment Services Regulation (PSR) (European Parliament and European Council, 2023b), intended, together with the subsequent third generation of PSD2 commonly referred to as PSD3, to form a tandem to improve payment security, promote open access to financial services and strengthen consumer protection.

The above regulations confirm the thesis of a rapidly growing EU financial market that will undoubtedly continue to play an increasingly important role in everyday life. Furthermore, the scope will certainly encompass FinTech institutions offering AI-based instruments. Currently, it is difficult to evaluate the effectiveness of the measures implemented to safeguard individuals' interests, and further research in this area is required.

Such studies should also consider the autonomy of AI-powered systems and the impact of AI-driven decisions on consumers of financial services. This brings us back to the question raised at the beginning of the article: Who is actually responsible for this decision? Will it be humans or code, as described by Lawrence Lessig? His theory of the four modalities is highly relevant to deliberations on the scope of AI application in the financial market, particularly with regard to consumers' right to opt out of digital technology. In reality, however, consumers are in a state of digital compulsion as a result of these modalities. Lessig's theory identifies the following four modalities (or models) that regulate human behaviour:

- Law: the formal rules backed by state coercion (laws, regulations, fines, penalties),
- Norms: social norms that are culturally acceptable or expected,
- Market: identified with economic forces: pricing, incentives, competition,
- Code (Architecture): the physical or logical structure of the environment (especially software code).

As Lessig (1999, pp. 87–89) explains, each of these modalities constrains behaviour in different ways. They are not merely models of law creation in the traditional legislative sense; rather, they are four regulatory forces that shape human behaviour. This is especially relevant in the digital environment (Dolniak et al., 2024); they interact and complement each other. This is evident in financial market regulation, where traditional legal rules must consider market realities and societal habits and customs. There is also room for a fourth modality: code which seems to be the centre of attention, embedded in Lessig's statement that:

> Code is law. This code poses the greatest threat to, and offers the greatest promise for, liberal and libertarian ideals. We can design cyberspace to protect values that we believe are fundamental, or we can design cyberspace to allow those values to disappear. There is no middle ground. Every choice involves some kind of construction. Code is never found; it is only ever created, and only ever created by us. (Lessig, 1999, p. 6)

As has already been demonstrated, code certainly shapes the space in which we function, influencing, if not outright creating, our choices through the use of specific techniques. One example is Thaler's and Sunstein's concept of 'nudging', which uses elements of behavioural psychology and choice architecture to encourage people to make decisions in a certain way (e.g. through advertising), without constraining them (Thaler & Sunstein, 2009, pp. 134–146). This raises questions about how this code is used and the limits of its autonomy and control. Although it is admittedly designed by humans, might its design, perhaps reinforced by its self-development, result in it becoming a self-enforcing law and a new incarnation of the legislator-regulator? The effectiveness with which the aforementioned EU legislation is implemented and enforced is crucial. Naturally, this will require highly specialised knowledge to understand and accept the solutions before they are applied, and to supervise their subsequent use (Fedorowicz & Zalcewicz, 2024). At the same time, we must be aware of Decentralised Finance (DeFi), a system of financial services based on blockchain technology that operates without traditional intermediaries such as banks, stock exchanges and supervisory institutions (Bilski, 2024). DeFi relies on smart contracts, sets of self-executing rules based on blockchain technology. As social norms evolve in response to modern technological advances, the openness, automation, decentralisation, immediacy and interoperability of the DeFi system are likely to strengthen its position as a key element of the global financial market (Roukny, 2022, pp. 14–16).

Looking ahead, one might conclude that regardless of the extent of control over the financial market, the most powerful tool for controlling our reality will be the rules governing it, whether created by the EU or by DeFi code. In combination with AI, these rules will effectively eliminate the possibility of opting out of digital technology. This will be the case even if the law does not formally impose an obligation to use these technologies. Individuals will be faced with the choice of either 'taking advantage' of technological coercion or facing financial exclusion. This will be facilitated by Lessig's four modalities combined: law (which encourages technological development), the market (which offers no alternative), social norms (which enforce compliance with the majority's rules) and code (which links all the modalities and is the key tool in creating our contemporary brave new world).

Conclusions

Looking to the future, it is clear that the 21st century will be remembered as a pivotal era in human history. This will largely be due to the technological revolution and the creation of AI. AI would not have been possible without the power of the human mind, whose creativity and abilities will lead to further inventions, which, if used wisely, should facilitate further progress. Hopefully, this will also be the case with AI, a tool with enormous potential that nevertheless raises many questions about its future evolution. Just as humans were present at the birth of AI, they should assist in its development, providing guidance and imposing limitations where necessary. After all, humans are curious beings who ask questions about life and the times in which they live; they are both aware and doubtful. AI, on the other hand, is merely a tool – albeit a powerful one – lacking inner awareness and the ability to reflect on existential questions.

Therefore discussions on the development of AI should emphasise the importance of human involvement in shaping the relationship between technology and traditional values, as outlined by Huxley with his Savage Reservation. It is these relationships that have enabled humanity to develop technology and reach the present day. Is the right to live offline as real as the right to freedom of speech? Or has it become more of a fiction? Do we still have the right not to use digital technologies, and is this right protected by law and other regulatory measures? Or has it already become an anachronism in the digital dogma of modernity? The answers to the last two questions are not optimistic for those who see freedom from digitalisation as a fundamental human right (Jóźwicki & Szoszkiewicz, 2025). The analysis conducted in this study concludes that while certain guarantees remain in place in theory, they are gradually being marginalised in practice, and in some areas are becoming illusory. The possibility of opting out of digitisation processes is increasingly purely declarative, and economic, regulatory and social pressures mean that the right to digital opt-out ceases to function in reality. After all, it seems that financial markets and the regulations that govern them enforce the use of digital tools. Rather than neutralising digital compulsion, many EU regulations actually strengthen it.

However, this does not mean that we should stop debating the need for technical alternatives that would allow consumers to retain the option of non-algorithmic decision-making on important matters in their lives (i.e. decisions made by a human being, not a code). We should also consider introducing a right to digital opt-out and including an impact assessment mechanism in the lawmaking process to analyse the use of digital technologies. To many reading these words, this proposal probably seems like science fiction. Perhaps. However, we must also remember that the law should be fair; at its core, it should be based on an axiological system. Although this view may be considered revolutionary in modern times, we should remember that the purpose of law is to protect and develop humanity, not to destroy or subjugate it.

REFERENCES

Armour, J. (2016). The financial system. In J. Armour, D. Awrey, P. Davies, L. Enriques, H. J. Gordon, C. Mayer, & J. Payne (Eds.), *Principles of financial regulation* (pp. 22–50). Oxford University Press.

Bauman, Z. (2006). *Płynna nowoczesność*. Wydawnictwo Literackie.

Bilski, A. (2024). Blockchain i smart contracts w sektorze bankowym. In K. Szpyt (Ed.), *FinTech. Nowe technologie w sektorze bankowym* (pp. 35–52). C.H. Beck.

Boden, A. M. (2020). *Sztuczna Inteligencja*. Wydawnictwo Uniwersytetu Łódzkiego.

Bybee, J. K. (2016). *How civility works*. Stanford University Press.

Chłopecki, A. (2018). *Sztuczna inteligencja – szkice prawnicze i futurologiczne*. C.H. Beck.

Cyman, D. (2023). Public interest as a determinant of state influence on the financial market in the European Union. *Studia Iuridica*, *98*, pp. 55–56.

Dolniak, P. (2024). Sztuczna inteligencja w wymiarze sprawiedliwości. In P. Dolniak, T. Kuźma, A. Ludwiński, & K. Wasik (Eds.), *AI na styku prawa i cyfryzacji* (pp. 79–107). Wolters Kluwer.

Dybiński, J. (2025). Wstęp. In J. Dybiński (Ed.), *Prawo rynku finansowego. Prawo usług płatniczych. Komentarz* Vol. XB. (pp. xiii–xiv). C.H. Beck.

European Banking Authority. (2020). *EBA guidelines on loan origination and monitoring, EBA/GL/2020/06*. https://www.eba.europa.eu/sites/default/files/document_library/Publications/Guidelines/2020/Guidelines%20on%20loan%20origination%20and%20monitoring/Translations/886690/Final%20Report%20on%20GL%20on%20loan%20origination%20and%20monitoring_COR_PL.pdf

European Banking Authority. (2021). *EBA guidelines on internal governance, EBA/GL/2021/05*.

European Banking Authority. (2025). *EBA guidelines on ICT and security risk management, EBA/GL/2019/04*. (Originally published 2019).

Engelen, E. (2008). The case for financialization. *Competition & Change*, *12*(2), pp. 111–119.

European Commission. (2024, 10 June). *Targeted consultation on artificial intelligence in the financial sector*. https://finance.ec.europa.eu/regulation-and-supervision/consultations-0/targeted-consultation-artificial-intelligence-financial-sector_en

European Commission, *Overview of digital finance*. https://finance.ec.europa.eu/digital-finance/overview-digital-finance_en

European Parliament and European Council. (2015, 25 November). Directive (EU) 2015/2366 on Payment Services in the Internal Market, Amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) no. 1093/2010, and Repealing Directive 2007/64/EC (Text with EEA Relevance) (PSD 2) (O. J. L 337, 23.12.2015).

European Parliament and European Council. (2016, 27 April). Regulation (EU) 2016/679 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA Relevance) (O. J. L 119, 04.05.2016).

European Parliament and European Council. (2022, 14 December). Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector and Amending Regulations (EC) no.

1060/2009, (EU) no. 648/2012, (EU) no. 600/2014 (EU), no. 909/2014 and (EU) 2016/1011 (DORA) (Text with EEA Relevance), PE/41/2022/INIT (O. J. L 333, 27.12.2022).

European Parliament and European Council. (2023a). *Proposal for a Directive of the European Parliament and of the Council on Payment Services and Electronic Money Services in the Internal Market Amending Directive 98/26/EC and Repealing Directives 2015/2366/EU and 2009/110/EC*, COM/2023/366 final (PSD 3).

European Parliament and European Council. (2023b). *Proposal for a Regulation of the European Parliament and of the Council on Payment Services in the Internal Market and Amending Regulation (EU) no. 1093/2010*, COM/2023/367 (PSR).

European Parliament and European Council. (2023c). *Proposal for a Regulation of the European Parliament and of the Council on a Framework for Financial Data Access and Amending Regulations (EU) no. 1093/2010, (EU) no. 1094/2010, (EU) no. 1095/2010 and (EU) 2022/2554* (FIDA), COM/2023/360 final.

European Parliament and European Council. (2023, 31 May). Regulation (EU) 2023/1114 on Markets in Crypto-Assets, and Amending Regulations (EU) no. 1093/2010 and (EU) no. 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (Text with EEA Relevance) (MiCA) PE/54/2022/REV/1 (O. J. L 150, 09.06.2023.

European Parliament and European Council. (2024, 31 May). Regulation (EU) 2024/1624 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing (AML/CFT) (Text with EEA Relevance), PE/36/2024/REV/1 (O. J. L 2024/1624).

European Parliament and European Council. (2024, 13 June). Regulation (EU) 2024/1689 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 (Artificial Intelligence Act) (Text with EEA Relevance), PE/24/2024/REV/1 (O. J. L 2024/1689).

European Union. (2012). *Consolidated version of the treaty on the functioning of the European Union* (O. J. C 326, 26.10.2012).

Fedorowicz, M. (2021a). Nadzór nad rynkiem kryptoaktywów w świetle projektu rozporządzenia MiCA – najnowsze wyzwania i tendencje regulacyjne cyfrowej stabilności i odpowiedzialności na rynku finansowym UE. In K. Królik-Kołtunik & I. Skibińska-Fabrowska (Eds.), *Inwestycje alternatywne – nowe spojrzenie*, (pp. 75–88). CeDeWu.

Fedorowicz, M. (2021b). Znaczenie soft law EBA dla określania normatywnego standardu ochrony konsumenta na rynku finansowym. *Internetowy Kwartalnik Antymonopolowy i Regulacyjny*, *10*, Article 7, pp. 21–34.

Fedorowicz, M., & Zalcewicz, A. (2024). Challenges posed to the EU financial market by the implementation of the concept of sustainable financing. *Bialystok Legal Studies*, *29*, pp. 54–56.

Footer, R. M. (2020). The EU's engagement with business on human rights. In J. Wouters, M. Nowak, A. L. Chané, & N. Hachez (Eds.), *The European Union and human rights: Law and policy* (pp. 312–344). Oxford University Press.

Gromski, W. (2007). Law and economics jako teoria polityki prawa. In J. Stelmach & M. Soniewicka (Eds.), *Analiza ekonomiczna w zastosowaniach prawniczych* (p. 51). Wolters Kluwer Polska.

Huxley, A. (1946). *Brave new world*. Harper Crest.

Jędrzejczak, M. (2024). Protection of personal data processed in artificial intelligence systems. *Gdańskie Studia Prawnicze*, *64*, Article 3, pp. 88–89.

Jóźwicki, W. W., & Szoszkiewicz, Ł. (2025). Non-use of the internet as human rights enabler? The curious cases of the right to privacy and the right to health. In D. Kloza, E. Kużelewska, E. Lievens, & V. Veerdoodt (Eds.), *The right not to use the internet: Concept, contexts, consequences* (pp. 106–120). RoutledgePoczątek formularza.

Jurkowska-Zeidler, A. (2008). *Bezpieczeństwo rynku finansowego w świetle prawa Unii Europejskiej*. Wolters Kluwer Polska.

Jurkowska-Zeidler, A. (2011). Nowa globalna architektura finansowa. *Gdańskie Studia Prawnicze*, *25*, pp. 535–547.

Kloza, D., Kużelewska, E., Lievens, E., & Veerdoodt, V. (Eds.). (2025.) *The right not to use the internet: Concept, contexts, consequences*. RoutledgePoczątek formularza.

Kowalewska, E., & Musiał, M. (2025). Accessibility of mobile banking apps in Poland: A legal analysis of recent developments. *Przegląd Ustawodawstwa Gospodarczego*, *3,* pp. 27–35.

Krizhevsky, A., Sutskever, I., & Hinton, E. G. (2017). ImageNet classification with deep convolutional neural networks. *Communications of the ACM*, *60*(6), pp. 84–90.

Kusak, M. (2022). Quality of data sets that feed AI and big data applications for law enforcement. *ERA Forum*, *23*, pp. 209–219.

Kużelewska, E. (2025). *Non-use of digital technologies and regulation*. https://bsp.uwb.edu.pl/libraryFiles/downloadPublic/8

Lessig, L. (1999). *Code and other laws of cyberspace*. Basic Books.

Mariański, M. (2024). Reflections on the possible application of Rome I Regulation to obligations related to crypto-assets. *Ruch Prawniczy, Ekonomiczny i Socjologiczny*, pp. 24–28.

Masłowski, M. (2024). *Otwarta bankowość*. C.H. Beck.

Nieborak, T. (2016). *Creation and enforcement of financial market law in the light of the economisation of law*. Wydawnictwo Naukowe UAM.

Nowakowski, M. (2020). *Fintech: Technologia, finanse, regulacje. Praktyczny przewodnik dla sektora innowacji finansowych*. Wolters Kluwer.

Nowakowski, M. (2023). *Sztuczna Inteligencja: Praktyczny przewodnik dla sektora innowacji finansowych*. Wolters Kluwer.

Roukny, T. (2022). *Decentralized finance: Information frictions and public policies. Approaching the regulation and supervision of decentralized finance*. Publications Office of the European Union.

Rutkowska-Tomaszewska, E. (2020). Prawo ochrony konsumenta usług finansowych w świetle założenia racjonalnego ustawodawcy – kilka wybranych uwag. *Przegląd Prawa i Administracji*, *120*, pp. 481–498.

Rutkowska-Tomaszewska, E., & Gałązka, P. (2024). The role of European supervisory authorities in consumer protection standard setting on the financial services market: Based on the example of the European Banking Authority. *Studies in European Affairs*, *28*(2), pp. 223–232.

Smolak, M. (2001). Jak prawo łączy się ze światem? Uwagi na marginesie książki W. Gromskiego, Autonomia i instrumentalny charakter prawa. *Ruch Prawniczy, Ekonomiczny i Socjologiczny*, *3*, pp. 191–198.

Stacewicz, P. (2023). O światopoglądowym oddziaływaniu informatyki w świecie współczesnym. In A. Zalcewicz & R. Kędziora (Eds.), *Nowe technologie. Wartości, prawa, zasady* (pp. 305–314). Politechnika Warszawska.

Szoszkiewicz, Ł. (2021). *Dostępność danych w czasach sztucznej inteligencji a prawa człowieka w dziedzinie nauki*. Wydawnictwo INP PAN.

Szoszkiewicz, Ł., & Świergiel, R. (2018). Financial institutions and the protection of individuals' autonomy: A human rights perspective. *Roczniki Nauk Prawnych*, *28*(4), pp. 125–136.

Szpringer, W., & Szpringer, M. (2014). Nowe zjawiska w regulacji rynku usług płatniczych (wybrane problemy na tle projektu noweli do dyrektywy PSD). *'e-mentor'*, *56*(4), pp. 73–83.

Thaler, R. H., & Sunstein, C. R. (2009). *Nudge: Improving decisions about health, wealth and happiness*. Penguin Books.

United Nations. (1948). *Universal declaration of human rights*. https://www.un.org/sites/un2.un.org/files/2021/03/udhr.pdf

Zalcewicz, A. (2016). Teoretycznoprawne wprowadzenie w problematykę rynku usług płatniczych – kilka uwag tytułem wstępu. In A. Zalcewicz & B. Bajor (Eds.), *Ustawa o usługach płatniczych. Komentarz* (pp. 19–28). Wolters Kluwer.

Zalcewicz, A. (2023). New technologies in the control of public finances and building public confidence in the state. *Bialystok Legal Studies*, *28*(2), pp. 23–25.

Ziętek, A. (2013). *Jean Baudrillard wobec współczesności: polityka, media, społeczeństwo*. Universitas.

Bialystok Legal Studies
Białostockie Studia Prawnicze
2025 vol. 30 no. 4

sciendo

DOI: 10.15290/bsp.2025.30.04.09

Received: 11.06.2025
Accepted: 23.09.2025

Dmytro V. Gryn
Yaroslav Mudryi National Law University, Ukraine
dmytro_hryn@edu-knu.com

Liubov V. Kotova
Volodymyr Dahl East Ukrainian National University, Ukraine
kotova@snu.edu.ua

Larysa Y. Velychko
V. N. Karazin Kharkiv National University, Ukraine
velychkolara71@gmail.com

Olena H. Sereda
Yaroslav Mudryi National Law University, Ukraine
osereda3@gmail.com

Vladyslav S. Tkachenko
Yaroslav Mudryi National Law University, Ukraine
ipz3311@protonmail.com

The Development and Implementation of the Right to Disconnect in Different Jurisdictions

Abstract: This article examines the development and implementation of the right to disconnect in selected jurisdictions, with particular attention to its legal foundations and its implications for employee well-being, productivity, and work–life balance. The central hypothesis is that explicit statutory regulation, supported by organizational practice, provides stronger protections for workers than reliance on general working-time provisions alone. The study applies doctrinal, comparative, historical, and socio-legal methods, and incorporates insights from a small-scale survey of remote workers. The analysis shows that while France and Italy have introduced comprehensive legislative frameworks, other countries, such as Romania and Japan, continue to rely primarily on working-time limits, and Canada is moving towards a mixed federal–provincial model. The article concludes that sustainable implementation of the right to disconnect requires not only statutory safeguards but also collective bargaining, cultural change, and sector-specific adaptations.

Keywords: right to disconnect, labour law, remote work, work–life balance, employee rights, labour and social rights

Introduction

The COVID-19 pandemic led to a massive shift to remote work. Employees faced challenges with their work environment, such as sharing space with family members and technical issues like lack of equipment or the internet (Jacques et al., 2023; Jaworska, 2022). At the same time, the pandemic allowed people to adapt and re-evaluate work's role in their lives. Now, many executives expect a return to the office (Gibson et al., 2023), but employees have grown accustomed to flexible conditions that balance work and personal lives. Remote work has become a new standard. However, constant communication outside working hours via phone, email, or messaging intrudes on free time, affecting both public and private sector employees (Jaworska, 2022). As technology advances, the line between work and personal time blurs, often causing overload and burnout. In this context, the right to disconnect – freedom from work calls, emails, and messages outside working hours – is essential for work–life balance (Bokor-Szőcs, 2023; Yaroshenko et al., 2025).

The introduction of this right helps to improve the quality of life of employees and increases their productivity and job satisfaction (State Labour Service of Ukraine, 2021). Research shows that employees who have the ability to completely disconnect from work in their free time demonstrate better performance and company loyalty. In addition, such employees are less prone to stress and professional burnout. Thus globalization, digitalization, and the growth of remote work create new challenges for workers around the world. The right to disconnect is particularly important in today's environment, contributing to a better work–life balance, maintaining employee health, and ensuring stable productivity in complex and unpredictable conditions.

The present study pursues a clearly defined objective: to examine how the right to disconnect is conceptualized and implemented across diverse legal systems, and to assess its implications for employee well-being, productivity, and work–life balance. To guide the analysis, the article is structured around the following research questions: (1) How do different jurisdictions legally define and regulate the right to disconnect? (2) What similarities and divergences can be observed between European Union Member States and non-EU jurisdictions? (3) To what extent does the recognition of the right to disconnect contribute to measurable improvements in health, productivity, and work–life balance? Based on existing scholarship and comparative analysis, the central hypothesis advanced here is that the right to disconnect, when explicitly codified in law and supported by organizational practices, produces more effective outcomes in safeguarding employee health and productivity than when it remains implicit or merely declarative.

For clarity and consistency, this article uses the term 'right to disconnect' to refer to the legal entitlement of employees to refrain from work-related communications, such as emails, phone calls, and instant messages, outside their contractual working hours without negative repercussions. Some scholars and policymakers also use the

expression the 'right to disengage'; however, in this paper, the two terms are treated as synonyms, with the right to disconnect designated as the primary expression. This reflects prevailing usage in European Union documents and comparative legal scholarship (see Bokor-Szőcs, 2023; Varela-Castro et al., 2022). A related but narrower concept, the 'right to chosen connectivity', emphasizes voluntary rather than mandatory disconnection (Pansu, 2018), but this study focuses on the broader statutory recognition of employees' right to be free from compulsory availability.

1. Methods

This study adopts a mixed-method legal research design combining doctrinal, comparative, historical, and socio-legal approaches. The doctrinal method was applied to identify and interpret legislative texts and judicial decisions relevant to the right to disconnect. The comparative method enabled a cross-jurisdictional analysis of selected EU and non-EU countries. The historical method traced the emergence and evolution of the concept from early international labour standards to its present recognition in national legal systems. To complement these approaches, a sociological dimension was incorporated through exploratory surveys of remote workers. These surveys involved 73 participants from different professional sectors, who were asked questions such as 'Do you feel pressured to respond to work communications outside of official working hours?' and 'Would a statutory right to disconnect improve your work–life balance?' The sample, while limited in size, included respondents from public administration, IT services, and education, providing preliminary insights into the lived experience of hyper-connectivity and employee attitudes towards potential regulation.

We also used the method of analysis and synthesis, the purpose of which is to break down complex concepts into smaller parts for detailed study (analysis) and to connect these parts to create a bigger picture (synthesis). We used this method to analyse legislative initiatives and practices supporting the right to disconnect in different countries, and based on this, general conclusions and recommendations were synthesized. In addition, the analysis and synthesis method was applied to the study of the positive impact of the right to disconnect on the life, health, and productivity of workers. The historical method involves the study of the development and evolution of phenomena in a temporal context; we used this method to study the development of the concept of the right to disconnect and its evolution in different countries over time.

We also used the comparative method, which involves comparing different phenomena or objects to identify similarities and differences. This method was used to contrast approaches to regulating the right to disconnect in different jurisdictions, identify best practices, and analyse their effectiveness. In addition, we used the sociological method, which involves the study of social processes, behaviour, and in-

teractions in society. Sociological surveys and interviews with remote workers were conducted to determine their attitudes towards the right to disconnect and its impact on their lives and productivity. It also used a combination of research methods to comprehensively examine the development and implementation of the right to disconnect in different jurisdictions, as well as its impact on workers' health, productivity, and work–life balance. This ensured the reliability of the research findings.

The choice of France, Italy, and Romania as examples of EU Member States is due to their different levels of regulatory enshrinement of the right to disconnect. We took into account the initial experience of France, where this right is enshrined at the legislative level. We then considered the intermediate model of Italy and the currently declarative approach of Romania. This comparison allows us to show the diversity of legal instruments within the common European legal space.

Ukraine, Canada, and Japan were selected for the non-European dimension. Ukraine is an associate member of the EU and seeks to implement European labour law standards. This makes it an interesting example of legal harmonization in a state of martial law. Canada demonstrates the approach of a case law system and a federal structure. Here, the right to disconnect is formed at both the federal and the provincial levels. Japan, in turn, represents the Asian legal and cultural model with traditionally high workload indicators. Analysis of its experience makes it possible to assess the effectiveness of preventive measures without the right to disconnect being directly enshrined.

This combination of jurisdictions provides a variety of legal, cultural, and socio-economic contexts, allowing for a comprehensive study of trends in the development and implementation of the right to disconnect on a global scale.

2. Literature review

In order to situate the present research within existing scholarship, the literature review has been moved forwards in the article so that it precedes the legal analysis, in accordance with recommendations for structuring comparative legal research. This ensures that the discussion of legislative frameworks is properly grounded in prior theoretical and empirical contributions. The academic debate on the right to disconnect has focused on definitional clarity and the emergence of related concepts such as the 'right to disengage' or the 'right to chosen connectivity', the psychosocial and health impacts of permanent digital connectivity, and comparative assessments of national experiences, particularly in Europe but increasingly in North America and Asia.

Pansu's (2018) paper explores the French right to disconnect legislation passed in January 2017, which allows employees in companies with more than 50 workers to negotiate disconnection after working hours. Using qualitative methods, including semi-structured interviews and questionnaires, the study finds that French employ-

ees, including managers, have a positive attitude towards this legislation. However, practical implementation faces challenges due to the entrenched work culture. Some employees and managers have begun exercising the right despite limited support from senior management, highlighting the need for a mindset shift. The article also considers the term 'right to chosen connectivity' as a flexible approach to regulating the use of digital tools at work.

Varela-Castro et al. (2022) show that the right to disconnect positively affects competitiveness, productivity, and creativity, emphasizing the need for legal and organizational measures to ensure its implementation and support employee well-being. Dima and Högback (2020) find that this right reduces work stress, improves work–life balance, and benefits physical and mental health. Their study surveyed 73 people to identify the key factors that contribute to the successful implementation of the right to disengage. It turned out that the need for organizations to recognize and understand this right is important to ensure the independence of employees allowing them to better use their free time for social interactions and knowledge development, which in turn increases their competitiveness and productivity. The article also emphasizes that the right to disconnect should be recognized at the legislative level to ensure its effective implementation, helping to create conditions for improving the psychological balance and the quality of life of employees, which will have a positive impact on their productivity and creativity (Dima & Högback, 2020).

The right to disengage is a relatively new legal phenomenon that has not yet been reflected in legislative acts around the world. While there is growing interest in its study, there are still some ambiguities in how it is understood and obstacles to its implementation, although trends around the world point to an improvement in the situation of workers. The introduction of the right to disengage has numerous positive effects for workers, contributing to their physical and mental well-being and increasing overall productivity (Escobar, 2019). One of the main positive effects of the right to disconnect is the reduction of stress (Sonnentag, 2012); constantly being connected to work tasks and communications outside of working hours can lead to a significant increase in employee stress levels (González, 2020). Establishing clear boundaries between work and personal time allows employees to rest and rejuvenate, which helps to reduce stress levels. Reducing stress also reduces the risk of burnout, which is often associated with being constantly connected to work (Varela-Castro et al., 2022). Regularly disconnecting from work tasks contributes to the improvement of employees' mental health; not having to constantly respond to work calls and emails during free time allows employees to rest more effectively, which has a positive impact on their mental health (Thomée et al., 2011). Research shows that a lack of adequate rest can lead to increased levels of anxiety and depression, so providing opportunities to disconnect can help reduce these risks (People Management, 2017).

3. Results

3.1. The historical development of the right to disconnect

The concept of the right to disconnect has gained particular importance in today's digital economy, where technology is constantly changing the nature of work (Becker et al., 2018). However, the history of its emergence and development includes several key stages that are worth considering in more detail. Leisure is free time dedicated to non-work-related activities, not essential domestic or educational tasks but rather recreational and motivating pursuits, and rest is the interruption of work to relax; both are essential for physical and mental health (Varela-Castro et al., 2022). These issues have been of great relevance and have been addressed by the International Labour Organization (ILO) since its foundation at the beginning of the 20th century. In 1948, the importance of these issues was further recognized when Article 24 of the Universal Declaration of Human Rights was adopted, officially acknowledging rest, leisure, and periodic paid vacations as fundamental human rights (United Nations, 1948).

The idea of the right to disconnect began to attract scholarly and policy attention in Europe in the early 2000s, as mobile devices and email accelerated the erosion of boundaries between work and personal life (Hesselberth, 2017; Pansu, 2018). The lack of clear boundaries between work and leisure led to overwork, increased stress, and mental health problems. The concept of the right to disconnect first emerged in France (Dima & Högback, 2020; Pansu, 2018); in 2016, it became the first country to officially incorporate this right into its labour legislation. The El Khomri law, also known as the Labour Law, included provisions requiring companies with more than 50 employees to negotiate with employees on policies regulating the use of digital technology outside working hours (République Française, 2016). This right was introduced in response to the increasing pressure on employees to stay connected to email and other communication tools even after the workday had ended. The lack of boundaries between work and personal life led to burnout, decreased productivity, and mental health issues (Sampaio, 2020).

Other countries began to recognize this problem and implemented their own solutions. For example, in Germany, some companies, such as Volkswagen and BMW, introduced policies limiting access to work emails outside working hours (Bouciqué & Vets, 2023). In Italy, the Agile Work Law (*Legge sul lavoro agile*) was passed in 2017, granting employees the right to negotiate with employers on the use of technology outside working hours (Italian Government Prime Minister's Office, 2017). The right to disconnect legislation mandates that companies with 50 or more employees establish a formal dialogue between employers and employees (through their representatives) which addresses the use of digital tools outside of working hours. Additionally, the right to disconnect must be included in the mandatory annual negotiation process, which focuses on enhancing quality of life at work and promoting gender equality (Hesselberth, 2017).

Thus the history of the right to disconnect is relatively new but rapidly evolving. It reflects a growing need to protect employees from constant work pressure in the digital age, where the boundaries between work and personal time are becoming increasingly blurred. The concept of the right to disconnect has gained traction not only at the national level but also internationally (Lomborg & Ytre-Arne, 2021). Various organizations and governing bodies have recognized the importance of this right and have taken steps to promote its implementation globally. The ILO has also acknowledged the significance of the right to disconnect; it has been promoting decent work conditions and emphasizing the importance of work–life balance as a fundamental aspect of worker welfare. While not yet a formalized part of ILO conventions, the discussion around the right to disconnect aligns with the organization's broader goals of protecting workers' rights and promoting fair labour practices worldwide. The European Union has also contributed to this, as we will discuss in more detail later.

3.2. The right to disconnect in the European Union and individual Member States (with the examples of France, Italy, and Romania)

The EU Labour Force Survey (2022) shows that the overall proportion of people working from home in the EU has almost doubled in the last few years, from 11.1% in 2019 to 20% in 2022 (Schmit, 2024). Although this number slightly decreased in 2023, according to Eurostat, remote work is still important, and the rights of remote workers need to be regulated in detail (Eurostat, 2024; Gnatenko et al., 2020). With this in mind, the European Union is actively engaged in the implementation of the right to disconnect to protect workers in the digital age. This right is aimed at ensuring work–life balance, as well as reducing stress and overwork among employees. The European Union has been at the forefront of advocating for the right to disconnect: in 2021, the European Parliament adopted a resolution urging the European Commission to propose legislation that ensures all workers have the right to disconnect from digital devices outside of working hours without facing adverse consequences. This move aims to standardize the approach across Member States and provide a cohesive framework for protecting workers' mental health and work–life balance (European Parliament, 2019).

The EU Strategic Framework on Health and Safety at Work 2021–2027 also draws attention to the importance of the right to disconnect. This document states that appropriate measures should be developed and implemented to protect workers who work remotely or use digital tools. It calls for research on the impact of psychosocial risks associated with digital and remote working practices, as well as the establishment of minimum standards and conditions to ensure the right of workers to disconnect from work outside of working hours (European Commission, 2021).

The European Commission is preparing recommendations and developing legislative initiatives aimed at harmonizing approaches to the right to disconnect across all Member States. These activities include consultations with Member States and social partners to develop effective mechanisms to protect workers. The EU Coun-

cil also supports initiatives aimed at ensuring the right to disconnect, in particular through the implementation of policies that improve working conditions and promote a healthy work–life balance (Kossek & Lautsch, 2009; Yaroshenko et al., 2024a).

It is important to note that a number of countries have already implemented the relevant right in their legislation, while others do not yet have a clear definition. In order to understand in more detail how the EU regulates the right to disconnect, let us look at the examples of France, Italy, and Romania. France is an interesting example, as it was the first country to define and enshrine the right to disconnect at the legislative level. As noted earlier, the El Khomri law, officially known as Labour Law no. 2016–1088, was enacted in France in 2016, and came into force on 1 January 2017 (République Française , 2016). It was named after the then French Minister of Labour, El Khomri. The law encompasses a broad range of reforms aimed at modernizing labour legislation, improving working conditions, and adapting to changes in the work environment.

A major innovation of the El Khomri law was the creation of the right to disconnect (*droit à la déconnexion*). It allows employees to refrain from using digital tools (emails, phones, etc.) outside working hours in order to protect their personal time in order to maintain a healthy work–life balance. The law requires companies with more than 50 employees to conduct annual negotiations with employee representatives regarding the use of digital tools outside working hours. The goal of these negotiations is to establish rules and boundaries for the use of digital technologies to ensure employees' rest and personal time. If an agreement is not reached during the negotiations, the employer must develop an internal policy (*charte*) after consulting with the Works Council or, in the absence of such a council, with employee representatives. This policy must define the terms for exercising the right to disconnect and include measures for training and raising awareness about the reasonable use of digital tools.

The law mandates training for employees, supervisors, and managers on the proper use of digital tools and the importance of maintaining a balance between work and personal life (République Française , 2016). The El Khomri law has had a significant impact on labour legislation in Europe, inspiring other countries to develop similar initiatives (Justo, 2017). The right to disconnect that it introduces is a crucial step in protecting employees from the constant pressure of being connected, thus promoting their mental and physical health (Pearce, 2019). This right has become an important element of modern labour legislation, highlighting the need to adapt working conditions to the new realities of the digital age.

One significant challenge is that without strict penalties, some companies may not prioritize the implementation of disconnection policies (Pélicier-Loevenbruck & Daubin, 2017; Yaroshenko et al., 2024b). Moreover, the digital age has blurred the lines between personal and professional life, making it difficult to create one-size-fits-all solutions. Employees in certain sectors, such as IT or international business, often need flexibility that traditional working hours do not accommodate (Lerouge

& Pons, 2022). Overall, while the El Khomri law has made strides in highlighting the importance of disconnecting from work, its full impact is still unfolding. It has inspired similar initiatives in other countries, indicating a growing recognition of the need to address work-related stress and promote better work–life balance globally.

On-call duty and unscheduled travel (the French concept of *astreinte*) are regulated separately in France. If an employee is officially on call outside the workplace, they must be ready to leave when called upon if necessary. The French code stipulates that this period of readiness is compensated either by additional pay or by additional time off. The time actually spent working when called out is counted as working time (République Française, 2008), which ensures a balance. In particular, outside of on-call duty, the employer has no right to require work during free time. However, if an employee is officially on call, they are guaranteed compensation and compliance with rest periods. As a result, France is now considered a leader in protecting the right to disconnect. Its legislation promotes a healthy balance between work and personal life for employees.

Italy was one of the first EU countries to adopt France's experience. Italy's Smart Working Law, officially known as Law no. 81/2017, introduced comprehensive regulations for flexible working arrangements, often referred to as 'smart working' or 'agile work' (Ius Laboris, 2025). This law aimed to modernize the Italian labour market by promoting flexibility and improving work–life balance for employees. One of the significant aspects of this legislation is the inclusion of the right to disconnect (Nespoli, 2018). The law requires that smart working arrangements be formalized in writing, and these agreements must include clear provisions guaranteeing the employee's right to disconnect. Article 19 of Law no. 81/2017 explicitly states that the smart working agreement must provide for the worker's right to disconnect, which ensures that employees are not obligated to engage in work-related communications outside of agreed working hours, protecting their personal time and mental health (Italian Government Prime Minister's Office, 2017). Employers are required to inform employees about the specific risks associated with smart working and to ensure their health and safety. This includes providing adequate equipment and ensuring that employees have safe working conditions, even when working remotely. The law also emphasizes the importance of mitigating risks associated with hyper-connectivity and social isolation (Clifford Chance, 2022).

Since the implementation of the Smart Working Law, there has been a notable shift towards more flexible working arrangements in Italy. The law has provided a legal framework that not only facilitates remote work but also protects employees' rights to rest and disconnect from work (Rossi, 2022). However, the effectiveness of these provisions largely depends on the commitment of individual employers to enforce and respect the agreements made with their employees. While the law has been praised for its forward-thinking approach, some challenges remain (Petrillo et al., 2021). Employees in certain sectors report difficulties in completely disconnecting due to the nature of their work. Moreover, the cultural shift towards respecting the

right to disconnect is still ongoing, and continuous monitoring and adaptation are necessary to ensure the law's objectives are fully realized (Loi, 2021). In conclusion, Italy's Smart Working Law represents a significant step towards protecting workers' rights in the digital age. By formally recognizing the right to disconnect, it aims to promote a healthier work–life balance and mitigate the negative effects of an 'always-on' work culture.

However, there is no system-wide right to disconnection for office or field workers in Italy; outside the scope of teleworking, standard labour law provisions on working time and rest apply. For example, the maximum working week and minimum breaks between shifts are set in line with EU standards. Workers who have to travel outside the work schedule are protected in Italy mainly through rules on overtime pay and the regulation of the 'availability to be contacted' (*reperibilità*); there is as yet no formal law. However, the issue of work–rest balance is on the agenda and is often provided for in the collective agreements of some companies (Voynarovska, 2017).

Romania is an interesting case study, as the right to disconnect is not currently regulated by law in this country, unlike the previous two. However, the country's labour law is very strict in regulating working hours and rest periods (Suciu & Petre, 2022). The Romanian Labour Code sets maximum working hours and minimum rest periods. All provisions regarding working hours and rest periods are mandatory, and employees cannot waive the rights recognized by law. Any agreements that attempt to limit these rights are null and void (Dima & Högback, 2020). Romanian law defines working time as any period during which employees perform work, are available to the employer, and fulfil their duties in accordance with the terms of an individual employment contract, collective bargaining agreement, or applicable law. Normal working hours are limited to 8 hours per day and 40 hours per week. Working time may be distributed unevenly, but the total working time may not exceed 48 hours per week, including overtime. Law no. 81/2018 on telework activity introduced special provisions protecting the rights of employees working remotely. According to this law, remote work may be performed outside the employer's premises at least one day a month using information and communication technologies. Employees and employers must both agree on the terms and conditions of such work, including the work schedule (EFILWC, 2018).

While the right to disengage is not explicitly provided for, existing rules limit working hours and provide for rest periods, which helps protect employees from overwork (Negrusa & Butoi, 2022). However, the practical implementation of these rules often leaves much to be desired, and employees may still work beyond normal working hours, leading to overwork and work–life balance issues (Belzunegui-Eraso & Erro-Garces, 2020; Topor & Şolea, 2021). In the context of ensuring the health and safety of employees, Romanian legislation is in line with the requirements of European law, including the obligation of employers to ensure the health and safety of employees in all aspects related to work. Compliance with working-time restrictions

is also considered an important aspect of ensuring the health and safety of employees (Von Bergen et al., 2019; Yaroshenko et al., 2025).

At the same time, the state is very cautious about regulation, an area where a complete ban on contact outside working hours is unrealistic. In particular, this applies to emergency situations; obviously, the law should take such exceptions into account (Muresan, 2025). In summary, in Romania the right to rest is currently guaranteed by the Labour Code, but there is no special concept of the 'right to disconnect'. However, the topic is gaining attention. It is likely that in the coming years, Romania will join the countries that formally enshrine this right, as soon as a balance is found between the interests of employees and the need to ensure the continuity of certain processes. Thus although Romania has not yet introduced a specific right to disengagement, the existing labour law contains elements that can serve as a basis for its future development and implementation.

The results of the analysis of the three EU countries are summarized in Table 1.

Table 1. Analysis of the three EU countries.

Country	Legislative regulation	Legislative basis	Key provisions	Challenges	Impact
France	Enshrined in legislation, regulated by the Labour Code.	El Khomri law (Law no. 2016–1088).	Mandatory annual negotiations on the use of digital tools outside working hours; development of internal policies if no agreement is reached; training on the proper use of digital tools.	Lack of strict penalties for non-compliance; blurred lines between personal and professional life.	Significant impact on labour legislation in Europe. Promotion of employee health.
Italy	Enshrined in legislation, regulated by the specific Smart Working Law.	Smart Working Law (Law no. 81/2017).	Written agreement between employer and employee; inclusion of the right to disconnect; information about risks and ensuring safety.	Difficulties for employees in some sectors to completely disconnect; ongoing cultural shift.	Promotion of flexible working conditions. Protection of employees' right to rest.
Romania	Not currently enshrined, but provisions exist on limiting working hours.	Labour Code and Law no. 81/2018.	Maximum working hours and minimum rest periods; remote work at least one day per month.	Absence of specific right to disconnect; practical implementation often lacking.	Potential for the development and implementation of a specific right to disconnect.

France, Italy, and Romania have different approaches to regulating the right to disconnect. France was the first country to legally establish this right, mandating

annual negotiations and company policies. Italy adapted this approach in its Smart Working Law, ensuring the right to disconnect through written agreements. Romania does not yet have specific legislation on the right to disconnect, but its labour laws include provisions that limit working hours and ensure rest periods. Although the three countries have different approaches to regulating the right to disconnect, they all recognize its importance, even if it is not explicitly enshrined in legislation, as in Romania's case. This recognition underscores the growing awareness of the need to address work-related stress and promote better work–life balance in the digital age. Given this, it is clear that the right to disconnect is becoming an essential element of modern labour policies, reflecting a broader commitment to protecting employees' mental and physical health across Europe.

3.3. The right to disconnect beyond the EU: A global perspective

The right to disconnect, which has become an important element of labour law in Europe, is gaining popularity in other parts of the world. The need to provide employees with the ability to disconnect from work communications outside of working hours is becoming increasingly important in the context of digital transformation and the expansion of remote work. This trend reflects a global trend towards recognizing the importance of work–life balance, protecting employees' mental health, and maintaining their productivity. In this section, we look at how different countries outside Europe are implementing and adapting this right in their legal systems.

We decided to analyse three countries: Ukraine, Canada, and Japan. Ukraine presents an intriguing case for analysis regarding the right to disconnect. Although situated in Europe, it is not a member of the European Union; however, it signed an Association Agreement with the EU in 2014, aspiring to future membership. This agreement has led it to implement many EU principles and legal norms (European Union, 2014; Yaroshenko & Lutsenko, 2022). Ukraine's commitment to aligning with EU standards, combined with its unique challenges, highlights the growing need to establish legal protections for employees, ensuring they have the right to disconnect and maintain their well-being despite the adverse conditions. The right to disconnect is not yet enshrined in labour law; however, there are general rules governing working hours and rest periods. According to the Labour Code of Ukraine, working hours may not exceed 40 hours per week, and overtime must be compensated by additional pay or additional rest time. Ukrainian law also provides for mandatory breaks and days off to ensure work–life balance. In the context of remote work, which has become more widespread due to the military conflict, these provisions are important for the protection of employees (Verkhovna Rada of Ukraine, 1996).

Efforts to introduce the right to disconnect into Ukrainian law were made with the adoption of Law no. 1213–IX in February 2021, aimed at regulating remote work. Article 60–2 of the Labour Code introduces the concept of a disconnection period, guaranteeing employees engaged in remote work a period of free time for rest, during

which they may interrupt any informational or telecommunication connection with the employer without violating the terms of their employment contract or labour discipline (Verkhovna Rada of Ukraine , 2021). The disconnection period is specified in the remote work agreement. Thus remote work has been legally defined as 'a form of labour organization where work is performed by an employee outside the employer's premises or territory, at any location chosen by the employee, using information and communication technologies' (Melnychuk et al., 2022, p. 87). For a remote work agreement, compliance with the written form is mandatory. The existence of a standard form of remote work agreement indicates that the parties do not have the right to deviate from the content of the employment agreement, but may specify its terms. Since remote work requires constant use of information and communication technologies, employees are guaranteed a free time period for rest (a disconnection period), during which they may disconnect from any informational or telecommunication connection with the employer without it being considered a breach of employment terms or discipline. To formalize this, the remote work agreement specifies the exact 'time intervals during the day and/or week when the employee may disconnect from any informational or telecommunication connection with the employer' (Melnychuk, 2022, p. 89). Given Ukraine's aspirations to integrate with the EU and implement European standards, we can expect that the issue of the right to disconnect will be actualized in Ukrainian law. The Association Agreement with the EU requires Ukraine to adapt many labour regulations, which may in the future include the right to disconnect.

Canada is an interesting example, as it represents the American continent, which has a radically different legal system and is based on precedent rather than law. At the federal level, Canada likewise has no explicit statutory right to disconnect, but is moving towards it. The Canada Labour Code provides nationwide minimums for hours of work, rest periods, and overtime pay in federally regulated sectors such as interprovincial transport, banking, and telecommunications. These provisions already limit excessive working time and provide a legal basis for employee rest (Government of Canada, 2022). While Canada is progressively addressing the right to disconnect through various legislative efforts, the challenge lies in the consistent and effective implementation of these policies. The focus is on creating a balanced approach that respects employees' personal time while accommodating the demands of modern work environments. As discussions and legislative developments continue, Canada aims to establish a more comprehensive framework to protect employees' right to disconnect.

In April 2024, the federal government explicitly stated its intention to amend the Canada Labour Code. Canada's 2024 budget provided funds for the development and implementation of legislative changes that would establish the right of employees to refuse work-related contact outside of their working hours. The bill also provides for exceptions, for example for emergencies or critical industries (Workewych, 2024). As of 2025, the bill has not yet been passed.

At the provincial level, in Quebec, Bill 1097 was introduced to ensure employees' rest periods by requiring employers to adopt a disconnection policy. The bill aimed to address the increasing challenges associated with the constant connectivity expected of employees in the digital age. It required employers to adopt a policy setting specific times when employees could ignore work communications, including emails and phone calls. For employers with more than 100 employees, the development of this policy would need to involve consultation with a committee of at least six members, half of whom would be employees. In contrast, smaller companies with fewer than 100 employees would only need to consult directly with their employees, without forming a formal committee (Assemblée Nationale du Québec, 2018). Although the bill did not pass, it sparked significant debate and brought attention to the importance of work–life balance and the need for legislative measures to protect employees' rights.

Ontario also introduced the Working for Workers Act 2021 (Bill 27), which mandates employers with 25 or more employees to develop and implement a written policy on disconnecting from work. This policy must address the employee's right to disconnect from work-related communications (such as emails, phone calls, and messages) outside of their regular working hours. It aims to provide employees with clear boundaries for their work and personal time, helping to reduce work-related stress and improve mental health (Ontario e-Laws, 2021). By prohibiting non-compete agreements and requiring disconnecting-from-work policies, the legislation aims to foster a healthier, more competitive job market and improve overall employee well-being.

Finally, we will conclude this section by analysing Japan, a prosperous country in Asia. Japan is known for being a country of workaholics, with extremely high rates of time spent at work (Kubota et al., 2012). In 2020, about 11.6% of Japanese workers reported working over 60 hours per week. This statistic underscores the prevalence of extended working hours in Japan, indicating that a significant portion of the workforce faces potential health and well-being risks due to overwork (WorldMetrics, 2024). Japan's culture of long working hours leads to serious health problems for employees, including *karoshi* (death from overwork) (Yamauchi et al., 2017). The government has taken several legislative measures to combat this phenomenon; although there is no specific concept of the right to disconnect in Japanese law, several legislative measures are aimed at reducing overwork and improving work–life balance. In 2019, a law aimed at regulating working hours and reducing cases of overwork, known as the Karoshi Prevention Law, was passed (Ministry of Health, Labour and Welfare, 2022); it provides for the key provisions of setting limits on working hours, introducing mandatory vacations, and encouraging employers to create conditions for work–life balance for employees. These measures are intended to ensure the right to disconnect and reduce the risks associated with excessive work.

The Labour Standards Act 2019 sets limits on overtime hours – a maximum of 45 hours per month and 360 hours per year. Even with a special agreement, the excess cannot exceed 100 hours per month or 720 hours per year. Employees are required to take

at least five days of paid vacation per year. The Act stipulates that employers must ensure a minimum interval between the end of one working day and the beginning of the next . Despite the legislative measures, the culture of long working hours is still deeply entrenched, and further efforts are needed to change public perceptions of working hours. Japan has taken important steps to improve working conditions by limiting working hours and making vacations mandatory. However, further efforts are needed at both the legislative and the cultural levels to fully realize the right to disconnect.

We have analysed three radically different countries that differ significantly in geographical, legal, and cultural terms. This analysis has allowed us to understand how the development of the right to disconnect is evolving outside the EU. We present the results in the form of a comparative table (Table 2).

Table 2. Comparative analysis of the right to disconnect outside the EU.

Country	Legislative regulation	Legislative basis	Key provisions	Challenges	Impact
Ukraine	Not currently fully enshrined, but contains elements supporting the concept.	Labor Code, Law no. 1213–IX.	Disconnection period for remote workers; specific time intervals for disconnection in employment contracts.	Provision is mostly declarative; lack of specific safeguards and mechanisms.	Potential to protect workers' rest periods. Alignment with EU standards.
Canada	Enshrined in specific provincial legislation, notably in Ontario.	Working for Workers Act 2021 (Ontario).	Mandatory disconnection-from-work policy for employers with 25+ employees; ban on non-compete agreements; licensing for temp agencies and recruiters.	Varies widely across industries; high-demand sectors may struggle to comply.	Varies widely across industries; high-demand sectors may struggle to comply.
Japan	Not currently fully enshrined, but contains elements supporting the concept.	Work Style Reform Act (2018).	Limits on overtime hours; mandatory annual leave; promotes equal pay for equal work.	Cultural resistance to reducing work hours; difficulties in practical enforcement.	Aims to reduce overwork and *karoshi*. Improves mental and physical health.

These countries highlight the global recognition of the need for work–life balance and the protection of employees' mental and physical health. While full implementation and cultural shifts are ongoing challenges, the legislative frameworks in place demonstrate a commitment to improving working conditions in the digital age. Countries within the European Union remain leaders in implementing the right to disconnect, setting comprehensive legislative frameworks and enforcing policies that support employees' right to rest and disengage from work outside of working hours.

In contrast, countries outside the EU, such as Ukraine, Canada, and Japan, are still catching up in this area. However, the legislative efforts in these non-EU countries indicate a growing understanding of the importance of employee rest and the increasing role of remote work, prompting necessary regulations to support a balanced and healthy work environment. This trend suggests a global shift towards better work–life balance and the protection of employee well-being.

4. Discussion

The findings presented above confirm that the right to disconnect has emerged as a normative response to the psychosocial risks associated with hyper-connectivity at work. Comparative evidence from France, Italy, and Canada suggests that legal codification combined with collective bargaining mechanisms tend to produce more enforceable and employee-centred outcomes (Justo, 2017; Rossi, 2022; Shaw et al., 2021). By contrast, jurisdictions such as Romania and Japan, where the right is not explicitly recognized in law, rely heavily on general working-time provisions and cultural expectations, which often leave employees without effective protection (Suciu & Petre, 2022; Yamauchi et al., 2017). These patterns support the hypothesis that legal recognition of the right to disconnect, when paired with implementation mechanisms, contributes to improved employee well-being and productivity (Giedrewicz-Niewińska et al., 2024).

The right to disconnect contributes to a better work–life balance (Varela-Castro et al., 2022); clearly defined working hours allow employees to spend more time with their personal affairs and family without worrying about work tasks, which contributes to healthy relationships and overall employee well-being (Mankins, 2017). Employees who have the opportunity to disconnect from work are more likely to feel satisfied with their lives, which has a positive impact on their motivation and productivity (Pansu, 2018). Studies show that rested employees demonstrate higher levels of productivity, so ensuring adequate rest time allows employees to be more focused and efficient during working hours (Jochman, 2021). This leads to better quality in the tasks performed and an overall increase in employee productivity. In addition, employees who have the opportunity to get adequate rest are less likely to get sick, which reduces sickness absence (Ollier-Malaterre et al., 2023).

In summary, the introduction of the right to disengage brings numerous benefits to employees, contributing to their health and increasing their work efficiency. It also helps to create a healthier and more harmonious workplace, which is beneficial for both employees and employers. Despite these benefits, the analysis shows that not all countries have implemented the right at the legislative level. Introducing the right to disconnect in countries where it is not yet enshrined in law is a difficult but necessary step to ensure work–life balance for employees. To successfully implement this right, we sug-

gest our own key steps: the first is to conduct a detailed analysis of the existing labour legislation to identify gaps and problem areas. It is also important to study best practices from countries where the right to disconnect has already been implemented, such as France, Italy, and Canadian provinces, to obtain useful examples and models.

The next step is to involve representatives of trade unions, employers, employees, and labour law experts in the discussion. Public consultations will help to collect opinions and suggestions from a wide range of people, which will contribute to the development of more balanced and effective legislation. To create an effective draft law, a working group should be formed to develop provisions on the right to disconnect. This draft law should include clear conditions and mechanisms for exercising the right to disconnect, including setting working hours, periods of disconnection, and employer liability. To ensure the successful implementation of the legislative initiative, it is important to secure support from political parties, non-governmental organizations, and public associations. Organizing an information campaign will help raise awareness of the importance of the right to disconnect and its positive effects for employees.

Adoption of the draft law at the level of parliament or the relevant legislative body is the next important step. After that, it is necessary to develop bylaws and instructions to ensure the effective implementation of the new law; establishing mechanisms to monitor compliance is a key aspect. This may include labour inspections and administrative sanctions for violators. Regularly analysing the impact of the legislation on workers and employers and making adjustments based on feedback are also necessary steps.

To ensure the effective implementation of the right to disconnect, training and educational activities for employers and employees should be conducted. The development of information materials and resources will contribute to a better understanding of the new rules and their importance. Implementing the right to disconnect is a complex process that requires coordinated cooperation between different stakeholders. However, following these steps will help to ensure a healthy work–life balance for employees, promote their mental and physical well-being, and increase overall productivity.

Legal recognition of the right to disconnect offers clear advantages. It protects employees' health and reduces the risks of burnout, stress, and related illnesses. Having clearly defined working hours increases the effectiveness of rest and recovery; in addition, it promotes long-term productivity and creates a more stable and motivated workforce. In a broader context, it increases social trust and reinforces the principle of decent work enshrined in the conventions of the International Labour Organization and the UN Sustainable Development Goals. At the same time, full and strict legal guarantees of the right to disconnect have their drawbacks, which make legislatures cautious. For sectors that by their nature require a constant readiness to respond, too strict a distinction between working and non-working hours can pose real threats to safety and operational efficiency. In addition, a universal obligation to im-

plement a disconnection policy imposes an additional administrative and financial burden on employers. In international companies operating in multiple time zones, this can lead to significant organizational difficulties. There is also a risk of a formalistic approach; that is, companies implement policies solely for compliance purposes, without actually changing their corporate culture. In some cases, overly strict rules may even encourage informal communication outside official channels, reducing the level of real protection for employees.

The combination of these factors explains why the right to disconnect has not yet become a universal standard in either European Union or international law. Although the European Parliament called for the development of a relevant directive back in 2021, the European Commission has not proposed any binding legislation. This is firstly due to significant differences in national labour regimes, which complicates unification. Secondly, the EU already has legislation in place that establishes basic guarantees for rest periods and gives countries broad scope for their own regulation. Thirdly, during consultations, social partners expressed concern about the potential impact of strict legal enforcement on the competitiveness of enterprises and the flexibility of work organization. As a result, the Commission gave preference to soft law and the encouragement of national initiatives.

Similar arguments can be found outside the EU, particularly in Canada. A telling example is the experience of the province of Quebec, where Bill 1097 was not passed. The reasons for this were legal doubts about its constitutionality in terms of the division of powers between the federal and provincial levels, and significant resistance from the business community. However, the very appearance of this bill sent a powerful signal for further initiatives, in particular for the Canadian federal government's 2022–2024 consultations on the possible introduction of nationwide standards. Thus the right to disconnect lies at the intersection of individual human rights and public safety needs. Its enshrinement brings undeniable social benefits, but requires a delicate balance between flexibility and obligation. It is emphasized that employer obligations in the context of remote work require not only technical safeguards but also organizational policies that respect workers' private time. Findings from Slovakia, the Czech Republic, and Poland reinforce the conclusion that the right to disconnect should be viewed as part of a broader framework of occupational health and safety rather than as an isolated labour right (Giedrewicz-Niewińska et al., 2024). Including this perspective broadens the comparative analysis and links the current study with ongoing debates in Central and Eastern Europe.

The right to disconnect cannot be interpreted as absolute and unconditional, because the modern economy and society require flexible mechanisms for responding to unforeseen circumstances. Many areas cannot fully function without the readiness of personnel for unplanned intervention. This poses a difficult task for the right to disconnect, which on the one hand guarantees the employee the inviolability of private life and rest, and on the other does not paralyse the ability of organizations to act

in cases of emergency, natural disasters, cyberattacks, or man-made accidents. That is why in most national legal systems, the law provides for exceptions for cases of *force majeure* or clearly regulated shifts, provisions which provide the employee with compensation. This approach confirms that the task of the legislature is not to formally distinguish between working and free time, but it is necessary to create a fair mechanism for flexible responses. Accordingly, in the future, the development of this institution will require in-depth differentiation, first of all to determine the categories of employees for whom exceptions are inevitable. In addition, it would be advisable to establish transparent criteria for what exactly is considered a 'critical situation'. The state should also guarantee adequate compensation. Such a balanced model will not only preserve the content of the right to disconnect but will also increase the resilience of key sectors of the economy and public administration in the face of the increasing risk of emergency events.

Conclusion

The conducted analysis confirms that the right to disconnect is emerging as a key legal response to the psychosocial risks of the digital work environment. Comparative research of France, Italy, and Romania, as well as Ukraine, Canada, and Japan, demonstrates that states are experimenting with different legal and institutional models rather than moving towards a single formula. The diversity of these approaches shows that the right to disconnect develops within national labour traditions and existing statutory frameworks. The Ukrainian model of explicitly defined disconnection periods for remote work, Canada's provincial and emerging federal initiatives, and Japan's reliance on strict overtime limits and cultural reform illustrate similar variety outside the EU.

These findings indicate that effective protection cannot be reduced to the mere adoption of legal norms. Sustainable implementation requires a combination of statutory guarantees with corporate practices and collective bargaining, as well as cultural change that redefines expectations of constant availability. The COVID-19 pandemic, which accelerated remote and hybrid work, has highlighted how easily working hours can expand beyond contractual limits and how urgently employees need clear, enforceable rest periods. At the same time, the research underlines that certain sectors demand narrowly tailored exceptions and well-compensated on-call regimes, proving that the right to disconnect must remain flexible and context-sensitive.

The study also explains why no universal international standard has yet emerged. Within the EU, existing instruments such as the Working Time Directive already secure minimum rest periods, and the heterogeneity of national labour markets, combined with concerns about competitiveness, has so far led the European Commission to refrain from proposing a binding directive, despite the European Parliament's

calls. Outside the EU, political economy factors and constitutional divisions of competence similarly slow down codification. The experience of Quebec, where Bill 1097 stimulated public debate but failed to pass because of legal and economic objections, illustrates these structural constraints.

Overall, the research supports the conclusion that the right to disconnect is evolving as a layered and pluralistic institution. It functions most effectively when embedded in a broader framework of occupational health and safety, supported by social dialogue and adapted to sector-specific needs. While the direction of change is clear – towards stronger recognition of employees' entitlement to genuine rest – the pathways remain diverse. This comparative perspective demonstrates both the global relevance of the right to disconnect and the necessity of nuanced, context-aware legal design, rather than one-size-fits-all regulation.

REFERENCES

Assemblée Nationale du Québec. (2018). *Journal des débats (Hansard) of the National Assembly*. https://www.assnat.qc.ca/en/travaux-parlementaires/assemblee-nationale/41–1/journal-debats/20180322/216243.html

Becker, W., Belkin, L., & Tuskey, S. (2018). Killing me softly: Electronic communications monitoring and employee and spouse well-being. *Academy of Management Proceedings*, *1*. https://doi.org/10.5465/AMBPP.2018.121

Belzunegui-Eraso, A., & Erro-Garces, A. (2020). Teleworking in the context of the Covid-19 crisis. *Sustainability*, *12*(9), 1–18.

Bokor-Szőcs, I. (2023). The right to disconnect. *Journal of Public Administration, Finance and Law*, *29*, 88–96. https://doi.org/10.47743/jopafl-2023–29-08

Bouciqué, W., & Vets, E. (2023). *The right to disconnect: Which countries have legislated?* Ius Laboris. https://iuslaboris.com/insights/the-right-to-disconnect-which-countries-have-legislated/

Clifford Chance. (2022). *Protecting mental health in the digital workspace: The right to disconnect*. https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2022/07/Right-to-disconnect-directive-employment-client-briefing.pdf

Dima, L., & Högback, A. (2020). *Legislating a right to disconnect: Labour and social justice*. Friedrich Ebert Stiftung. https://library.fes.de/pdf-files/bueros/bukarest/17025.pdf

Escobar, M. (2019). *El derecho a la desconexión digital* [Undergraduate dissertation, Universidad de Valladolid]. https://uvadoc.uva.es/bitstream/handle/10324/35307/TFG-N.1040.pdf

European Commission. (2021). *EU strategic framework on health and safety at work 2021–2027*. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12673-Health-Safety-at-Work-EU-Strategic-Framework-2021–2027-_uk

European Foundation for the Improvement of Living and Working Conditions. (2018). *Measures for simplifying conduct of teleworking*. https://static.eurofound.europa.eu/covid19db/cases/RO-2021–19_1935.html

European Parliament. (2021). Resolution 2019/2181(INL) The Right to Disconnect. https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2019/2181(INL)&l=en

European Union. (2014). *Association agreement between the European Union and its member states, of the one part, and Ukraine, of the other part*. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A22014A0529%2801%29

Eurostat. (2024). *Employed persons working from home as a percentage of the total employment, by sex, age and professional status*. https://ec.europa.eu/eurostat/databrowser/view/LFSA_EHOMP/default/table?lang=en

Gibson, C. B., Gilson, L. L., Griffith, T. L., & O'Neill, T. A. (2023). Should employees be required to return to the office? *Organizational Dynamics*, *52*(2). https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10126217/

Giedrewicz-Niewińska, A., Križan, V., & Komendová, J. (2024). The obligations of the employer in the implementation of remote work: The examples of Slovakia, the Czech Republic and Poland. *Białostockie Studia Prawnicze*, *29*(2), 83–97. https://doi.org/10.15290/bsp.2024.29.02.07

Gnatenko, K. V., Yaroshenko, O. M., Anisimova, H. V., Shabanova, S. O., & Sliusar, A. M. (2020). Prohibition of discrimination as a principle of social security in the context of ensuring sustainable well-being. *Rivista di studi sulla sostenibilita*, *2*, 173–187. https://doi.org/10.3280/RISS2020–002-S1013

González, G. G. (2020). Public employees' right to digital disconnection: Scope and significance of an emerging right in the context of the health crisis. *Revista catalana de dret public*, *1*, 54–71. http://revistes.eapc.gencat.cat/index.php/rcdp/article/view/10.2436-rcdp.i0.2020.3505/especialCOV-ID-garcia-es.pdf

Government of Canada. (2022). *Final report of the Right to Disconnect Advisory Committee*. https://www.canada.ca/en/employment-social-development/corporate/portfolio/labour/programs/labour-standards/reports/right-to-disconnect-advisory-committee.html

Hesselberth, P. (2017). Discourses on disconnectivity and the right to disconnect. *New Media & Society*, *20*(4), 1994–2010. https://doi.org/10.1177/1461444817711449

Italian Government Prime Minister's Office. (2017). Law no. 81 Misure per la tutela del lavoro autonomo non imprenditoriale e misure volte a favorire l'articolazione flessibile nei tempi e nei luoghi del lavoro subordinato. https://www.gazzettaufficiale.it/eli/id/2017/06/13/17G00096/sg

Ius Laboris. (2025). Smart working and 'short weeks' are here to stay in Italy. Retrieved from. https://iuslaboris.com/insights/smart-working-and-short-weeks-are-here-to-stay-in-italy/

Jacques, P. H., Garger, J., Mullen, A., & Petrarca, P. (2023). The future of work and teleworking: A conceptual study of employee preferences, managerial strategies, and RTO mandates. *Journal of Behavioral and Applied Management*, *23*(2), 74–83.

Jaworska, K. (2022). The right to disconnect. *Studies on Labour and Social Policy*, *29*, 51–58. https://doi.org/10.4467/25444654SPP.22.005.15373

Jochman, T. (2021). Effects on employees' compensation under the right to disconnect. *Marquette Benefits and Social Welfare Law Review*, *22*(2), 209–224.

Justo, S. (2017). *An analysis of the El Khomri law and its effects on the French North African population* [Undergraduate dissertation, The Pennsylvania State University]. https://honors.libraries.psu.edu/files/final_submissions/4492

Kossek, E., & Lautsch, B. A. (2009). *CEO of me: Creating a life that works in the flexible job age*. Prentice Hall Professional.

Kubota, K., Shimazu, A., Kawakami, N., & Takahash, M. (2012). Workaholism and sleep quality among Japanese employees: A prospective cohort study. *International Journal of Behavioral Medicine*, *21*(1), 66–76. https://doi.org/10.1007/s12529–012-9286–6

Lerouge, L., & Pons, F. T. (2022). Contribution to the study on the 'right to disconnect' from work: Are France and Spain examples for other countries and EU law? *European Labour Law Journal*, *13*(3), 450–465.

Loi, D. (2021). *The impact of teleworking and digital work on workers and society*. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662904/IPOL_STU(2021)662904(ANN04)_EN.pdf

Lomborg, S., & Ytre-Arne, B. (2021). Advancing digital disconnection research: Introduction to the special issue. *Convergence*, *27*(6), 1529–1535.

Mankins, M. (2017). *Why the French email law won't restore work–life balance*. Harvard Business Review. https://hbr.org/2017/01/why-the-french-email-law-wont-restore-work–life-balance

Melnychuk, O. F. (2022). The right to disengagement in the labour legislation of Ukraine and foreign countries. *Забезпечення прав Людини: національний та Міжнародний виміри* (pp. 87–92). https://vspu.edu.ua/content/confer/k_1001.pdf

Melnychuk, O. F., Melnychuk, M. O., & Pavlichenko, I. M. (2022). Legal regulation and specifics of remote work appliance in conditions of martial law. *Scientific Bulletin of Uzhhorod National University*, *70*, 242–247. https://doi.org/10.24144/2307–3322.2022.70.37

Ministry of Health, Labour and Welfare (Japan). (2022). *White paper on measures to prevent karoshi*. https://www.mhlw.go.jp/content/11200000/001065344.pdf

Muresan, D. (2025). *Ce implicații are munca după program. Ministrul Muncii explică dreptul la deconectare pe înțelesul tuturor*. DCNews. https://www.dcnews.ro/ce-implicatii-are-munca-dupa-program-ministrul-muncii-explica-dreptul-la-deconectar-tuturor_989968.html

Negrusa, A. L., & Butoi, E. (2022). The work–life balance and well-being of Romanian teleworkers during pandemic. *Studia UBB Negotia*, *67*(1), 7–25.

Nespoli, E. (2018). *Italy – Employment law review*. Ius Laboris. https://iuslaboris.com/insights/italy-employment-law-review-2017/

Ollier-Malaterre, A., Allen, T., Ernst Kossek, E., Chang-Qin, L., Morandin, G., Pellerin, S., Rostami, A., & Russo, M. (2023). Digital regulation in the service of sustainable work–life balance. In P. Kruyen, S. André, & B. Van der Heijden (Eds.), *Maintaining a sustainable work–life balance* (pp. 41–45). Edward Elgar Publishing. https://doi.org/10.4337/9781803922348.00023

Ontario e-Laws. (2021). Working for Workers Act. https://www.ontario.ca/laws/statute/s21035

Pansu, L. (2018). Evaluation of right to disconnect legislation and its impact on employee's productivity. *International Journal of Management and Applied Research*, *5*(3), 99–119. https://doi.org/10.18646/2056.53.18–008

Parliament of Canada. (2006). Fair Access to Regulated Professions and Compulsory Trades Act. https://www.ontario.ca/laws/statute/06f31

Pearce, D. (2019). *The working world: France gave workers the right to disconnect – but is it helping?* https://blog.dropbox.com/topics/work-culture/france-right-to-disconnect-law

Pélicier-Loevenbruck, S., & Daubin, S. (2017). *Sorting out the truth about the right to disconnect in France*. JDSupra. https://www.jdsupra.com/legalnews/sorting-out-the-truth-about-the-right-50707/

People Management. (2017). *It's up to managers to make sure employees disconnect from work*. https://www.peoplemanagement.co.uk/voices/comment/managers-make-sure-employees-disconnect-work

Petrillo, A., De Felice, F., & Petrillo, L. (2021). Digital divide, skills and perceptions on smart working in Italy: From necessity to opportunity. *Procedia Computer Science*, *180*(2), 913–921.

République Française. (2008.) Code du travail. https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006072050/

République Française. (2016, 8 August). Loi no. 2016–1088 relative au travail, à la modernisation du dialogue social et à la sécurisation des parcours professionnels (1). https://www.legifrance.gouv.fr/loda/id/JORFTEXT000032983213

Rossi, L. (2022). *Post-pandemic 'smart working': What has changed in Italy?* Ius Laboris. https://iuslaboris.com/insights/post-pandemic-smart-working-what-has-changed-in-italy/

Sampaio, L. (2020). *The 'El Khomri law' on François Hollande's employment and competitiveness politics. (2012–2017)*. https://www.researchgate.net/publication/366696487_The_El_Khomri_Law_on_Francois_Hollande's_Employment_and_Competitiveness_Politics_2012–2017

Schmit, N. (2024). *Commission launches first-stage consultation of social partners on fair telework and the right to disconnect*. European Commission. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1363

Shaw, A., Anandarajah, A., & Scarcello, A. (2021). *Ontario passes the Working for Workers Act*. Canadian Labour and Employment Law. https://www.labourandemploymentlaw.com/2021/12/ontario-passes-the-working-for-workers-act/

Sonnentag, S. (2012). Psychological detachment from work during leisure time. *Current Directions in Psychological Science*, *21*(2), 114–118.

State Labour Service of Ukraine. (2021). *Remote work: What employers need to know about*. https://dsp.gov.ua/podolannia-nelehalnoi-zainiatosti/dystantsiina-robota-pro-shcho-treba-znaty-robotodavtsiu/

Suciu, M., & Petre, A. (2022). Telework in Romania: Current state and sustainable socio-economic effects of its development. *Management Dynamics in the Knowledge Economy*, *10*(1), 53–68.

Thomée, S., Harenstam, A., & Hagberg, M. (2011). Mobile phone use and stress, sleep disturbances, and symptoms of depression among young adults: A prospective cohort study. *BMC Public Health*, 11(66), 1–12.

Topor, A., & Şolea, R. (2021). *Telework in Romania*. Blekinge Institute of Technology. https://www.diva-portal.org/smash/get/diva2:1744482/FULLTEXT02.pdf

United Nations. (1948). *Universal declaration of human rights*. https://www.un.org/en/about-us/universal-declaration-of-human-rights

Varela-Castro, W. H., Briceño-Santacruz, M., & Castro-Solano, M. O. (2022). The right to disconnect: Influence on competitiveness, productivity and creativity. *Mercados y Negocios*, *46*(23), 5–30.

Verkhovna Rada of Ukraine. (1996). Law of Ukraine no. 322–308. https://zakon.rada.gov.ua/laws/show/322–08#Text

Verkhovna Rada of Ukraine. (2021). Закон України "Про внесення змін до деяких законодавчих актів України щодо удосконалення правового регулювання дистанційної, надомної

роботи та роботи із застосуванням гнучкого режиму робочого часу". Law of Ukraine no. 1213–IX. https://zakon.rada.gov.ua/laws/show/1213–20#Text

Von Bergen, C. W., Bressler, M., & Proctor, T. L. (2019). On the grid 24/7/365 and the right to disconnect. *Employee Relations Law Journal*, *45*(2), 3–20.

Voynarovska, O. (2017). *Is the right to 'disconnect' a new trend?* VKP. https://vkp.ua/publication/is_the_right_to_disconnect_a_new_tendency

Workewych, L. (2024). *Right to disconnect proposed for federally regulated employees*. Dentons Canadian Employment & Labour Law. https://www.employmentandlabour.com/right-to-disconnect-proposed-for-federally-regulated-employees

WorldMetrics. (2024). *Japanese work hours statistics*. https://worldmetrics.org/japanese-work-hours-statistics/#sources

Yamauchi, T., Yoshikawa, T., Takamoto, M., Sasaki, T., Matsumoto, S., Kayashima, K., Takeshima, T., & Takahashi, M. (2017). Overwork-related disorders in Japan: Recent trends and development of a national policy to promote preventive measures. *Industrial Health*, *55*(3), 293–302.

Yaroshenko, O. M., Ivchuk, Y. Y., Maliuha, L. J., Nesterovych, O. S., & Lutsenko, O. Y. (2024b). Legal status of the self-employed person in the field of social protection in Ukraine. *International Journal of Discrimination and the Law*, *24*(3), 217–233. https://doi.org/10.1177/13582291241264181

Yaroshenko, O. M., Sereda, O., Harashchuk, V., Mohilevskyl, L., & Yushko, A. (2024a). Non-fixed working hours in the context of globalisation: The impact of international trends on national legislation and employers' practices. *Revista jurídica portucalense*, *35*, 238–260. https://doi.org/10.34625/issn.2183–*2705*(35)2024.ic-12

Yaroshenko, O. M., Vitvitskyi, S. S., Nesterovych, O. S., Sereda, O. H., & Yakovlyev, O. A. (2025). Legal protection of employee privacy in the workplace. *Journal of Legal Affairs and Dispute Resolution in Engineering and Construction*, *17*(2), 04525003. https://doi.org/10.1061/JLADAH.LADR-1202

Yaroshenko, O., & Lutsenko, O. (2022). The working in war: Main changes in labour relations and working conditions under martial law in Ukraine. *Access to Justice in Eastern Europe*, *17*, 139–155. https://doi.org/10.33327/AJEE-18–5.4-a000466

Bialystok Legal Studies
Białostockie Studia Prawnicze
2025 vol. 30 no. 4

sciendo

DOI: 10.15290/bsp.2025.30.04.10

Received: 16.04.2025
Accepted: 20.09.2025

Mariusz Jabłoński
University of Wroclaw, Poland
mariusz.jablonski@uwr.edu.pl
ORCID ID: 0000–0001–8347–1884

The Right to Privacy and the Obligation to Transfer and Authenticate Personal Data through the Internet: Conflicting Issues

Abstract: Contemporary legal and commercial solutions practised by various types of businesses are associated with a definition of precisely specified obligations imposed on the actors of the indicated activities (natural persons, legal persons and other legal entities). This also includes an obligation to perform specific actions only (or in parallel) electronically, including the implementation and application of top-down (authoritative) authentication processes, defined by legislation and by commercial entities. In practice, there is a lot of controversy concerning both the necessity of such solutions and the definition of the nature and scope of protection of the rights of individuals who are obliged to transfer certain information in this way. This is not only about minimizing the possible liability of the specific actor who obtains this type of data (the administrative body, institution or entity, e.g. an entrepreneur) for its loss and/or improper use, but in general about justifying the necessity of this type of obligation. Analysis of these issues will be presented as part of a substantive study considered in the light of limits for protecting the right to privacy.

Keywords: obligations, businesses, electronic authentication, privacy rights, data protection

Introduction

The formation of the content of the privileges granted to individuals is related to the evolution of the consciousness and the basis of existence of social groups in a particular country, continent or globally. The dynamic development of information technology (ICT) has significantly influenced (and will continue to influence) a redefinition of the content of many previously normatively identified rights and

freedoms. This development has resulted in the concepts of so-called 'digital personalization' and 'digital transformation' (European Parliament, 2021), which involve, for example, the multifaceted identification of user data provided by an individual while using available digital technologies. These technologies are understood as a set of mechanisms and ways of implementing digital operations in software. The consequence of this process is an increase in new challenges, primarily related to ensuring adequate protection of the information autonomy of individuals.

There is no doubt that '[i]nternational human rights law recognizes a fundamental right to privacy, including privacy in one's electronically-stored personal communications. This right is reflected and given concrete form in the legal regimes of countries around the world, including through statutes, constitutional provisions, and international agreements that regulate data processing by both private entities and government actors' (Supreme Court of the United States, 2018; pp. 6–7). In reality, however, this does not mean that the protection of privacy, including personal data, is always adequate and complete (Rise, 2018). Personal data protection is considered a part of the privacy of the individual, and together with freedom of information and expression, they create the personal information sphere (Eskens, 2020). Whereas the right to privacy is a wider and older concept, it is personal data protection which has recently gained the spotlight, especially in the context of ICT, surveillance and the exploitation of users' data. Personal data protection protects privacy by regulating the processing of personal data (de Andrade, 2011).

Of course, most of the current legal regulations (primarily EU and national), as well as implemented business practices (such as procedures, road maps, to-do lists and business standards), include a definition of the obligations imposed on the parties (natural persons and/or legal entities) of activities carried out electronically (de Gregorio, 2022; Jablonowska & Tagiuri, 2023). These activities often require the implementation of identification and authentication processes, either defined by the legislature (top-down authority) or contractually by businesses (standardized by consent). In practice, however, there is a lot of controversy about the necessity and indispensability of such practices and the definition of the nature and extent of the protection of the rights of individuals who are obliged to transfer their personal data by these means (including those related to ensuring their subsequent processing). It is not only a matter of minimizing the possible liability of the controller who acquires authentication data for its loss and/or misuse; a challenge also arises by the justification of identification and authentication obligations. Additionally, in many cases the current solutions, at least to some extent, transfer some of the dangers to the weaker party, i.e. the user and/or consumer (Jabłoński & Węgrzyn, 2023; Rise, 2018). These mechanisms rely on users bluntly accepting terms and conditions or consenting to certain features (without a real alternative) and a lack of efficient enforcement mechanisms which would secure their rights and control over their data. At the same time, many users of ICT systems lack basic knowledge of the contemporary risks associated with irresponsible sharing of their

personal data, which leads to all sorts of negative consequences and/or a lack of control over who is processing it and for what purpose.

The current phase of the digitization of states and societies leads to the conclusion that society is at a transitional stage. On the one hand there is a desire to deformalize various types of activities and procedures as far as possible, and on the other there is a need for the creation of an objectively secure system for the transmission and processing of various types of information. Reconciling these two different goals, however, is not always possible to achieve.

1. The formation of the information society as a consequence of the implementation of modern technologies

The modern approach towards the use of ICT in day-to-day activities is based on the assumption that the world has entered the era of the information society. This has been emphasized on multiple occasions by the European Union and Member States, and the idea of the digitization of public administration is predefined through the existence of a society which cannot properly function without new technologies. The concept of an information society, i.e. one whose members make organized and conscious use of existing information resources using available technologies in particular information systems (Webster, 2014) in order to achieve an intended result, has already been known for several decades. The functioning of such a society involves the need to distinguish the concept of the so-called 'information public space'. This space is identified with publicly accessible data sets, but also with the legislature's imperative to implement dynamic safeguards, procedures, mechanisms and technological standards in implementing various tasks, by public and private organizations. In the information society, members of the community are able to independently and at the same time responsibly use the available digital technology to determine various types of processes, ranging from political, social and control, to economic, consumer and educational ones (Avgerou & Madon, 2005 de Gregorio, 2022).

The base of the functioning of the information society is knowledge, including both access to information and also an understanding of technology (its advantages and risks), which is used by the members of society for a specific and intended purpose. The natural environment that supports each of its members is the world of digital technologies – the sum of available functionalities and information resources (bases). These technologies make it possible to achieve various types of effects (legal and factual) at a distance, including:

- informational – getting acquainted with specific information,
- interactional – providing an interested party with two-way communication with a specific entity (consumer, educational, etc.),

- transactional –equivalent to the creation of an electronic procedure, the use of which is used to bring about intended legal effects,
- electoral – providing participation in various types of processes of the expression of will, such as elections,
- entertainment – providing users with features aiming solely (or mostly) at entertainment (i.e. videogames, video streaming, music, etc.).

Knowledge is the starting point for assuming that members of the information society are capable of identifying which technologies they use in connection with achieving a specific goal and understanding the essence of the mechanisms of implementing digital operations and the software that serves this purpose. Achieving such a state is based on the presumption that they are skilled enough, which is the result of appropriate education, in an institutionalized (i.e. organized by the state) and dynamic form. Accepting that we are dealing with a prepared and responsible member of the information society therefore requires demonstrating that he or she has been properly trained (educated).

The functioning of the information society in a particular state (as well as in an international organization) is subject to the applicable regulatory regime. The existing legal rules (including constitutional principles) should define guarantees for freedoms and rights and adequately specify the essence and nature of obligations imposed on entities that are able or are already obliged to use specific technologies. Lawmakers must also define standards for ensuring adequate security and protection against the risks that are associated with the use of ICT systems.

2. The digital accessibility and digital security model

The starting point to evaluate the operations of public and private entities carrying out public tasks is the establishment of a normative framework for interoperability that specifies how those entities should proceed, while deciding on the means, methods and standards used in their ICT systems. The next steps are the specification of the standard of minimum requirements for public registers and the exchange of information in electronic form, considering accessibility, and ways to ensure security in the exchange of information (also in cross-border exchanges), including data formats and communication and encryption protocols in interface software. These regulations are intended to ensure the digital accessibility of websites and applications by ensuring their functionality, compatibility, perceptibility and comprehensibility as per the EU Directive on the Accessibility of Websites and Mobile Applications of Public Sector Bodies. Normatively guaranteed accessibility is the starting point, and its absence must be treated as a negative premise in terms of imposing a regulatory obligation on an individual to use a specific ICT system while cooperating with the state (and its representatives). A lack of accessibility may also lead to discrimination

(Kuźnicka, 2017), because defining the technological aspects of accessibility makes it possible to properly 'train' its user and, consequently, prepare him or her to use it independently and responsibly. For this reason, the principle that an individual cannot be burdened with a duty to use applications whose accessibility does not simultaneously meet the requirements of functionality, compatibility, perceptibility and comprehensibility should also be taken as a basis.

The next step becomes the identification and implementation of all those solutions that serve to protect information security, including personal data. The European Union has intensified its activity in this field in recent years, considering the implementation of the Regulation on Measures for a High Common Level of Security of Networks and Information Systems within the Union, the Regulation on the Processing of Personal Data (GDPR), the Directive on Measures to Promote a High Common Level of Cybersecurity within the Union, the Regulation on the Cryptocurrency Markets, and the Regulation on Operational Digital Resilience of the Financial Sector (Dunaj, 2023; Milczarek, 2020; Yang et al., 2019). All of these regulations impose certain obligations in regard to security measures and the protection of information on, for example, public entities, as well as private conducting public tasks. Analysing the actions of the EU lawmakers, it becomes apparent that they are consequential in nature; they do not usually precede the effects of the implementation of increasingly innovative information and digital technologies.

It is sufficient to point out the use of artificial intelligence (AI) algorithms, for example. These technologies, which have been in use for years, will only now become the subject of a normative definition, through the adoption of the EU AI Act. In the proposal, it was emphasized that the newly adopted regulation is aligned with current EU law, including the Charter of Fundamental Rights but also regulations introducing specific standards on information protection. The AI Act is supposed to further implement 'a set of harmonised rules applicable to the design, development and use of certain high-risk AI systems and restrictions on certain uses of remote biometric identification systems' (European Commission, 2021). The AI Act is supposed to complement 'existing Union law on non-discrimination with specific requirements that aim to minimise the risk of algorithmic discrimination, in particular in relation to the design and the quality of data sets used for the development of AI systems complemented with obligations for testing, risk management, documentation and human oversight throughout the AI systems' lifecycle' (European Commission, 2021). This in fact proves that operability and information security become immanent parts of any ICT used to conduct public tasks.

The laws and regulations introduced in the area of requirements for ICT services define the legal standards and specify principles and rules of ethics. Additionally, these laws impose measures and procedures to ensure the security and technical resilience of the systems used. Digital security as a concept related to the protection of individual freedoms and rights is therefore complex; it must involve the real existence

of a catalogue of specific legal, technical and ethical obligations incumbent on the organization (whether public or private) that implements and uses a particular technology (which may include an obligation for the person to use it). When deciding on the regulatory framework applicable to the organization, one must consider obligations connected with the accessibility and security of the solutions provided. Additionally, standards for the protection of all individual rights must be specified, therefore not only those that are limited to the sphere of information autonomy.

3. The personal and informational autonomy of the individual

Personal autonomy, including the informational autonomy of the individual, is identified with an independent right that is part of the content of the right to privacy, equatable to the concepts of 'self-creation' or 'self-determination' (Judgments of the ECHR, 1984, 1992, 2007; Roagna, 2012).

Instead of providing a clear-cut definition of private life, the Court has identified, on a case-by-case basis, the situations falling within this dimension. The result is a rather vague concept, which the Court tends to construe and interpret broadly: over the years the notion of private life has been applied to a variety of situations, including bearing a name, the protection of one's image or reputation, awareness of family origins, physical and moral integrity, sexual and social identity, sexual life and orientation, a healthy environment, self-determination and personal autonomy, protection from search and seizure and privacy of telephone conversations. (Roagna, 2012; p. 12)

In this regard, it is emphasized that an individual has a subjective right 'to decide independently on the disclosure to others of information concerning his or her person, as well as the right to exercise control over such information in the possession of others' (Judgments of the Polish Constitutional Tribunal of 2002, 2009, 2014).

In negative terms, the protection of informational autonomy is identified with the prohibition of excessive external interference, such as obtaining and collecting personal data and information about the habits or behaviours of an individual (informational privacy). This protection – at the vertical level – serves to limit the ability of the state to obtain information about a particular private person (Grzelak & Zielińska, 2021; Roagna, 2012, p. 60). The protection of privacy requires in each case that the specifics of the particular situation are taken into account (such protection is not absolute), including values (also equivalent ones) that are in conflict with each other, e.g. the right to privacy, or national security (European Data Protection Supervisor, 2024; Judgment of the CJEU, 2010; Judgments of the ECHR, 1992, February 2000, May 2000, 2002, 2003).

With regard to public figures and, in particular, to persons performing public functions, the protection of such autonomy is even more limited (but not excluded). Horizontally, respect for informational autonomy means respect for the guaranteed

rights in the relationships between individuals, as well as between them and other private entities. In a situation of their violation, it allows the possibility for individuals as well as legal entities to invoke normatively guaranteed rights in the settlement of civil and labour disputes.

Any form of communication, regardless of the physical medium (e.g. personal and telephone conversations, written correspondence, fax, text and multimedia messages or electronic mail), is protected. This is a matter of guaranteeing the confidentiality and integrity of the messages' content, as well as all the circumstances of the communication process, which include, among other things, the personal data of the participants (protection against acquisition, processing, storage and disclosure, in a manner that violates the rules of usefulness, necessity and proportionality, *sensu stricto*, of information (Judgments of the CJEU, 2014, 2016, 2020; Judgment of the ECHR, 2015)). The protection of information autonomy is aimed at restricting the limits of formally guaranteed freedoms in the area of information sharing (data, knowledge, etc., including freedom of expression) collected by an individual. In this approach, it is also a matter of concretizing the span of the implementation of normatively confirmed powers and freedoms, which concern both the vertical and horizontal scope of their validity and application. Thus, model-wise, we are dealing here with the sum of guarantees, the purpose of which is to provide an individual with protection against unauthorized and secret monitoring of his or her life (and activity in various fields).

From the vertical (state–individual) perspective, it is assumed that the legalization of encroachment into the sphere of guaranteed informational autonomy is an explicit provision of law based on the principle of proportionality and legality. The risk of infringement of civil liberties and fundamental rights must be proportional to the purpose it serves. Discussion around the vertical and horizontal level of validity is crucial considering that proper identification is required not only in relation to the individual and the state but also between individuals and private entities. The same applies to the protection of the rights affirmed to the individual (including the assured 'freedom from' and 'freedom to'). Scholarly literature emphasizes that the concept of the horizontal operation of individual rights must be identified with the application of constitutional norms concerning them precisely in private law, which is also obvious in relation to the settlement of civil and labour disputes (Safjan, 2014).

With the right of the individual to decide to disclose information about themselves to others or not, the right to exercise control as to the scope and nature of the information disclosed and the subsequent processing of the information by the entity or entities acquiring it is also related. This approach is also expressed in the GDPR through its principles and general approach. The purpose of enacting the GDPR was to strengthen and harmonize the protection of the fundamental freedoms and rights of individuals in connection with processing activities and to ensure the free flow of personal data between Member States (Recital 3 of the Preamble). Indeed, this protection is not limited to the creation of safeguards to define the regularity of process-

ing and the flow of personal data. It must be understood more broadly, and indirectly as the protection of all freedoms and rights defining the individual's information autonomy in the broadest sense. This autonomy, in the simplest terms, is identified with the individual's freedom to decide independently to disclose information about him – or herself and his or her own life to other bodies, institutions or entities (e.g. businesses or social organizations, as well as various types of organizational units), as well as the real right to exercise control over the processing of such data if it is in the possession of other entities, and in particular those whose obligation to provide access results from the provisions of generally applicable law.

The legalization of data processing on the basis of a specific premise (Articles 6 and 9 of the GDPR) will not be considered lawful if the processing that occurs involves (at the will of the controller) data other than what is necessary in the context of the controller's articulated purpose. In practice, appropriate action by the controller must take the form not only of preparing specific policies, clauses, contracts, records, procedures, mechanisms and assessments, but also of properly implementing them, and then adequately modifying them, depending on changing conditions (including risks). This is because each controller must identify the specifics of the premises and processes of the data processing and the accompanying risks, also in order to eliminate existing risks and apply appropriate and adequate safeguards (technical and organizational measures). The amount and diversity of analyses conducted by controller must therefore result in the individualization of solutions, and consequently the possibility of using identical patterns or standard implementation models by other, even generic and identical, controllers is excluded. This is because even if the majority of processing operations may be similar, the controller's ability to respond to the changing landscape of risks and its organization is different. There is no one 'fit for all' solution, and considering the basic principles of the GDPR that are visible, for example, in a risk-based approach, the controller is required to carefully analyse each operation in order to ensure that data is processed safely and lawfully.

4. The ability and requirements to identify digital threats

The question which needs to be answered in this part is whether an individual will at any point be obliged to use specific technologies to exercise his or her rights and freedoms, or will have obligations imposed on him or her to communicate with public and private organizations through ICT. Unlike obtaining a driving licence, the use of both hardware and software to perform various types of activities that produce legal effects is not, in principle, subject to a need for the user to obtain any 'certificate of skill'. Thus in practice, it is irrelevant whether a person knows how to operate the available (and changing) applications (or an aggregate of applications). It is the same with the ability to consciously understand the content of regulations and secu-

rity policies (including user manuals), as well as even verification of the functionality of the equipment and systems one owns. For most people, concepts such as phishing, deepfakes, whaling, spoofing, spearphishing cryptojacking and typosquatting are unknown. Even if some users are aware of the threats, mechanisms such as homoglyphs and homographs, typosquatting, bitsquatting and punycode are completely incomprehensible and, even if generally known, difficult to identify within the daily use of available ICT systems (ETSI, 2023; Szurdi, 2020).

Apart from the specific knowledge and ability needed to understand the mechanisms behind ICT and its threats, there is also a question of an individual having the conditions (including the economic conditions) to acquire the necessary equipment and relevant software at all. This also includes access to software and applications which were introduced based on national regulations. Secondly, it becomes important to specify how to create a presumption that such a person has (or has acquired) the necessary digital competence. This approach, moreover, involves the necessity of adopting a model for defining the permanence of such competencies and assessing the timeliness of their actual existence (van Dijk, 2005).

Even if we assume that it is now no longer possible to talk about mass digital exclusion (understood as a lack of access to appropriate hardware, software or the internet; compare Avgerou & Madon, 2005), there is a strongly questionable presumption about the average user's ability to identify risks in the use of available information technology. It is also difficult to unequivocally define what the standard of 'due diligence' includes, the preservation of which by an individual would be tantamount to the recognition that he or she will not suffer the negative consequences of being misled. Consequently, it is not possible to make a presumption based on the recognition that we are already dealing with a properly formed information society; such a presumption is tantamount to saying that any digital technology that is imposed on an individual in the form of an obligation to use it has been adequately and appropriately prepared for its secure use. It is therefore not sufficient for an entity implementing and using certain solutions to prove that it has conducted a complete risk-management process aimed at identifying system assets, corresponding vulnerabilities and threats, the likelihood of their occurrence and the magnitude of potential loss. The risk analysis must be combined with the presentation of a developed standard of user 'training'.

5. Identification, authentication and authorization

The dynamic implementation of technology is significantly improving the functioning not only of the state, but especially of many private organizations (including, of course, NGOs of various kinds). This is because it involves the omission of what was considered a standard only a dozen years ago, namely personal (physical) par-

ticipation in the act performed in order to effectively ensure that certain effects arising from it are produced. This physical participation was, of course, associated with the appropriate demonstration (confirmation) of one's identity (authorization and/or power of attorney), which made it possible to confirm that it is done by the right person and indeed the one authorized to do so. Of course, there were cases of fraud, although their scale was limited, not only because of the possibility of easier detection, but primarily because of the complex sum of actions that had to be taken to impersonate another person. Technological developments that allow an interested party to effectively carry out various types of legal actions at a distance have revolutionized the model of personal participation and direct identification, allowing – as is widely accepted – their effective performance to be streamlined, simplified and facilitated. Consequently, the identification and verification of data on the spot, during personal contact between individuals, has largely been replaced by identification, authentication and authorization processes. These use a range of different types of personal data that, to the extent that they eliminate any doubt, confirm and effectively verify not only the identity but also the legitimacy of the user to use specific resources or participate in a specific action. The essence of authentication, consisting in the verification of the identity of a specific user, may include various solutions, e.g. login and password, fingerprint, behavioural biometrics and so on. Each of these techniques involves the prior acquisition of personal data, which will be a component of the verification process. The obliged party, while conducting his or her business diligently, has the opportunity to properly organize him – or herself in terms of satisfying all the requirements that are associated with the proper acquisition and subsequent processing of information. However, in order for this to occur, consistent procedures must be in place, the purpose of which is to conjugate the activities undertaken at various organizational and technical levels.

A kind of paradox of the processes of identification, authentication and authorization is that in many cases, they are combined with the acquisition by controllers of various types of personal data. These are not only classic data (first name, last name, ID data, home address, date of birth, etc.), but also biometric data. The assumption is that these data, being unique, guarantee that impersonation does not occur. It should be assumed that the definition of the obligation to transfer this type of data at the level of the individual–state relationship must be adequately anchored in the provisions of generally applicable law.

The entity acquiring certain personal data while implementing specific technical (as well as technological) solutions cannot act arbitrarily or define the circumstances justifying the necessity or indispensability of their processing. Proving a lack of alternative solutions leading to the achievement of the intended purpose requires the demonstration of a risk analysis carried out beforehand, based on objective criteria and premises (also from the perspective of a newly implemented procedure for data processing and the performance of a data protection impact assessment). This assess-

ment demonstrates that the viable and effective standard measures applied to date have not achieved the intended effect, and in principle there are no alternative (less intrusive) measures that could secure authorization.

The resources of public and private organizations include a lot of data, such as copies of signatures, images, locations, digital copies of voices or other specific personal data (ranging from names, identity document data, personal identification transmission data, location data and others), the use of which was not previously identified with a real threat (e.g. posting a video on the internet can be used to create a digital deepfake). The risk identification must therefore take the form of a 'backward-looking' mechanism, in the sense that it becomes necessary to verify the protection of what is currently being transmitted as information, what can be used for possible deception in the context of identification, authentication and authorization, and how.

Even well-organized organizations have so far failed to implement even basic anti-deepfake procedures, because it turns out that even the various possibilities of impersonating a device identified as authorized to participate in communications (whether by using an identical IP, etc., or a duplicate SIM card, as part of the procedure outlined by the operator) have not resulted in the implementation of a separate obligation to authenticate the participant in the communication and a two-level authentication of decisions made during this type of contact (the concept of two independent decision-making 'centres' using separate information (documentation) paths).

6. Postulates de lege ferenda: The paradox of improving identification, authentication and authorization procedures

There is also no doubt that society is entering an era of a significant evolution in the understanding of information autonomy. This will happen because of the comprehensive acquisition by controllers of information on users of specific devices and software, and primarily because of the profiteering that will be associated with it. After all, the ease, speed and convenience of obtaining a particular access, service or benefit will always induce a potential user to share more information about him – or herself.

We are living in a time when data protection and the use of modern digital technologies is becoming an example of seeking the simplest and, in many cases, the cheapest solutions. Paradoxically, therefore, it turns out that the best ways of identification, authentication and authorization involve the need for an individual to share various types of personal data, including, for example, biometric data. In the opinion of those implementing further information technologies, this data will serve to protect individual freedoms and rights in an appropriate, secure way. At the same time, in the era of the fight against cybercrime, which for several years now has been associated with the formation of the phenomenon of so-called mass surveillance carried out by various types of public institutions (European Union Agency for Fundamental

Rights, 2015) and private entities, it is necessary to realize that the constant development of digital technologies, including AI used for the purpose of facial recognition (Hill, 2023), has had and will have a huge impact on defining the nature and scope of the protection of an individual's privacy (and also the protection of the confidentiality of business secrets).

Realizing that one-factor authentication (by password alone) already seems to be an overly simplistic means of protection, it is therefore worth considering the use of at least two-factor authentication, based, however, not on the use of classic personal data but on a mechanism of security questions or devices generating a special code token, i.e. based, neutral and ad hoc generated data. Building an IT security system on the use of biometric data (biometric authentication) with ever-improving technology is not only insecure but can lead to a minimization of respect for an individual's privacy and of information autonomy more broadly.

Conclusions

The dynamic development of information technologies that has been going on for several decades has significantly influenced (and will fundamentally continue to influence) the redefinition of the content of many previously normatively identified civil liberties and rights. This development, of course, involves among other things the multifaceted identification of user data made available through the use of available digital technologies, understood as a set of mechanisms and ways of implementing digital operations in digital elements and software. The consequence of this process is the emergence of a number of new problematic issues, primarily related to ensuring adequate protection of the information autonomy guaranteed to every person. Introducing additional authentication methods should not involve processing extra categories of personal data (especially sensitive ones), as this may lead to infringement in the field of information autonomy. Instead, two-factor identification mechanisms should rely on either generating special codes and tokens or answering specific predefined questions which do not involve the processing of personal data.

REFERENCES

Avgerou, C., & Madon, S. (2005). Information society and the digital divide problem in developing countries. In J. Berleur & C. Avgerou (Eds.), *Perspectives and policies on ICT in society* (pp. 205–218). Springer. http://eprints.lse.ac.uk/2576/1/Information_society_and_the_digital_divide_problem_in_developing_countries_(LSERO).pdf

de Andrade, N. N. G. (2011). Data protection, privacy and identity: Distinguishing concepts and articulating rights. In S. Fischer-Hübner, P. Duquenoy, M. Hansen, R. Leenes, & G. Zhang (Eds.), *Privacy and identity management for life* (pp. 90–107). Springer. https://doi.org/10.1007/978–3-642–20769-3_8

de Gregorio, G. (2022). *Digital constitutionalism in Europe: Reframing rights and powers in the algorithmic society*. Cambridge University Press.

Dunaj, K. (2023). Unijne standardy ochrony prawa do prywatności w obszarze cyberbezpieczeństwa, *Kwartalnik Prawa Międzynarodowego*, *3*, pp. 17–19.

Eskens, S. (2020). The personal information sphere: An integral approach to privacy and related information and communication rights. *Journal of the Association for Information Science and Technology*, *71*(9), 1116. https://doi.org/10.1002/asi.24354

ETSI. (2023). *Group report. Securing artificial intelligence (SAI): Automated manipulation of multimedia identity representations* (*ETSI GR SAI 011 V1.1.1 (2023–06)*). ETSI. https://www.etsi.org/deliver/etsi_gr/SAI/001_099/011/01.01.01_60/gr_SAI011v010101p.pdf

European Commission. (2021, 21 April). Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM(2021)206 final. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206

European Data Protection Supervisor. (2024, 24 January). *Opinion 8/2024 on the proposal for a regulation amending Regulation (EU) 2021/1232 on a temporary derogation from certain eprivacy provisions for combating CSAM*. https://www.edps.europa.eu/system/files/2024–01/2023–1261_d0219_opinion_en.pdf

European Parliament and European Council. (2016, 27 April). Regulation (EU) 2016/679 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data and Repealing Directive 95/46/EC (O. J. L 119, 2016).

European Parliament and European Council. (2016, 6 July). Directive EU 2016/1148 on Measures for a High Common Level of Security of Networks and Information Systems within the Union (O. J. L. 194, 2016).

European Parliament and European Council. (2016, 26 October). Directive (EU) 2016/2102 on the Accessibility of Websites and Mobile Applications of Public Sector Bodies (O. J. L 327, 2016).

European Parliament and European Council. (2022, 14 December). Directive (EU) 2022/2555 on Measures to Promote a High Common Level of Cyber-Security within the Union, Amending Regulation (EU) no. 910/2014 and Directive (EU) 2018/1972 and Repealing Directive (EU) 2016/1148 (NIS Directive 2) (O. J. L. 333, 2022).

European Parliament and European Council. (2022, 14 December). Regulation (EU) 2022/2554 on Operational Digital Resilience of the Financial Sector and Amending Regulations (EC) no. 1060/2009, (EU) no. 648/2012, (EU) no. 600/2014, (EU) no. 909/2014 and (EU) 2016/1011.

European Parliament and European Council. (2023, 31 May). Regulation (EU) 2023/1114 on Cryptocurrency Markets and Amending Regulations (EU) no. 1093/2010 and (EU) no. 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937.

European Parliament. (2021, April 22). *Shaping the digital transformation: EU strategy explained*. https://www.europarl.europa.eu/topics/en/article/20210414STO02010/shaping-the-digital-transformation-eu-strategy-explained

European Union Agency for Fundamental Rights. (2015). *Surveillance by intelligence services: Fundamental rights safeguards and remedies in the European Union*. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-surveillance-intelligence-services-summary_en.pdf

Grzelak, A., & Zielińska, K. S. (2021). Między prawem do prywatności i ochrony danych osobowych a zapewnieniem bezpieczeństwa publicznego i walką z przestępczością. Problemu retencji danych ciąg dalszy – glosa do wyroków Trybunału Sprawiedliwości z 06.10.2020 r.: C 623/17, Privacy International, oraz w sprawach połączonych C-511/18, C-512/18, C-520/18, La Quadrature du Net i in. *Europejski Przegląd Sadowy*, *7*, 26–36.

Hill, K. (2023). *Your face belongs to us: The secretive startup dismantling your privacy*. Simon & Schuster.

Jabłonowska, A., & Tagiuri, G. (2023). Rescuing transparency in the digital economy: In search of a common notion in EU consumer and data protection law. *Yearbook of European Law*, *42*, 347–387.

Jabłoński, M., & Węgrzyn, J. (2023). Consumer protection in the EU law and the constitution of the Republic of Poland: General comments. In J. Cremades & C. Hermida (Eds.), *Encyclopedia of contemporary constitutionalism* (pp 2–14). Springer.

Judgment of the CJEU of 9 November 2010 on the case of *Volker und Markus Schecke*, C 92/09.

Judgment of the CJEU of 4 April 2014 on the joined cases of *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, the Attorney General*, C 293/12, and *Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others*, C 594/12.

Judgment of the CJEU of 21 December 2016 on the joined cases of *Tele2 Sverige AB v. Post – och telestyrelsen and Secretary of State for the Home Department v. Tom Watson, Peter Brice, Geoffrey Lewis*, C 203/15 and C 698/15.

Judgment of the CJEU of 6 October 2020 on the joined cases of *La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à internet associatifs, Igwan.net v. Premier ministre, Garde des Sceaux, Ministre de la Justice, Ministre de l'Intérieur, Ministre des Armées oraz Ordre des barreaux francophones et germanophone, Académie Fiscale ASBL, UA, Liga voor Mensenrechten ASBL, Ligue des Droits de l'Homme ASBL, VZ, WY, XX v. Conseil des ministers*, C 511/18, C 512/18 and C 520/18.

Judgment of the Polish Constitutional Tribunal of 9 July 2009, no. SK 48/05.

Judgment of the Polish Constitutional Tribunal of 26 February 2014, no. K 22/10.

Judgment of the European Court of Human Rights of 2 August 1984 on the case of *Malone v. UK*, application no. 8691/79.

Judgment of the European Court of Human Rights of 16 December 1992 on the case of *Niemietz v. Germany*, application no. 13710/88.

Judgment of the European Court of Human Rights of 16 February 2000 on the case of *Amann v. Switzerland*, application no. 27798/95.

Judgment of the European Court of Human Rights of 4 May 2000 on the case of *Rotaru v. Romania*, application no. 28341/95.

Judgment of the European Court of Human Rights of 16 April 2002 on the case of *Société Colas Est et al. v. France*, application no. 37971/97.

Judgment of the European Court of Human Rights of 28 January 2003 on the case of *Peck v. United Kingdom*, application no. 44647/98.

Judgment of the European Court of Human Rights of 20 March 2007 on the case of *Tysiąc v. Poland*, application no. 5410/03.

Judgment of the European Court of Human Rights of 4 December 2015 on the case of *Zakharov v. Russia*, application no. 47413/06.

Judgment of the Polish Constitutional Tribunal of 19 February 2002, no. U 3/01.

Judgment of the Polish Constitutional Tribunal of 23 june 2009, no. K 54/07.

Judgment of the Polish Constitutional Tribunal of 22 july 2014 r., no. K 25/13.

Kuźnicka, D. (2017). Dyskryminacja w zakresie dostępu do informacji publicznej a widzialność stron internetowych administracji. *Przegląd Prawa Konstytucyjnego*, *38*(4), 175–194. https://doi.org/10.15804/ppk.2017.04.09

Milczarek, E. (2020). *Prywatność wirtualna. Unijne standardy ochrony prawa do prywatności w internecine*. Beck.

Rise, M. (2018, May). *Human rights and artificial intelligence: An urgently needed agenda* [HKS faculty research working paper series RWP18–015], https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://appext.hks.harvard.edu/publications/getFile.aspx%3FId%3D1664&ved=2ahUKEwiPteSAj7CQAxXyc_EDHSVmE8kQFnoECBYQAQ&usg=AOvVaw2Xau_yNlWokYm7Pjk7WqLq

Roagna, I. (2012). *Protecting the right to respect for private and family life under the European Convention on Human Rights*. Council of Europe, Strasbourg.

Safjan, M. (2014). O różnych metodach oddziaływania horyzontalnego praw podstawowych na prawo prywatne. *Państwo i Prawo*, *2*, 3–33.

Supreme Court of the United States. (2018). *Brief of Privacy International, human and digital rights organizations and international legal scholars as amici curie in support of respondent – United States v. Microsoft Corp., 584 US, no. 17–12.* https://www.supremecourt.gov/DocketPDF/17/17–2/28354/20180118170547648_17–2%20USA%20v%20Microsoft%20Brief%20of%20Privacy%20International%20Human%20and%20Digital%20Rights%20Organizations%20and%20International%20Legal%20Scholars%20as%20Amici%20Curiae%20in%20Support%20of%20Respondent.pdf

Szurdi, J. (2020). *Measuring and analysing typosquatting toward fighting abusive domain registrations* [Doctoral dissertation, Carnegie Mellon University]. https://janos.szurdi.com/content/thesis/jszurdi-phd-thesis.pdf

van Dijk, J. (2005). *The deepening divide: Inequality in the information society*. Sage.

Webster, F. (2014). *Theories of the information society* (4th ed.). Routledge.

Yang, L., Li, J., Pricket, T., & Chao, F. (2019). Towards big data governance in cybersecurity. *Data-Enabled Discovery and Applications*, *3*, 10. https://www.researchgate.net/publication/337692258_Towards_Big_data_Governance_in_Cybersecurity

Bialystok Legal Studies
Białostockie Studia Prawnicze
2025 vol. 30 no. 4

sciendo

DOI: 10.15290/bsp.2025.30.04.11

Received: 23.09.2025
Accepted: 13.11.2025

Halina Sierocka
University of Bialystok, Poland
h.sierocka@uwb.edu.pl
ORCID ID: 0000–0002–6930–6409

Legal and Ethical Issues Related to the Use of Artificial Intelligence in the Field of Justice[1]

Abstract: The rapid development of artificial intelligence (AI) has created many opportunities in various areas of human life, such as facilitating healthcare and education, improving production processes and creating labour efficiencies, or enabling human connections through social media, to name a few. Even though AI technology can be of excellent service to humanity, it also risks embedding biases which result in discrimination and inequality, as well as violations of human rights and fundamental freedoms, which, not surprisingly, raise numerous legal and ethical concerns. Given these issues, this paper endeavours to provide some insights into the application of artificial intelligence in the judiciary and to answer some questions which might be posed in this context: Are AI algorithms capable of simulating judicial decision-making? Can legal and ethical standards characteristic of the judicial function be maintained when AI tools are employed in the field of justice? The main highlights of the paper refer to the shaping of the legal framework in the AI area, compliance with ethical guidelines and recommendations, and risks and biases created and embedded by AI algorithms, as well as the issue of transparency towards both parties and the public, and in the area of AI algorithmic reasoning and methods. The paper concludes with some examples of national case law from courts' decisions on AI from five EU Member States, which provide specific case background for the issue in question.

Keywords: artificial intelligence, bias, ethics, human rights, judiciary

Introduction

1 The article is financially supported by the Polish Minister of Science under the 'Regional Initiative of Excellence' (RID) programme.

Defining AI is difficult due to the complexity of the issue. While numerous scholars have endeavoured to define the concept, others have cast doubt on whether it is possible to do so at all due to the rapid changes which affect this area. A full discussion of the notion of AI lies beyond the scope of this study; however, two definitions are worth mentioning. John McCarthy, considered the inventor of AI, and his collaborators describe AI in their study 'A proposal for the Dartmouth summer research project on artificial intelligence' as 'allowing a machine to behave in such a way that it would be called intelligent if a human being behaved in such a way' (2016, p.1). As Reiling highlights in this context, 'it is important to establish, defining human intelligence as the measure of what AI does' (2020). Intelligence as such can be 'the ability to reason abstractly, logically and consistently, discover, lay and see through correlations, solve problems, discover rules in seemingly disordered material with existing knowledge, solve new tasks, adapt flexibly to new situations, and learn independently, without the need for direct and complete instruction' (Reiling, 2020). For this paper, I will adopt the definition proposed by UNESCO's Recommendation on the Ethics of Artificial Intelligence, which suggests a dynamic understanding of AI; it interprets AI broadly as a system with the ability to process data in a way that resembles intelligent behaviour. This definition is fairly general, but this is an advantage, as the rapid pace of technological advancement would quickly make any fixed and narrow definition outdated and hence make adopted policies unfeasible.

To understand the way AI works, it is important to realise that this sophisticated software, which is programmed to automate routine, generally involves Machine Learning (ML), i.e. a subset of AI which focuses on enabling machines to 'learn' how to perform certain tasks and improve with human direction and feedback. In turn, as Heshmaty (2022) explains, it uses Natural Language Processing (NLP) software that can understand written and spoken commands from people who may not have any computer programming knowledge, and this combination of AI, ML and NLP enables people who do not understand computer codes to interact with and train the software to assist them in their study, work or hobbies.

As was mentioned above, AI has evolved greatly; it is everywhere and affects everyone, and not surprisingly its relevance to and impact on the justice system have become particularly significant. The literature on this subject is not yet particularly extensive, but it is growing rapidly, along with the abundance and variety of research problems. They cover such issues as the impact of AI on ethics, human rights, democracy and the rule of law (Franguloiu, 2023; Guitton et al., 2025; John et al., 2023; Josten, 2023; Moore et al., 2025; Muller, 2020), the role of AI in the judiciary (Cabrera et al., 2024; Kuo, 2024; Yu, 2022), the application of AI in the criminal justice system (Jadhav et al., 2020; Shi, 2022; Simmons, 2018; Stănilă, 2020; Watamura et al., 2025) or judges' perception of AI as well as judges using AI in their decision-making process (Fine et al., 2025; Yalcin et al., 2023). The importance of AI is also reflected in

numerous initiatives and actions taken, as well as the laws adopted in recent years to regulate the issue, which will be presented in detail in the following section.

1. Shaping the legal framework for AI

On 16 December 2024 the Council of the European Union (Justice and Home Affairs) approved a set of conclusions on the use of artificial intelligence in the field of justice, which include the most significant documents in the area:

- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (the AI Act) is the first comprehensive legislative instrument in the world to regulate AI. It classifies AI systems for certain applications in the fields of justice, law enforcement and alternative dispute resolution as high risk, and subjects them to a set of requirements, such as conformity assessment procedures and controls, with a view to ensuring a high level of trustworthiness. The main priority was to make sure that AI systems used in the EU are transparent, safe, traceable, non-discriminatory and environmentally friendly;
- A number of conclusions by the Council of the European Union which address the issue of digitalisation, i.e.:
  - the Council Conclusions of 9 June 2020 on shaping Europe's digital future, which drew attention to the challenges created by increased digitalisation in the European economy and society, including by AI;
  - the Council Conclusions of 13 October 2020 on digitalisation on 'Access to justice – seizing the opportunities of digitalisation', which stressed the importance of the digital transition in increasing the effectiveness and efficiency of justice systems;
  - the Council Conclusions of 20 October 2023 on digital empowerment to protect and enforce fundamental rights in the digital age, which concern the digital empowerment of individuals and sectors that are key for the defence of fundamental rights, such as justice, as well as the construction of a safe digital environment where fundamental rights are properly protected;
  - the Council Conclusions of 5 March 2024 on the application of the EU Charter of Fundamental Rights, which promote trust through effective legal protection and access to justice, including by 'seizing the opportunities of digitalisation'.

The conclusions also enumerate several other documents adopted by numerous international organisations which might constitute significant input in shaping the legal framework for the application of AI in the judiciary. Those that address ethics,

bias, discrimination or protection of human rights, democracy and the rule of law are particularly worth mentioning:

- the European Commission for the Efficiency of Justice (CEPEJ) of the Council of Europe's European Ethical Charter on the use of artificial intelligence in judicial systems and their environment, alongside related guidelines by CEPEJ on the use of AI in the judiciary;
- the UN Human Rights Council Resolution of 10 July 2024 on the promotion and protection of all human rights and civil, political, economic, social and cultural rights, including the right to development, especially its provisions on the independence and impartiality of the judiciary, jurors and assessors, and the independence of lawyers;
- the Council of Europe framework convention on artificial intelligence and human rights, democracy and the rule of law, opened for signatures on 5 September 2024, which aims to ensure that the activities within the lifecycle of AI systems are fully consistent with the protection of human rights, democracy and the rule of law, while being conducive to technological progress and innovation; it has also been emphasized that this first internationally binding treaty on AI aims to fill any legal gaps that may result from rapid technological advances, however it does not aim to regulate technology to stand the test of time;
- the reports prepared by the European Union Agency for Fundamental Rights, such as 'Getting the future right: Artificial intelligence and fundamental rights' and 'Bias in algorithms: Artificial intelligence and discrimination'.

Artificial intelligence was and still is a challenge not only for legislatures but also for the judiciary. Undoubtedly, AI can strengthen access to justice and make judicial administration more efficient; however, it needs to be governed with care, especially in areas such as transparency, human rights or ethical concerns like bias, discrimination and privacy. In that vein, the role of the judiciary cannot be overestimated. However, for most judiciaries, AI is a new concept too, thus guidelines are strongly desired. According to the UNESCO (2024) Global Judges' Initiative, a survey on the use of AI systems by judicial operators, 44% of respondent judges use ChatGPT and other AI tools for work purposes. However, only 9% of them receive training or have institutional guidelines at work. In response to this need, some countries, such as Brazil (2020), Canada (2023), New Zealand (2023) and the United Kingdom (2023), have already issued guidelines for the use of generative artificial intelligence in courts and tribunals. It is worth mentioning UNESCO's initiatives in more detail here, as they approach the problem in a more comprehensive way.

On the basis of the Recommendation on the Ethics of Artificial Intelligence adopted in 2021 by 193 UNESCO Member States, the programme called Artificial Intelligence and the Rule of Law was launched in 2022, which aimed to engage stakeholders within justice systems in a global discussion on the applications of artificial

intelligence and its impact on the rule of law. One of the practical outcomes is the Global Toolkit on AI and the Rule of Law for the Judiciary, which is intended as a curriculum to serve national judicial training institutions, universities and other legal education organisations offering training. Moreover, a Global Network of Experts on AI and the Rule of Law was established within the programme, an interdisciplinary group of experts (both academics and practitioners) which provides technical assistance and training to judiciaries worldwide, hence supporting the responsible adoption and governance of AI technologies.

In addition, in response to the aforementioned survey, respondents strongly supported mandatory regulations and training on AI use in judicial activities, with 92% calling for such measures. UNESCO has thus started to develop guidelines for the use of AI systems in courts and tribunals, based on the UNESCO Recommendation. These guidelines are to provide guidance both for the organisations of the judiciary and for individuals, to make sure that AI technologies are adopted in alignment with justice, human rights and the rule of law. A special emphasis is put on the protection of human rights, especially in the context of personal data protection, proportionality, non-discrimination, accountability and legality. It is highlighted that courts and tribunals exploiting AI for their work are strongly recommended to use the principle of proportionality and necessity, together with algorithmic impact assessment tools. They are recommended to disclose key information about the AI systems used by the judiciary, i.e. what AI systems are adopted, how they operate and how they are used. In addition, the guidelines demonstrate the need for establishing internal procedures as regards access to the appropriate training, risk management systems or cybersecurity measures. Individuals (i.e. judges, prosecutors, judicial officers and judicial support staff), on the other hand, are advised to use tools that are tested and approved, to always verify outputs and to disclose the use of GenAI systems for drafting rulings, opinions and other documents that may bear legal consequences. It has also been emphasised that they should avoid overreliance on AI tools while making substantive decisions.

2. Challenges of the use of artificial intelligence in the field of justice in the light of legal and ethical standards

The development of artificial intelligence raises novel issues and profound concerns for which current legal systems are only partially prepared. These include questions of rights, freedoms and ethics. Some questions might be posed here: To what extent can AI tools assist the judiciary in the administration of justice? Are AI algorithms capable of simulating judicial decision-making? Can the legal and ethical standards inherent in the judicial function be maintained when AI tools are exploited

in the process? The questions arise from the potential AI systems have to reinforce bias and put human rights at risk.

The awareness of EU lawmakers that the use of AI systems might have a detrimental impact on people's health, safety and fundamental freedoms and rights resulted in the risk-based AI classification system in the AI Act. The AI systems that can be exploited in various applications are analysed and classified according to the risk they pose to users. The Act introduces different provisions for different risk levels, thus providing AI compliance requirements. The classification system identifies four different risk categories: unacceptable risk, high risk, transparency risk and minimal to no risk. The first group includes AI tools which are banned and refers to:

- the cognitive behavioural manipulation of people or specific vulnerable groups, i.e. voice-activated toys that incite dangerous behaviour in children;
- social-scoring AI, i.e. classifying people based on behaviour, socioeconomic status or personal characteristics;
- the biometric identification and categorisation of people;
- real-time and remote biometric identification systems, such as facial recognition in public spaces.

However, for law enforcement purposes and to prosecute serious crimes, the Act provides for some exceptions as regards real-time and remote biometric identification systems.

The category of 'high-risk' AI systems concerns tools that might affect safety and fundamental rights. They include:

- AI systems that are used in products falling under the EU's product safety legislation, such as toys, aviation, cars, medical devices and lifts;
- AI systems that fall into specific areas that require registration in EU databases, i.e. the management and operation of critical infrastructure, education and vocational training, employment, worker management and access to self-employment, access to and enjoyment of essential private services, public services and benefits, law enforcement, migration, asylum and border-control management, assistance in legal interpretation and application of the law.

Moreover, all high-risk AI tools will be subject to assessment both before them being made available on the market and throughout their life cycle. The Act also provides for the possibility to file a complaint about AI systems to respective national authorities.

Transparent-risk AI systems (generative AI), like ChatGPT, are not classified as high risk but will have to comply with transparency requirements and EU law. This means informing users that the content was generated by AI, designing the model to prevent it from generating illegal content and publishing summaries of copyrighted data used for training, as well as labelling content that is either generated or modified with the help of AI, like images, audio or video files (e.g. deepfakes), as AI-generated.

As mentioned before, AI technology can be of great service to humanity, but without ethical standards it risks embedding biases that result in discrimination and inequality, as well as violations of human rights and fundamental freedoms. Recognising the importance of this problem, more than 25 international institutions have addressed the issue of ethical standards for the application of AI systems in court practice. As their content overlaps, and due to practical constraints, only two main instruments will be described here in more detail.

In 2018 the European Commission for the Efficiency of Justice (CEPEJ) of the Council of Europe, adopted the first European text setting out ethical principles relating to the use of artificial intelligence in judicial systems. The main highlights are:

- ensuring that the design and implementation of artificial intelligence tools and services are compatible with fundamental rights (Principle of respect of fundamental rights);
- preventing the development or intensification of any discrimination between individuals or groups of individuals (Principle of non-discrimination);
- using certified sources and intangible data with models conceived in a multi-disciplinary manner, in a secure technological environment (Principle of quality and security: with regard to the processing of judicial decisions and data);
- making data processing methods accessible and understandable, authorising external audits (Principle of transparency, impartiality and fairness);
- precluding a prescriptive approach and ensuring that users are informed actors and in control of their choices (Principle 'under user control').

Another document worth mentioning is UNESCO's Recommendation on Ethics and Artificial Intelligence, adopted in 2021. This comprehensive instrument makes a strong call to governments around the world to establish the necessary institutional and legal frameworks to ensure ethical standards for AI technologies, in full respect of international law and in particular human rights law. The protection of human rights and dignity is the cornerstone of the Recommendation, which is reflected in a human rights-centred approach to the ethics of AI. The document introduces ten principles:

1) *Proportionality and do no harm* – AI systems cannot be used beyond what is necessary to achieve a legitimate aim, and the risk should be assessed to prevent harms which may result from such uses;
2) *Safety and security* – AI actors, i.e. anybody involved in any stage of the AI life cycle (from research through development and use to disassembly and termination), should avoid unwanted harm and the danger of attack;
3) *Right to privacy and data protection* – privacy must be protected and promoted through the AI life cycle;
4) *Multi-stakeholder and adaptive governance and collaboration*;

5) *Responsibility and accountability* – AI tools should be auditable and traceable, i.e. there should be oversight, impact assessment, audits and due diligence mechanisms to avoid violations of human rights norms; for example, if when someone applies for a loan, the bank uses AI to make an automated assessment of their finances, and if the decision is taken without human oversight and accountability, the consequences might be significant – the system may make a mistake, and there is nobody who can take responsibility for the decision, hence appeals are in fact not possible.
6) *Transparency and explainability* – the ethical implementation of AI tools should be based on their transparency and explainability, which means that people should be aware that the decision is taken by AI and that the logic behind the algorithmic decision-making can be fully interpreted by experts and be explained to users in accessible language. The term 'black box' has been used to describe AI systems that are opaque and hard to interpret.
7) *Sustainability*;
8) *Human oversight and determination* – AI systems should not displace ultimate human responsibility and accountability;
9) *Awareness and literacy*;
10) *Fairness and non-discrimination* – social justice, fairness and non-discrimination should be promoted, while taking an inclusive approach to ensure AI's benefits are accessible to all.

It is worth mentioning that apart from values and principles which are crucial to establishing a basis for any ethical AI framework, the Recommendation also sets out key areas for policy actions where ethics play an important role. They include ethical impact assessments, ethical governance and stewardship, gender equality, data policy, development and international cooperation, education and research, culture, labour markets, the environment and ecosystems, communication and information, health and social being, and the economy. Overall, all the documents refer to the five key aspects of ethical standards for the use of AI in the judiciary: AI under user control, respect for fundamental rights, equal treatment, data security and transparency.

An important aspect highlighted by some researchers (e.g. Reiling, 2020) and lawmakers / institutions (e.g. the CEPEJ principle) is to have AI under user control, which means that the algorithm may not be used as a prescription, i.e. the AI system cannot prescribe anything and cannot decide by itself. Users must know and understand what the AI does and must be in control of the decisions they make, meaning that they must be able to 'deviate from the outcome of the algorithm without difficulty' (Reiling, 2020). In her article, Reiling provides a striking example of what can happen when an AI system is relied on blindly. In the UK, a piece of IT determines the financial capacity of (ex-)spouses in maintenance proceedings; the parties fill in a form and the AI tool cal-

culates their capacity. As a result of a small, unnoticed mistake, calculations were made wrongly in 3,638 cases (between April 2011 and January 2012, and between April 2014 and December 2015). The assets taken into account were too high, as, instead of being deducted, debts had been added. In the pending cases, this could be and was corrected, but more than 2,200 wrong decisions were issued.

The human oversight of AI-created output is of paramount importance when the AI technology is exploited in the judicial decision-making process. Within this context, so-called predictive justice tools (the AI tools used for the assessment and prediction of possible litigation outcomes) raise serious ethical concerns, which are reflected in numerous provisions. To quote just one of these, Article 22(1) of the General Data Protection Regulation 2016/679 (GDPR) states that: 'The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.' Predictive tools are attracting a lot of attention because they claim to be able to reduce the risk of an unpredictable litigation outcome. The more complex a case becomes with additional information and circumstances, and the more the risk increases, the more desirable the AI tool becomes. According to a report by the European Commission for the Efficiency of Justice, predictive justice tools are more popular in the United States than in the EU; however, as they are offered commercially (and the owners/creators are reluctant to share their business secrets), not much is known about how they operate. Below are some examples of predictive justice tools introduced to the judiciary, along with the risks they may pose.

Lex Machina and Solomonic are two commercial products that use AI to filter thousands of court judgments available online to help lawyers predict the outcome of cases by analysing vast collections of historical judgments, looking at the facts of each specific case and the decisions made by the judge. As the creators claim, the AI system can reduce the likelihood of wasting time and money on going to trial where a case is unlikely to succeed, can help lawyers decide on the best settlement and can generally reduce risk when developing litigation strategies. Nevertheless, AI systems are not able to explain exactly *why* certain litigation strategies are more successful than others. It is often seen as (de)coding justice, i.e. translating law into code without considering unpredicted circumstances or re-examination in the light of social change. Interestingly enough, both systems are known to be misused by legal professionals and are forbidden in some countries (for example in France).

Across the world, judges, prosecutors and court staff are increasingly exploiting various risk-assessment algorithms to assess a criminal defendant's likelihood of becoming a recidivist. The tools furnish judges with information on pre-trial bail, sentencing and parole, suggesting who can be released at each stage of the criminal proceedings. One of the most commonly exploited pieces of risk-assessment software in the US, developed especially for courts, is the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS). On the basis of 137 questions an-

swered by the offender during interview and on the information obtained from their criminal history, and taking into account criminological factors such as socioeconomic status, family background and employment, etc., the algorithm provides a report on a calculated risk score (1 to 10), categorising the offender as at high, medium or low risk of re-offending. In Eric Loomis's case, the Wisconsin Supreme Court highlighted the need for cautious use of COMPAS, particularly arguing that 'studies have raised questions about whether COMPAS scores disproportionately classify minority offenders as having a higher risk of recidivism' (Papp et al., 2022).

Another interesting example, described by Kravetz (2014), refers to a machine-learning application developed by a group of American academics chaired by Josh Blackman, a South Texas College of Law scholar, which claims to be able to predict, with 70% accuracy, whether the US Supreme Court (SCOTUS) will uphold or reverse the lower-court decision before it. The AI tool is even more accurate when it comes to the voting behaviour of individual judges (71.9%). Blackman went even further, wondering whether humans are more accurate than an algorithm, and created FantasySCOTUS, a Supreme Court 'Fantasy League' where attorneys, law students and other Supreme Court followers make predictions about cases before the Supreme Court. Interestingly enough, some FantasySCOTUS participants hit a 75% accuracy level.

Aletras et al. (2016) present in detail another AI application which claims to be capable of predicting the decisions of the European Court of Human Rights (ECHR) with even 79% accuracy. This AI system exploits NLP and ML to forecast whether or not in a particular case the ECHR will adjudicate on the violation of a particular provision of the European Convention on Human Rights. The scholars observed that the most important part of 'obtaining on average the strongest predictive performance of the Court's decision outcome' is the information on the factual background of the case as it is formulated by the Court in the respective part of its judgment. The AI system recognises the patterns in a text document and can thus quickly identify in which direction a judgment could go. It is important to remark here that the study was not free from some limitations, like data access issues: the tool only used the data obtained from earlier HUDOC judgments, which are easily and freely available. Other kinds of data (such as the texts of individual applications, briefs submitted by parties, domestic judgments or inadmissible requests) were not included in the study due to limited or no access.

Another serious concern in terms of the ethical use of AI systems relates to preserving equal treatment and avoiding discrimination between individuals or groups of individuals. In fact, we can claim that AI systems may reinforce salient inequalities embedded in structures of prevailing patterns of social behaviour under the cover of impersonal impartiality and rational objectivity. The next example shows that bias and discrimination between individuals and groups are a real risk, and errors the AI makes concern one social group more frequently than another, particularly in areas such as asylum, social protection benefits, family disputes and sanctioning. The study

in question was conducted in 2016 by ProPublica, a non-profit investigative journalism organisation, which assessed COMPAS, mentioned above, to reveal the underlying accuracy of their recidivism algorithm and to examine whether the algorithm was biased against certain groups of individuals (Larson et al., 2016). The study looked at more than 10,000 criminal defendants in Broward County, Florida, and compared their predicted recidivism rates with the rate that occurred over two years. Most defendants filled in a COMPAS questionnaire when booked into jail; their answers fed into the COMPAS software to generate several scores, including predictions of 'Risk of Recidivism' and 'Risk of Violent Recidivism'. The study showed that COMPAS correctly predicted recidivism 61% of the time, but revealed that black defendants were far more likely than white ones to be incorrectly judged to be at a higher risk of recidivism, while white defendants were more likely than black ones to be incorrectly flagged as low risk.

Prediction Fails Differently for Black Defendants

	WHITE	AFRICAN AMERICAN
Labeled Higher Risk, But Didn't Re-Offend	23.5%	44.9%
Labeled Lower Risk, Yet Did Re-Offend	47.7%	28.0%

Source: Larson et al., 2016

The analysis also indicated that even when controlling for prior crimes, future recidivism, age and gender, black defendants were 45% more likely to be assigned higher risk scores than white ones. As regards violent recidivism, it also showed that even when controlling for prior crimes, future recidivism, age and gender, black defendants were 77% more likely to be assigned higher risk scores than white defendants.

In a society governed by the rule of law, the use of judicial power must be transparent; judges justify their power by providing reasoning for their decisions. The transparency and interpretability of algorithms are low; although most powerful Large Language Model tools operate through multi-dimensional computational space with trillions of computations, their transparency and interpretability are low and in fact lead to paradoxes like the 'opacity paradox' (the more effective an AI tool is, the less transparent and understandable it is to human comprehension) or the 'hallucination paradox' (the more extensive the input data is, the less detectable fake output data is), with little or no guarantee that false correlations are excluded. The inability to explain the reasoning through which an algorithm has reached its output in the form of the verdict, i.e. which facts were given relevance, what evidence was deliberated on and weighted, how relevant legal provisions were prioritised, etc., raises

fair trial concerns, and hence the violation of the fundamental human right that is the right to a fair trial.

Apart from the legal and ethical concerns described above, it needs to be highlighted that AI tools lack reasoning; they neither think nor provide the meaning of the legal texts, and they do not assess the facts and search for the truth – they compute, i.e. calculate, probability and determine correlations and patterns between lexical groups composing judicial decisions, hence de facto reducing reasoning to syntax and pure form. Judges do not compute. They employ all means of human reasoning (mastery of law, formal logic and procedure, human intuition, emotional intelligence, common sense, life experience, etc.) to reach a decision in an individual case that best achieves the purposes of the applicable law, in conformity with fundamental values of the legal order such as fairness, common sense or equality.

3. National case law on decisions on AI

National case law on artificial intelligence is not yet particularly elaborate. Therefore in the context of this study, it is worth presenting those cases that refer to ethical standards relating to the use of artificial intelligence, especially with regard to fundamental rights, the protection of personal data or access to information about data.

3.1. Fundamental rights: The automatic analysis and use of data

In its judgment of 19 February 2023, the Federal Constitutional Court (*Bundesverfassungsgericht*) of Germany held that two statutory provisions of the *Länder* of Hesse and Hamburg are unconstitutional. The provisions in question (§25a(1) (first alternative) of the Security and Public Order Act for Hesse (*Hessisches Gesetz über die öffentliche Sicherheit und Ordnung*) and §49(1) (first alternative) of the Act on Data Processing by the Police for Hamburg (*Hamburgisches Gesetz über die Datenverarbeitung der Polizei*)) authorise the police to process stored personal data either through automated data analysis or automated data interpretation for the prevention of criminal acts. The Court held that in the absence of a sufficient limit on intervention, these provisions violate the general right of personality (Article 2(1) in conjunction with Article 1(1) of the Basic Law (*Grundgesetz*)) in its manifestation, i.e. as the right to informational self-determination. It was underlined that due to the particularly broad wording of the powers, in terms of both the data and the methods concerned, there is a particularly high degree of interference. The method of automated analysis or use is therefore all the more intrusive (it is possible to obtain a wide-ranging and thorough knowledge of data subjects), the risks of errors and discrimination are high and it is difficult to trace the generation of results, therefore there is identifiable danger. The Court decided that §25a(1) (first alternative) of the Hessian Security and Public Order Act continues to apply, subject to some restrictions whereas §49(1) (first alternative) of Hamburg's Act on Data Processing by the Police was declared null and void.

3.2. Protection of personal data: The use of algorithms by the Public Employment Service in Austria

The Austrian Supreme Administrative Court (*Verwaltungsgerichtshof*) examined a case concerning an algorithm used by the Austrian Public Employment Service to assess jobseekers' labour market opportunities; the AI automatically calculates the probability of applicants being employed within a specific period. In its judgment, the Court classed the algorithm (i.e. the calculation of the chances of candidates on the labour market) as profiling under Article 4(4) of the General Data Protection Regulation (GDPR). In its judgment of 21 December 2023, the Court held that an algorithm determining the likelihood of job applicants being hired is prohibited automated decision-making under Article 22 GDPR, even if the result is used exclusively by a public body to provide jobseekers with targeted employment counselling. However, the Court stated that this issue could not be conclusively examined, as the first instance administrative court had not given sufficient findings on the precise use of the AI by the Austrian Employment Service, particularly as regards the procedures and/or other parameters used in the process; it was therefore referred back to the first instance administrative court.

3.3. Data protection: Freedom of opinion and elections

When the Spanish Constitutional Court dealt with the issue of the use of artificial intelligence algorithms in electoral processes, it referred to Article 58(b)(1) of the Organic Law on the General Electoral Regime (LOREG), which allows political parties to collect personal data on political opinions as part of their activities. In its judgment of 22 May 2019, (No 76/2019) the Court declared the aforementioned provision unconstitutional as it could enable political parties to manipulate unaware voters using tailored propaganda that is automatically elaborated based on their profiles. The Court pointed out in its reasoning that the purpose of data processing stated under Article 58(bis) of the LOREG is quite vague (only a generic public interest is mentioned), making a constitutionality check on restrictions to the fundamental right to personal data protection impossible. Moreover, the provision does not provide for clear rules on the conditions of data processing and its limitations. This lack of precision was found to be a violation of legal certainty and of the core of the fundamental right in question. In that light the Court concluded that there are no adequate and precise guarantees to protect the aforementioned right, hence the law does not meet the requirements of certainty and predictability which are indispensable to guarantee the fundamental right to personal data protection. Consequently, the Spanish Constitutional Court held that the provision in question violated Articles 18(4) and 53(1) of the Spanish Constitution.

3.4. Automated decisions: The right of access to information

The Amsterdam Court of Appeal dealt with the case of taxi drivers whose collaboration with Uber Driver was terminated (and consequently their smartphone application deactivated) using an 'automated decision'. The Uber Driver company claimed in that automated decision that the drivers had failed to fulfil their contractual obligations by committing fraud. After analysing the character of the contested decisions, the Court of Appeal, in its judgment of 4 April 2023, held that Uber Driver, in accordance with Article 15(1)(h) of the General Data Protection Regulation, was under the obligation to give the drivers access to information on the existence of the automated decision so that they could defend their rights, as the decisions, along with the allegations of fraud included therein, might have a significant impact on their lives (i.e. lost investments and/or taxi licences). Moreover, the Court highlighted that the decisions were formulated in very general terms, and although Uber Driver claimed that its staff assessed the reported frauds, it failed to prove that there had been human intervention in the process, as the reviews were rather symbolic.

3.5. The protection of personal data: The use of smart video surveillance

On 19 May 2023, France enacted the legal framework for the 2024 Olympic and Paralympic Games (Law no. 2023–380), which includes provisions concerning different areas of the Games. One of the most significant provisions of this law refers to the implementation of enhanced security measures for the 2024 Olympic Games to prevent breaches of public order. Article 10 authorises the enforcement authorities to use intelligent video surveillance facilitated by artificial intelligence, which through 'augmented cameras' might detect 'predefined events' like suspicious behaviour, abandoned bags or crowd movements in real time. Moreover, images collected by authorised video protection systems may be subject to algorithmic processing. It is noteworthy to mention that limitations on the treatment of collected data were explicitly outlined in Article 10, i.e. the use of biometric identification systems, the processing of biometric data and the implementation of facial recognition techniques were prohibited. Interestingly enough, the aforementioned provision was considered by the French Constitutional Council (Conseil Constitutionnel), which in its decision of 17 May 2023 (No. 2023–850 DC 1217) declared that Article 10 of the Olympic and Paralympic Games Act 2024 is compatible with the Constitution. In its unprecedented decision, the Council held that to prevent breaches of public order, which is the constitutional objective, the algorithmic processing of images collected using a video surveillance system or cameras installed on aircraft is legal and valid. It was pointed out that such processing, along with a systematic and automated analysis of the collected images, considerably increases the quantity and precision of the information that can be extracted from them; therefore the implementation of such monitoring systems must be accompanied by specific guarantees to safeguard the right to respect for private life.

Conclusions

It can be stated without a doubt that the rapid development of AI has created many opportunities in almost every aspect of human life, including in the field of justice. As many scholars emphasise (Cabrera, 2024; Guitton et al., 2025; Simmons, 2018; Watamura et al., 2025; Yu, 2022), AI tools can facilitate court management and assist judges in office work, in the courtroom and in the judicial decision-making process, hence allowing them to focus on more complex legal reasoning. For example, in Taiwan, artificial intelligence is exploited to recognise Mandarin in court proceedings, to automatically identify factors which affect the degree of penalty (hence ensuring that sentences imposed comply with the principles of proportionality and equality), to analyse electronic documentation and allocate it to departments, or to provide citizens with instant answers to questions about the judicial system or court proceedings by means of intelligent customer service chatbots (Kuo, 2024).

Nevertheless, these rapid changes also raise serious legal and ethical concerns, among both authorities and the public, with respect to compliance with current regulations, standards and ethical guidelines (Fine et al., 2025; Franguloiu, 2023; John et al., 2023), the necessity of human oversight of AI-created output (Fine et al., 2025; McCown Jones, 2025) and risks and biases created and embedded in AI algorithms (Angwin et al., 2016; Josten, 2023; McCown Jones, 2025; Moore et al., 2023), as well as its transparency or lack of it. This is a field that definitely needs further investigation, as technology must work for us and not against (some of) us. With the present study, the author hopes to provoke some discussion of and further research into this area.

REFERENCES

Aletras, N., Tsarapatsanis, D., Preoţiuc-Pietro, D., & Lampos, V. (2016). Predicting judicial decisions of the European Court of Human Rights: A Natural Language Processing perspective. *PeerJ Computer Science*, *2*, e93. https://doi.org/10.7717/peerj-cs.93

Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016, 23 May). *Machine bias*. ProPublica. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

Cabrera, B. M., Luiz, L. E., Cavalcante, D. L., & Teixeira, J. P. (2024). History of technological evolution in the Brazilian judiciary system and the application of artificial intelligence. *Procedia Computer Science*, *239*, 1188–1195.

Canadian Judicial Council. (2024, September). *Guidelines for the use of artificial intelligence in Canadian courts*. https://cjc-ccm.ca/sites/default/files/documents/2024/AI%20Guidelines%20-%20FINAL%20-%202024–09%20-%20EN.pdf

Conseil Constitutionnel (France). (2023, 17 May.) *Décision no. 2023–850 DC du 17 mai 2023*. https://perma.cc/8LC6-HW23

Council of Europe. (2024, 5 September). *Council of Europe framework convention on artificial intelligence and human rights, democracy and the rule of law*. https://rm.coe.int/1680afae3c

Council of the European Union. (2020, 9 June). *Council conclusions on shaping Europe's digital future*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020XG*0616*(01)

Council of the European Union. (2020, 13 October). *Council conclusions: 'Access to justice – seizing the opportunities of digitalisation'*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020XG*1014*(01)

Council of the European Union. (2023, 20 October). *Council conclusions on digital empowerment to protect and enforce fundamental rights in the digital age*. https://data.consilium.europa.eu/doc/document/ST-14309–2023-INIT/en/pdf

Council of the European Union. (2024, 5 March). *Conclusions on the application of the EU Charter of Fundamental Rights: Promoting trust through effective legal protection and access to justice*. https://data.consilium.europa.eu/doc/document/ST-7127–2024-INIT/en/pdf

Council of the European Union. (2024, 16 December). *Council conclusions (16933/24) on the use of artificial intelligence in the field of justice*. https://data.consilium.europa.eu/doc/document/ST-16933–2024-INIT/en/pdf

Courts and Tribunals Judiciary (UK). (2023, 12 December). *Artificial intelligence (AI): Guidance for judicial office holders*. https://www.judiciary.uk/wp-content/uploads/2023/12/AI-Judicial-Guidance.pdf

Courts and Tribunals Judiciary (UK). (2025, 15 April). *Artificial intelligence (AI): Judicial guidance*. https://www.judiciary.uk/guidance-and-resources/artificial-intelligence-ai-judicial-guidance/

Courts of New Zealand. (2023, 7 December). *Guidelines for use of generative artificial intelligence in courts and tribunals*. https://www.courtsofnz.govt.nz/going-to-court/practice-directions/practice-guidelines/all-benches/guidelines-for-use-of-generative-artificial-intelligence-in-courts-and-tribunals

European Commission. (2025, 4 February). *Commission publishes the guidelines on prohibited artificial intelligence (AI) practices, as defined by the AI Act*. https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act

European Commission for the Efficiency of Justice. (2019, February). *European ethical charter on the use of artificial intelligence in judicial systems and their environment*. https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c

European Parliament and Council of the European Union. (2016, 27 April). Regulation (EU) 2016/679 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679

European Parliament and Council of the European Union. (2024, 13 June). Regulation (EU) 2024/1689 Laying Down Harmonised Rules on Artificial Intelligence. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689

European Parliament. (2023, 19 October). *Shaping the digital transformation: EU strategy explained*. https://www.europarl.europa.eu/topics/en/article/20210414STO02010/shaping-the-digital-transformation-eu-strategy-explained

European Union Agency for Fundamental Rights. (2020, 14 December). *Getting the future right: Artificial intelligence and fundamental rights*. https://fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights

European Union Agency for Fundamental Rights. (2022.) *Bias in algorithms: Artificial intelligence and discrimination*. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2022-bias-in-algorithms_en.pdf

FantasySCOTUS (n.d.). *FantasySCOTUS*. Retrieved 24 September 2025, from https://fantasyscotus.net/

Fine, A., Berthelot, E. R., & Marsh, S. (2025). Public perceptions of judges' use of AI tools in courtroom decision-making: An examination of legitimacy, fairness, trust, and procedural justice. *Behavioral Sciences*, *15*(4), 476. https://doi.org/10.3390/bs15040476

Franguloiu, S. (2023). Principles for the use of artificial intelligence (AI) in the judiciary as derived from the European Ethics Charter: Justice efficiency and limitations. *Bulletin of the Transilvania University of Braşov*, *16*(65). https://doi.org/10.31926/but.ssl.2023.16.65.3.5

Grupo de Trabalho sobre Inteligência Artificial no Poder Judiciário (Brazil). (2024, 12 December). *Resolution no. 332/2020 of the National Council of Justice (CNJ)*. https://www.cnj.jus.br/wp-content/uploads/2025/02/draft-ai-resolution.pdf

Guitton, C., Druta, V., Hinterleitner, M., Tamò-Larrieux, A., & Mayer, S. (2025). Adoption of artificial intelligence in the judiciary: A comparison of 28 advanced democracies. *Discover Artificial Intelligence*, *5*(169). https://doi.org/10.1007/s44163–025-00311-y

Heshmaty, A. (2022, 1 February). *Use of AI in law firms to predict litigation outcomes*. https://www.lexisnexis.co.uk/blog/future-of-law/using-ai-to-predict-litigation-outcomes

Jadhav, E. B., Sankhla, M. S., & Kumar, R. (2020). Artificial intelligence: Advancing automation in forensic science & criminal investigation. *Seybold Report*, *15*(8).

John, A. M., Aiswarya, M., & Panachakel, J. T. (2023). Ethical challenges of using artificial intelligence in judiciary in 2023. In *IEEE International Conference on Metrology for eXtended Reality, Artificial Intelligence and Neural Engineering (MetroXRAINE)* (pp. 723–728). IEEE.

Josten, W. (2023). *Addressing bias in AI: Surveying the current regulatory and legislative landscape*. Thomson Reuters Institute. https://www.thomsonreuters.com/en-us/posts/technology/ai-bias-report-duke-law/

Judgment of the Federal Constitutional Court of Germany of 16 February 2023. https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2023/02/rs20230216_1bvr154719en.html

Judgment of the Gerechtshof Amsterdam of 4 April 2023, no. 200.295.742/01. https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:GHAMS:2023:793&showbutton=true&keyword=ecli%253anl%253aghams%253a2023%253a793&idx=1

Judgment of the Verwaltungsgerichtshof of Austria of 21 December 2023. Ro 2021/04/0010–11 (DE). https://www.vwgh.gv.at/medien/mitteilungen/Ro_2021040010.pdf

Junta Electoral Central (Spain). (2025, 14 July). *Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General*. https://www.juntaelectoralcentral.es/cs/jec/loreg/contenido

Kravetz, D. (2014, 14 July). *Algorithm predicts US Supreme Court decisions 70% of time*. ARSTechnica. https://arstechnica.com/science/2014/07/algorithm-predicts-us-supreme-court-decisions-70-of-time

Kuo, J. S. (2024). Wpływ sztucznej inteligencji na tajwańskie sądownictwo. *Iustitia*, *3*(4), 148–150.

Larson, J., Mattu, S., Kirchner, L., & Angwin, J. (2016, 23 May). *How we analyzed the COMPAS recidivism algorithm*. ProPublica. https://www.propublica.org/article/how-we-analysed-the-compas-recidivism-algorithm

McCarthy, J., Minsky, M. L., Rochester, N., & Shannon, C. E. (2016). A proposal for the Dartmouth summer research project on artificial intelligence (31 August 1955). In Jerry Kaplan (Ed.), *Artificial intelligence: What everyone needs to know* (p.1). Oxford University Press.

McCown Jones, E. (2025). Navigating AI hallucinations in the US legal system: Challenges and solutions. *Journal of Business and Behavioural Sciences*, *37*(1) pp. 90–99.

Moore, C., Ferguson, E., & Guerin, P. (2023, August). Pretrial risk assessment on the ground: Algorithms, judgments, meaning, and policy. *MIT Case Studies in Social and Ethical Responsibilities of Computing*. https://doi.org/10.21428/2c646de5.b016a7b3

Muller, C. (2020). *The impact of AI on human rights, democracy and the rule of law*. ALLAI. https://allai.nl/wp-content/uploads/2020/06/The-Impact-of-AI-on-Human-Rights-Democracy-and-the-Rule-of-Law-draft.pdf

Papp, D., Krausz, B., & Gyuranecz, F. Z. (2022). *The AI is now in session: The impact of digitalisation on courts*. https://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.ojs-doi-10_35467_cal_151833

Reiling, A. D. (2020). Courts and artificial intelligence. *International Journal for Court Administration*, *8*. https://doi.org/10.36745/ijca.343

République Française. (2023, 19 May). Loi no. 2023–380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions. https://perma.cc/PX93–4XMH

Senado de España. (2024, 19 February). *Spanish Constitution*. https://www.senado.es/web/conocersenado/normas/constitucion/detalleconstitucioncompleta/index.html?lang=en

Shi, J. (2022). Artificial intelligence, algorithms and sentencing in Chinese criminal justice: Problems and solutions. *Criminal Law Forum*, *33*(2), 121–148. https://doi.org/10.1007/s10609–022-09437–5

Simmons, R. (2018). Big data, machine judges, and the legitimacy of the criminal justice system. *UC Davis Law Review*, *52*, 1067–1118. https://lawreview.law.ucdavis.edu/sites/g/files/dgvnsk15026/files/media/documents/52–2_Simmons.pdf

Spanish Constitutional Court. (2019, 22 May). *Sentencia 76/2019 (Official State Gazzete) number 151, of 25 June 2019*. https://hj.tribunalconstitucional.es/en/Resolucion/Show/25942#complete_resolucion&completa

Stănilă, L. M. (2020). *Artificial intelligence, criminal law and the criminal justice system: Memories about the future*. Universul Juridic Publishing House.

UNESCO. (2021.) *Recommendation on the ethics of artificial intelligence*. https://unesdoc.unesco.org/ark:/48223/pf0000380455

UNESCO. (2023). *Global toolkit on AI and the rule of law for the judiciary*. https://unesdoc.unesco.org/ark:/48223/pf0000387331

UNESCO. (2024). *Draft UNESCO guidelines for the use of AI systems in courts and tribunals*. https://unesdoc.unesco.org/ark:/48223/pf0000390781

UNESCO. (2024). *UNESCO global judges' initiative: Survey on the use of AI systems by judicial operators*. https://unesdoc.unesco.org/ark:/48223/pf0000389786

UNESCO. (n.d.) *Artificial intelligence and the rule of law*. Retrieved 24 September 2024, from https://www.unesco.org/en/artificial-intelligence/rule-law

United Nations General Assembly. (2024, 11 July). *Resolution adopted by the Human Rights Council on 10 July 2024*. https://documents.un.org/doc/undoc/gen/g24/120/36/pdf/g2412036.pdf

Watamura, E., Liu, Y., & Ioku, T. (2025). Judges versus artificial intelligence in juror decision-making in criminal trials: Evidence from two pre-registered experiments. *PLoS ONE*, *20*(1), e0318486. https://doi.org/10.1371/journal.pone.0318486

Yalcin, G., Themeli, E., Stamhuis, E., Philipsen, S., & Puntoni, S. (2023). Perceptions of justice by algorithms. *Artificial Intelligence and Law*, *31*(2), 269–292. https://doi.org/10.1007/s10506–022-09312-z

Yu, E. (2022, 12 December). *China wants legal sector to be AI powered by 2025*. ZDNET/innovation. https://www.zdnet.com/article/china-wants-legal-sector-to-be-ai-powered-by-2025/

Bialystok Legal Studies
Białostockie Studia Prawnicze
2025 vol. 30 no. 4

sciendo

DOI: 10.15290/bsp.2025.30.04.12

Received: 31.12.2024
Accepted: 21.09.2025

Katarzyna Barbara Wojtkiewicz
SWPS University, Poland
kwojtkiewicz@swps.edu.pl
ORCID ID: 0000–0003–0630–4139

The Legal Entity Identifier and Legacy Systems: Harmonisation, Interoperability, and Balance in Digital Governance[1]

Abstract: This article examines the Legal Entity Identifier (LEI) as a cornerstone of contemporary digitalised governance. Originally introduced in response to the 2008 financial crisis to address systemic opacity in financial markets, the LEI has since evolved into a global public-good infrastructure that enables interoperability, transparency, and accountability across jurisdictions and sectors. This study investigates the extent to which the LEI can be effectively implemented in Poland and the European Union, and what legal, institutional, and economic barriers constrain its universal adoption. The research employs a multi-method design, combining doctrinal and comparative analysis with empirical evidence from European supervisory projects (the EIOPA, ESMA, ECB, and EBA) and a Polish case study conducted under an NCN project on tax administration. Findings confirm that the LEI strengthens systemic risk monitoring, audit quality, and SME participation in global trade, but also reveal persistent barriers, including renewal costs, administrative burdens, and fragmented domestic identifiers. The analysis identifies four pillars of reform – universality, interoperability, continuity, and public co-financing – necessary to embed the LEI within governance systems. Comparative lessons from the United States and Japan demonstrate that statutory identifiers can extend beyond finance and support innovation while oversight is maintained. The article concludes that only by recognising the LEI as a structural

1 This article was written as part of the implementation of the NCN grant no. 2024/08/X/HS5/00945, titled 'Identyfikacja podmiotów prawnych w systemach governance administracji publicznej: Studium przypadku administracji skarbowej w Polsce' [Identification of legal entities in public administration governance systems: A case study of tax administration in Poland], funded by the National Science Centre (NCN), Poland.

component of digitalised governance can its transformative potential for transparent, resilient, and inclusive public administration be fully realised.

Keywords: Legal Entity Identifier (LEI), digital governance, legal harmonisation, interoperability of registers, public law, law reform

Introduction

The digitalisation of governance and law highlights the urgent need for infrastructures that guarantee transparency, efficiency, and interoperability across institutional systems. Among these, the Legal Entity Identifier (LEI) has emerged as a global standard to enhance regulatory compliance, reduce systemic risk, and support data-driven decision-making. Established under a G20 mandate in response to the 2008 financial crisis, the LEI has become a cornerstone of efforts to harmonise entity identification across jurisdictions (Financial Stability Board, 2024; Morales et al., 2024).

In an earlier, conceptual work, I argued that legal norms in digitalised governance no longer derive solely from legislative acts but increasingly from the operational logic of data infrastructures (Wojtkiewicz, 2025). Identifiers such as the LEI thus function as constitutive elements of governance, embedding legality into algorithmic and economic processes. This contribution positioned the LEI within the paradigm of 'law as an achievement of governance' (Kornhauser, 2022, p. 13), demonstrating its normative as well as technical significance.

1. Research methodology

1.1 Research question

This study is guided by the following research questions: To what extent can the Legal Entity Identifier be effectively implemented as a harmonising and interoperable infrastructure within digital governance? And what legal, institutional, and economic barriers constrain its universal adoption in Poland and the European Union? To address this problem, three working hypotheses were formulated. First, the universality hypothesis assumes that the LEI constitutes a globally unique and indispensable instrument for regulatory harmonisation and interoperability, and that partial adoption undermines its effectiveness. Second, the barrier hypothesis recognises that without complementary national reforms, addressing renewal costs, fragmented registers, and operational risks, the LEI's functionality will remain constrained, particularly for SMEs. Third, the public-good hypothesis emphasises that because the systemic benefits of the LEI outweigh private costs, its effective implementation requires public support, including mechanisms of co-financing.

1.2 Methodological design

The research employs a multi-method legal and governance design, combining normative analysis with empirical evidence generated within European and international supervisory projects in which I actively participated. The doctrinal method provided the basis for interpreting EU regulations such as the Regulation on OTC Derivatives, Central Counterparties and Trade Repositories (EMIR), Directive on markets in financial instruments (MIFID II), and the Regulation on Transparency of Securities Financing Transactions (SFTR), as well as Polish laws governing identifiers, such as the National Court Register (*Krajowy Rejestr Sądowy*, KRS), the Tax Identification Number (*Numer Identyfikacji Podatkowej*, NIP), the National Official Business Register (*Rejestr Gospodarki Narodowej*, REGON), and the Central Registration and Information on Business (*Centralna Ewidencja i Informacja o Działalności Gospodarczej*, CEIDG). The comparative method offered a broader perspective by examining US and Japanese practices, including the introduction of the US Unique Entity Identifier (UEI) under the Code of Federal Regulation (CFR) 2, Part 25, and the Financial Data Transparency Act, and Japanese initiatives in electronic trade instruments (Congressional Research Service, 2025; Czaplicki, 2021; Data Foundation & GLEIF, 2018). The case study method was applied in the NCN project 'Identification of legal entities in public administration governance systems: A case study of tax administration in Poland' (2024–2025), which tested the mapping of domestic identifiers to the LEI. This project revealed administrative burdens, cost sensitivities, and interoperability challenges within fragmented registers.

The impact assessment approach drew on methodologies developed in supervisory institutions, including the European Insurance and Occupational Pensions Authority's (EIOPA) guidelines on LEI use (EIOPA, 2014), the European Securities and Markets Authority's (ESMA) cost–benefit analysis on MiFID II/MiFIR (ESMA, 2015), and the European Central Bank's (ECB) Integrated Reporting Framework [cost–benefit analysis (CBA)] (ECB, 2024). These frameworks were adapted to the Polish context to evaluate the costs and benefits of LEI implementation, particularly for SMEs. Finally, the research integrated empirical evidence from supervisory surveys and consultations conducted by EIOPA, ESMA, the ECB, the European Banking Authority (EBA), and the Global Legal Entity Identifier Foundation (GLEIF). These instruments captured first-hand data on renewal costs, administrative complexity, and adoption barriers, while also documenting the systemic benefits of LEI for transparency and stability.

In addition to drawing on published supervisory methodologies, the research incorporates my direct involvement in European and international projects. As a member of the EIOPA IT and Data Committee and the leader of its Business Subgroup, I contributed to the development of the 2014 guidelines on LEI use, including the design of supervisory templates and consultations with national authorities (EI-

OPA, 2014b). At the ECB, I participated in preparatory work for the Register of Institutions and Affiliates Database and the Integrated Reporting Framework (IReF), where impact assessment and cost–benefit methodologies were tested. Contributions to ESMA consultations on MiFID II/MiFIR implementation further informed the empirical base of this study, especially regarding the 'no LEI, no trade' principle. Moreover, I engaged in EBA reporting of harmonisation projects and cooperated with GLEIF, gaining access to survey data and stakeholder feedback on LEI adoption across sectors. These experiences provided first-hand insights into how supervisory bodies design questionnaires, evaluate systemic costs and benefits, and manage the integration of identifiers into reporting frameworks. Embedding this perspective strengthens the methodological triangulation of this study by combining legal analysis with policy design practice and empirical supervisory evidence.

1.3 Methodological triangulation

By combining doctrinal and comparative analysis, case study evidence, cost–benefit assessments, and empirical data from supervisory projects, this study ensures methodological triangulation. This approach integrates theoretical, legal, and practical perspectives, thereby strengthening the validity of the findings and enhancing their relevance for policy debates at both EU and national levels.

2. The Legal Entity Identifier: Evidence, findings, and implications

2.1 The Legal Entity Identifier in global and national contexts

The Legal Entity Identifier was created in response to the 2008 financial crisis, when a lack of reliable counterparty identification magnified systemic risks. Earlier Polish analyses of financial market infrastructures revealed comparable issues of fragmented supervision and limited transparency of institutional investors (Sas-Kulczycka [Wojtkiewicz], 2014). Mandated by the G20, the Financial Stability Board (FSB) developed the Global Legal Entity Identifier System to provide a universal identifier for legally distinct entities (Financial Stability Board, 2024). The LEI, based on ISO 17442, is a neutral, 20-character alphanumeric code with no embedded information, ensuring both universality and simplicity. It provides two categories of data: Level 1 ('who is who'), which includes the entity's official name, legal form, registered address, jurisdiction, and registration authority; and Level 2 ('who owns whom'), which maps ownership and control structures, allowing regulators to identify direct and ultimate parents. Together, these features support systemic transparency and reduce data fragmentation across jurisdictions (Jenkinson & Leonova, 2013; Powell et al., 2011). As I have previously demonstrated, the integration of identification standards within financial market infrastructures enhances both transparency and governance efficiency by clarifying 'who is who' on the digitized market (Wojtkiewicz, 2022b).

The governance of the LEI follows a federated model. Strategic oversight is exercised by the Regulatory Oversight Committee (ROC), an international network of regulators. Operational responsibility lies with GLEIF, a non-profit created in 2014, which accredits Local Operating Units (LOUs), sets data quality standards, and maintains the open global LEI database. LOUs perform registrations, validations, and renewals in national markets, often working with local business registers (Legal Entity Identifier Regulatory Oversight Committee, 2015).

Since its inception, the LEI has been integrated into over 300 regulatory instruments worldwide. In the European Union, it is mandated under EMIR, MiFID II/MiFIR, and SFTR, making it a cornerstone of transparency in capital markets (European Securities and Markets Authority, 2017, 2018). Its applications now extend to non-financial domains, including trade digitalisation, supply chain management, and Environmental, Social and Governance (ESG) (Asian Development Bank, 2019; Morales et al., 2024). As I have argued elsewhere (Wojtkiewicz, 2025), the LEI is not merely a technical instrument but part of the normative infrastructure of governance in the digital age, embedding legality into operational processes and enhancing both efficiency and legitimacy (Brownsword, 2023; Kornhauser, 2022).

2.2 Empirical evidence from European supervisory projects

One of the first large-scale applications of the LEI in Europe was led by EIOPA, which in 2014 introduced binding guidelines on the use of the LEI for insurers and pension institutions (EIOPA, 2014a). As a member of EIOPA's IT and Data Committee and its Business Subgroup leader, I contributed directly to the methodology that shaped these guidelines. The project addressed the inefficiencies caused by the absence of a common identifier, which hindered Solvency II reporting and increased supervisory costs. Before the adoption of the guidelines, EIOPA conducted a six-month in-depth analysis of legislation and the related business processes carried out within the authority. This identified the LEI as a fundamental element of reference data and as a cornerstone of EIOPA's organisational architecture (Wojtkiewicz, 2022a; Wojtkiewicz, 2018). Building on these findings and following a fast-track consultation process, the guidelines required all entities within the Solvency II scope to obtain LEIs by mid-2015, with Institutions for Occupational Retirement Provision (*IORPs*) added by mid-2016. National competent authorities were tasked with ensuring compliance and verifying that LEIs were systematically used in quantitative templates, registers, and stress tests (EIOPA, 2014a, 2014b).

The results confirmed the feasibility of embedding the LEI in supervisory processes. Data comparability improved, group supervision became more effective, and duplication was reduced. Yet challenges emerged: smaller firms reported disproportionate renewal costs, National Competent Authorities struggled with aligning legacy systems, and stakeholders raised concerns about overlapping national identifiers (EIOPA, 2014b). These findings echoed the ROC's (2015) survey on regulatory uses

of the LEI and ESMA's (2015) cost–benefit analysis, which concluded that mandatory use, embodied in the 'no LEI, no trade' rule, was essential to overcome coordination failures. The ECB's (2024) Integrated Reporting Framework cost–benefit analysis further reinforced that standardised identifiers are crucial for reducing reconciliation costs and ensuring supervisory efficiency.

2.3 Findings from the Polish case study: The tax administration pilot

National-level insights were provided by the NCN MINIATURA project 'Identification of legal entities in public administration governance systems: A case study of tax administration in Poland' (2024–2025). This project piloted the mapping of domestic identifiers – KRS, NIP, REGON, and CEIDG – against the LEI (Wojtkiewicz, 2024–2025). The study demonstrated the persistent fragmentation of Polish identification systems. Legal analysis showed that parallel registers lack interoperability, resulting in duplication and errors. Computational methods, including text mining, semantic tagging, and language-model analysis, were used to process over 8,000 legal acts and identify provisions referring to entity identifiers. The mapping revealed that LEI Level 1 attributes largely overlap with Polish identifiers, while Level 2 ownership data provide transparency absent in domestic law (Wojtkiewicz, 2025).(Wojtkiewicz, 2025b).

The findings confirmed that the LEI could serve as a unifying identifier in tax administration, reducing reporting errors and strengthening compliance. Legislative mapping identified concrete reforms, such as amending the National Court Register Act and the Rules for Registration and Identification of Taxpayers Act to include LEI references, and integrating LEI into REGON. Recommendations emphasised the need for a coordinating statute to harmonise identifiers and ensure alignment with EU standards. Importantly, the project not only validated the LEI's potential but was also an innovative methodological approach combining legal analysis with computational tools.

2.4 Systemic benefits versus practical barriers

The systemic benefits of the LEI are well established: it enables aggregation of exposures across markets, supporting financial stability (Jenkinson & Leonova, 2013, pp. 105–107; Powell et al., 2011, pp. 2–3; European Systemic Risk Board, 2021, p. 22). Its Level 2 data make ownership hierarchies visible, thereby enhancing transparency and accountability (Yen & Wang, 2024). It also reduces verification costs, improves audit quality, and supports disclosure in sensitive contexts such as offshore finance (Keloharju, 2024). Moreover, it lowers barriers for SMEs to access trade finance and global markets, reinforcing inclusivity (Asian Development Bank, 2019; Morales et al., 2024). Yet practical barriers remain significant. Renewal fees and administrative burdens fall disproportionately on SMEs, while national systems with multiple identifiers, such as Poland, exacerbate inefficiencies. Many firms perceive LEI obligations as compliance burdens without immediate benefits (Banco de España, 2024). The gap

between systemic advantages and individual costs underscores the need for state involvement and coordinated reforms to ensure sustainable adoption.

2.5 International comparisons and transferable lessons

Comparative experience strengthens the case for reform. In the United States, the Unique Entity Identifier (UEI) was mandated for all federal procurement and grant recipients under CFR 2, Part 25, replacing the Data Universal Numbering System (*DUNS*) number. Complementing this, the Financial Data Transparency Act of 2022 requires interoperable data standards across regulators, with the LEI considered a key tool for alignment (Congressional Research Service, 2025; Office of the Comptroller of the Currency, 2024; US Federal Register, 2024). This dual framework illustrates how statutory identifiers can extend beyond finance and how interoperability between domestic and global identifiers can be institutionalised. Japan offers another instructive case. The development of electronic bills of exchange shows how digital identity solutions can be embedded in legal frameworks to balance innovation and regulatory oversight (Czaplicki, 2021). Together, these examples demonstrate that statutory mandates and interoperability frameworks are achievable and transferable, providing concrete lessons for Poland and the EU.

2.6 Policy implications

The findings of this section converge on one conclusion: the LEI must be recognised as a foundational infrastructure of digital governance. The evidence from European supervisory projects, the Polish case study, and international comparisons highlights both the systemic benefits of the LEI and the barriers that obstruct its universal adoption. The analysis points to four areas requiring reform: universality of coverage, interoperability with domestic and global identifiers, the continuity of accurate and timely renewals, and public co-financing mechanisms. These pillars form a bridge to the reform agenda developed in Section 3, where *de lege lata* and *de lege ferenda* recommendations are articulated in detail.

3. The legal reform agenda: De lege lata and de lege ferenda

3.1 De lege lata: Current legal obligations and practice

At present, the LEI is firmly embedded in the European Union's financial regulatory framework. Under EMIR, MiFID II/MiFIR, and SFTR, market participants must provide LEIs in reporting transactions, a requirement operationalised through ESMA's enforcement of the 'no LEI, no trade' principle (ESMA, 2017, 2018). These rules have made the LEI indispensable for financial institutions and infrastructures, providing systemic transparency and enhancing risk monitoring.

In Poland, the LEI is applied primarily within this EU-driven framework. Domestic legal acts, such as the National Court Register Act and the Rules for Regis-

tration and Identification of Taxpayers Act, do not mandate LEI use, leaving most entities reliant on national identifiers such as the KRS, NIP, REGON, and CEIDG. This fragmented landscape undermines interoperability and increases compliance burdens. Moreover, SMEs often perceive LEI renewal costs as disproportionate, a concern echoed in supervisory assessments across Europe (Banco de España, 2024). EIOPA's 2014 guidelines confirmed the regulatory expectation that insurers and pension institutions use LEIs systematically in Solvency II reporting, a milestone that demonstrated the feasibility of integrating the LEI into supervisory processes (EIOPA, 2014a, 2014b). Yet despite such successes, adoption remains uneven, and gaps in national law persist, particularly outside the financial sector.

3.2 De lege ferenda: Towards universal and sustainable implementation

To move beyond sectoral application, reforms should focus on four interrelated pillars. First, universality must be established through statutory obligation. As the US experience with the UEI shows, mandatory coverage for all entities that engage with public authorities is both feasible and effective (Code of Federal Regulations, 2025; Congressional Research Service, 2025; Office of the Comptroller of the Currency, 2024). For Poland, extending the obligation to all registry-eligible entities would align the LEI with the universal duty of KRS registration. Second, interoperability requires systematic mapping of the LEI to national identifiers (KRS, NIP, REGON, CEIDG) and to the UEI in cross-border contexts. The ECB's IReF cost–benefit analysis demonstrated that harmonised identifiers significantly reduce reconciliation costs and enhance reporting quality (ECB, 2024). Third, continuity must be safeguarded through legal mechanisms that ensure timely renewals and assist renewal processes. The FSB's 2024 progress report stressed that lapsed or inactive LEIs undermine the system's integrity, creating risks of transactional blockage. Fourth, public co-financing is necessary to balance costs and benefits. Because the LEI functions as an infrastructure of governance with systemic benefits, renewal subsidies or tax incentives for SMEs would ensure equitable adoption. This reflects the view of Kornhauser (2022) that law is an achievement of governance and of Brownsword (2023) that legitimacy in digital governance requires balancing efficiency with fairness.

3.3 Innovative extensions of the LEI

Beyond mandatory adoption, future-oriented reforms should address innovative uses of the LEI. The development of verifiable LEIs (vLEIs) as cryptographic credentials opens new possibilities for secure digital verification in blockchain-based transactions and automated compliance. Linking LEIs with natural person identifiers would broaden transparency by covering the full spectrum of actors in governance systems. The LEI framework should also be extended to emerging entities such as AI agents or decentralised autonomous organisations whose activities increasingly intersect with legal and economic systems. Finally, its application should move deci-

sively into non-financial domains – healthcare, education, ESG reporting, and supply-chain management – where verifiable and interoperable identification is critical for accountability and trust (Asian Development Bank, 2019; Morales et al., 2024). Comparative experiences, such as Japan's electronic instruments regime, show that legal frameworks can successfully integrate innovative identity solutions without undermining oversight (Czaplicki, 2021).

3.4 Synthesis

The reform agenda outlined above positions the LEI as a foundational infrastructure for digital governance. Current obligations under EU law (de lege lata) provide a robust starting point, but their scope is too narrow to address fragmentation and ensure inclusivity. As Kettl (2015) observes, governance in the twenty-first century increasingly depends on adaptive, networked systems rather than hierarchical control — a principle equally relevant to digital infrastructures. Proposed reforms (de lege ferenda), focused on universality, interoperability, continuity, and public co-financing, are essential to achieve systemic benefits. Innovative extensions, including vLEIs, blockchain integration, and coverage of emerging entities, would future-proof the system and ensure adaptability in rapidly evolving governance environments. Taken together, these measures would allow Poland and the EU to align domestic law with global best practices, transforming the LEI from a sectoral compliance tool into a universal and resilient governance infrastructure.

Conclusion

This article has demonstrated that the Legal Entity Identifier must be regarded not merely as a technical tool of compliance but as a foundational infrastructure of digital governance. Evidence from European supervisory initiatives, including the EIOPA guidelines and ESMA's 'no LEI, no trade' rule, has confirmed that mandatory adoption significantly improves transparency, risk monitoring, and data quality. The Polish case study conducted under the NCN project further highlighted both the feasibility and the necessity of LEI integration: while Level 1 data overlap with existing identifiers such as the KRS, NIP, and REGON, the Level 2 ownership information provides a depth of transparency absent in domestic registers. These findings underscore that universal LEI adoption would directly address fragmentation in national systems and reduce compliance errors. The comparative perspective reinforces this conclusion. The United States, through the introduction of the Unique Entity Identifier and the Financial Data Transparency Act, and Japan, through its regulation of electronic instruments, have shown that statutory identifiers can extend beyond the financial sector and support innovation while oversight is maintained. Such examples illustrate that the reforms proposed for Poland and the EU are both achievable and consistent with international practice.

The study also contributes theoretically by situating the LEI within the paradigm of 'law as an achievement of governance' (Kornhauser, 2022, pp. 13–14). As argued in my earlier work, identifiers in the digital era function as constitutive elements of governance. The LEI exemplifies this by embedding legality into the operational logic of data infrastructures, thereby enhancing not only efficiency but also legitimacy in governance systems. The policy implications are clear. To realise the LEI's transformative potential, reforms must focus on universality, interoperability, continuity, and public co-financing. These pillars, combined with innovative extensions such as verifiable LEIs, blockchain integration, and the inclusion of emerging digital entities, would allow the LEI to evolve into a sustainable infrastructure for both financial and non-financial governance.

Future research should further explore the integration of the LEI with artificial intelligence, semantic legal analysis, and cross-sectoral data governance. Such studies will be essential for ensuring that the LEI continues to adapt to technological change and remains capable of supporting governance systems that are transparent, resilient, and inclusive.

REFERENCES[2]

Beck, S., Sutken, C., Estrada, C., Doyle, R., & Malaket, A. (2019). Trade and the Legal Entity Identifier. DOI: http://dx.doi.org/10.22617/BRF190490–2

Brownsword, R. (2023). Law, regulation, and technology: The bigger picture of good governance. In B. Brożek, O. Kanevskaia, & P. Pałka (Eds.), *Research handbook on law and technology* (pp. 12–27). Edward Elgar Publishing.

Code of Federal Regulations. (2025, 3 January). *Part 25: Unique entity identifier and system for award management*. https://www.ecfr.gov/current/title-2/subtitle-A/chapter-I/part-25

Congressional Research Service. (2025, 25 August). *Financial Data Transparency Act: Implementation status of data standards*. https://www.congress.gov/crs-product/IF13093

Czaplicki, P. (2021). The electronic bill of exchange concept from an international perspective. *Białostockie Studia Prawnicze*, *26*(5), 187–195. https://doi.org/10.15290/bsp.2021.26.05.11

Data Foundation & Global Legal Entity Identifier Foundation. (2018). *Envisioning comprehensive entity identification for the US federal government*. Global LEI Foundation. Retrieved from https://datafoundation.org/news/reports/508/508-Envisioning-Comprehensive-Entity-Identification-for-the-US-Federal-Government

Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (recast). *Official Journal of the European Union*, L 173, published on 12 June 2014. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014L0065

2 There are also numerous level 2 and level 3 EU legal acts, along with various locally developed implementing regulations, that mandate the use of the LEI as an identifier, significantly increasing the total number of regulations requiring the LEI within the EU.

European Central Bank. (2024, June 15). *Cost–benefit analysis of the Integrated Reporting Framework (IReF)*. European Central Bank. Retrieved from https://www.ecb.europa.eu/stats/ecb_statistics/consultations/html/complementary-assessment.en.html

European Insurance and Occupational Pensions Authority. (2014a, October 7). *Guidelines on the use of the Legal Entity Identifier (LEI) (EIOPA-BoS-14/133)*. European Insurance and Occupational Pensions Authority. Retrieved from https://www.eiopa.europa.eu/publications/guidelines-use-legal-entity-identifier_en

European Insurance and Occupational Pensions Authority. (2014b, November 13). *Final report on public consultation no. 14/037: Proposal for guidelines on the use of the Legal Entity Identifier (LEI)*. European Insurance and Occupational Pensions Authority. Retrieved from https://www.eiopa.europa.eu/publications/guidelines-use-legal-entity-identifier_en

European Securities and Markets Authority. (2015, November 11). *Cost–benefit analysis: Annex II to draft RTS/ITS under MiFID II/MiFIR (ESMA/2015/1464)*. European Securities and Markets Authority. Retrieved from https://www.esma.europa.eu/sites/default/files/library/2015/11/2015-esma-1464_annex_ii_-cba-_draft_rts_and_its_on_mifid_ii_and_mifir.pdf

European Securities and Markets Authority. (2017, 20 December). *ESMA issues statement on LEI implementation under MiFID II*. European Securities and Markets Authority. Retrieved from https://www.esma.europa.eu/press-news/esma-news/esma-issues-statement-lei-implementation-under-mifid-ii

European Securities and Markets Authority. (2018, 20 June). *ESMA statement on LEI requirements under MiFIR (ESMA70–145-872)*. European Securities and Markets Authority. Retrieved from https://www.esma.europa.eu/sites/default/files/library/esma70–145-872_public_statement_on_lei.pdf

European Systemic Risk Board. (2021, December 15). *The benefits of the Legal Entity Identifier for monitoring systemic risk: Evidence from Germany (Occasional Paper No. 18)*. European Systemic Risk Board. Retrieved from https://www.esrb.europa.eu/pub/pdf/occasional/esrb.op.18~7977fb4f23.en.pdf

European Union. (2012, 4 July). *Regulation (EU) No 648/2012 of the European Parliament and of the Council on OTC Derivatives, Central Counterparties and Trade Repositories (EMIR). Official Journal of the European Union*, L 201, published on 27 July 2012. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32012R0648

European Union. (2014, 15 May). *Regulation (EU) No 600/2014 of the European Parliament and of the Council on Markets in Financial Instruments (MiFIR). Official Journal of the European Union*, L 173, published on 12 June 2014. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0600

European Union. (2014, 23 July). *Regulation (EU) No 909/2014 of the European Parliament and of the Council on Improving Securities Settlement in the European Union and on Central Securities Depositories (CSDR). Official Journal of the European Union*, L 257, published on 28 August 2014. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0909

European Union. (2015, 25 November). *Regulation (EU) 2015/2365 of the European Parliament and of the Council on Transparency of Securities Financing Transactions and of Reuse (SFTR). Official Journal of the European Union*, L 337, published on 23 December 2015. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015R2365

European Union. (2018, 30 May). *Directive (EU) 2018/843 of the European Parliament and of the Council Amending Directive (EU) 2015/849 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing (AMLD V). Official Journal of the European Union*, L 156, published on 19 June 2018. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843

Financial Stability Board. (2024, 21 October). *Implementation of the Legal Entity Identifier: Progress report*. Financial Stability Board. Retrieved from https://www.fsb.org/uploads/P211024–2.pdf

Global LEI Foundation (n.d.). *Global LEI index*. Retrieved 30 June 2024, from https://www.gleif.org/en/lei-data/global-lei-index

Global LEI Foundation. (n.d.). *The LEI: The key to unlocking financial inclusion in developing economies*. Retrieved 30 June 2024, from https://www.gleif.org/en/lei-solutions/the-lei-the-key-to-unlocking-financial-inclusion-in-developing-economies/

Jenkinson, N., & Leonova, I. S. (2013). The importance of data quality for effective financial stability policies-Legal entity identifier: a first step towards necessary financial data reforms. *Financial Stability Review*, *17*, 101–10. Available at SSRN: https://ssrn.com/abstract=2538229

Kettl, D. F. (2015). *The transformation of governance: Public administration for the twenty-first century*. JHU Press.

Kornhauser, L. A. (2022). Law as an achievement of governance. *Journal of Legal Philosophy*, *47*(1), 1–23.

Legal Entity Identifier Regulatory Oversight Committee. (2015, March 11). *Survey on regulatory uses of the LEI: Final report*. https://www.leiroc.org/publications/gls/lou_20151105–1.pdf

Morales, A., Ortega, M., Rivero, J., & Sala, S. (2024). How to Identify All Companies Worldwide: Experience with the Legal Entity Identifier (LEI). https://doi.org/10.53479/36259

Office of the Comptroller of the Currency. (2024, 22 August). *Financial Data Transparency Act of 2022: Proposed joint data standards* Bulletin, 2024–24). https://www.occ.gov/news-issuances/bulletins/2024/bulletin-2024–24.html

Powell, L. F., Montoya, M., & Shuvalov, E. (2011). Legal entity identifier: What else do you need to know? http://dx.doi.org/10.2139/ssrn.1956664

Rumsey, M., Data Foundation, & Global Legal Entity Identifier Foundation. (2018, September 12). *Envisioning comprehensive entity identification for the U.S. federal government.* Data Foundation & Global Legal Entity Identifier Foundation. Retrieved from https://www.gleif.org/_documents/blog/20180912-envisioning-comprehensive-entity-identification-for-the-u-s-federal-government/2018–09-12_GLEIF-and-Data-Foundation_Research-Report_Envisioning-Comprehensive-Entity-Identification-for-the-US-Federal-Government.pdf

Sas-Kulczycka (Wojtkiewicz), K. B. (2014). *Instytucje wspólnego inwestowania w Polsce: Fundusze inwestycyjne i emerytalne*. WIG-Press. (Original work published 1998).

Sejm Rzeczypospolitej Polskiej. (1995). Ustawa z dnia 13 października 1995 r. o zasadach ewidencji i identyfikacji podatników i płatników (Dz.U. 1995 Nr 142, poz. 702).

Sejm Rzeczypospolitej Polskiej. (1995). Ustawa z dnia 29 czerwca 1995 r. o statystyce publicznej (t.j. Dz.U. 2015, poz. 2009).

Sejm Rzeczypospolitej Polskiej. (1997). Ustawa z dnia 20 sierpnia 1997 r. o Krajowym Rejestrze Sądowym (Dz.U. 1997 Nr 121, poz. 769).

Sejm Rzeczypospolitej Polskiej. (1997). Ustawa z dnia 28 sierpnia 1997 r. o organizacji i funkcjonowaniu funduszy emerytalnych (Dz.U. 1998 Nr 69, poz. 456).

Sejm Rzeczypospolitej Polskiej. (2004). Ustawa z dnia 27 maja 2004 r. o funduszach inwestycyjnych (t.j. Dz.U. 2016, poz. 2188).

US Federal Register. (2024, 22 August). *Financial Data Transparency Act: Joint data standards (proposed rule)*. US Government Publishing Office. https://www.federalregister.gov/documents/2024/08/22/2024–18415/financial-data-transparency-act-joint-data-standards

Wojtkiewicz, K. B. (2018). Efektywne zarządzanie informacją jako strategiczny czynnik sukcesu nadzoru rynku finansowego. In T. Czerwińska & A. Z. Nowak (Eds.), *Rynek kapitałowy – regulacje i fundamenty* (Vol. 5) (pp. 25–40). Wydawnictwo Naukowe Wydziału Zarządzania Uniwersytetu Warszawskiego.

Wojtkiewicz, K. B. (2022a). Applying the business-process-oriented approach to data designs, governance, and management: Case study of the EIOPA. In A. Szpaderski, P. Cywiński, W. Karczewski, C. P. Neck, & K. B. Wojtkiewicz (Eds.), *International leadership and management: Emerging, contemporary, and unorthodox perspectives* (pp. 163–176). SWPS University and Institute of Leadership and Management.

Wojtkiewicz, K. B. (2022b). Identification of legal entities in financial market infrastructures: 'Who is who on the digitized market?' In A. Szpaderski, P. Cywiński, W. Karczewski, C. P. Neck, & K. B. Wojtkiewicz (Eds.), *International leadership and management: Emerging, contemporary, and unorthodox perspectives* (pp. 143–162). SWPS University and Institute of Leadership and Management.

Wojtkiewicz, K. B. (2024–2025). *Identification of legal entities in public administration governance systems: A case study of tax administration in Poland* [Research project, National Science Centre (NCN), Grant No. 2024/08/X/HS5/00945]. National Science Centre, Poland.

Wojtkiewicz, K. B. (2025a). The role of legal entity identification in modern governance and data management. In E. Dawidziuk, A. Tarwacka, & S. Kursa (Eds.), *Historical and contemporary issues of democracy, person and human rights* (pp. 467–482). Peter Lang. https://doi.org/10.3726/b23045

Wojtkiewicz, K. B. (2025b). *Project final report on the implementation of Legal Entity Identifier (LEI) standards in Polish administrative registers* [Unpublished research report]. SWPS University, Warsaw.

Yen, J. C., & Wang, T. D. (2024). Legal Entity Identifier and Future Research Directions. *International Journal of Computer Auditing*, *6*(1), 1–2. https://doi.org/10.53106/256299802024120601001

Bialystok Legal Studies
Białostockie Studia Prawnicze
2025 vol. 30 no. 4

sciendo

DOI: 10.15290/bsp.2025.30.04.13
Received: 09.07.2025
Accepted: 26.09.2025

Sławomir Patrycjusz Kursa
SWPS University, Poland
slawomirpatrycjusz@wp.pl
ORCID ID: 0000–0001–9327–0728

The Right to (Not) Make an Electronic Will: The Case of Nevada

Abstract: In 2001, the US state of Nevada became the first in the world to issue regulations directly introducing electronic wills into the legal system. This article provides a brief historical overview of this regulation, as well as the practice of preparing them (or rather the lack thereof) for many years after their introduction. In July 2019, the Uniform Law Commission (Electronic Wills Committee) completed work on the framework for the Uniform Electronic Wills Act, which can be easily adopted by all states. This Act covers the basic regulations necessary for preparing electronic wills, omitting the more controversial and extensive ones found in the Nevada Revised Statutes and leaving states free to choose some of the proposed solutions. The approval of the Uniform Electronic Wills Act and the emergence of the COVID-19 pandemic and the associated isolation undoubtedly contributed to the increased interest of state legislatures in electronic wills, as well as the acceleration of work on related legislation. The possibility of witnesses participating in the preparation of a will without being personally present but rather using remote attestation using audiovisual communication turned out to be particularly attractive. The list of states explicitly regulating the form of electronic wills has begun to grow, and at the same time, mentions of the first electronic wills being prepared have begun to appear.

Keywords: electronic wills, Nevada Revised Statutes, Uniform Electronic Wills Act, COVID-19 pandemic, digital technologies, qualified custodians

Introduction

Constant technological progress, especially in digital technologies, creates enormous new possibilities in various spheres of human activity, and consequently also leaves its mark in the area of law and its regulations. An example of this is the admission of electronic forms of submitting declarations of will, and to some extent also applies to

the issue of the forms of wills, which lies in the area of inheritance law (Osajda, 2010, pp. 50–51; Załucki, 2017, p. 17). Until almost the end of the 20th century, only traditional forms of wills were used in legal practice (they were already known in principle in ancient Rome), different varieties taking an oral or a written form. They also take different forms in the regulations of different countries today: the holographic form (a will handwritten and signed by the testator), which is used in many regulations (especially European ones, and about half of US states), attested (witnessed) wills and different varieties of public or notarial wills (drafted with the participation of a person of public trust, possibly witnesses, and sometimes deposited with such a person), as well as oral wills, which usually appear in a special form which can be drawn up with the participation of witnesses in the event of extraordinary circumstances (cf. Kucia, 2017, pp. 1179–1182; Świrgoń-Skok, 2019, pp. 135–136, 138–139; Załucki, 2017, pp. 18–19; Załucki, 2018, pp. 56–66, and the literature cited by these authors). Without going into details regarding the forms of these wills, which determine their distinctiveness, in each case they constitute different mutations or combinations of form requirements: oral or written wills. In these cases, the bearer of the content of the testator's last will is the memory of witnesses or a written document.

An absolute novelty and at the same time a revolution in the preparation of wills when it comes to the medium of their content are forms such as video wills (Załucki, 2017, pp. 20–23; Załucki, 2018) and electronic wills. These are recognized in the legal system of some countries thanks to judgments based on explicit statutory provisions (e.g. regulations on 'harmless error' or 'dispensing power' and also on 'substantial compliance', which permit departures from formal requirements when the testator's intention to make a will is proven; see Załucki, 2021, pp. 77–106); sometimes they are directly regulated as a separate form of will. In 2001, the US state of Nevada was the first legislature in the world to issue regulations introducing the electronic form of wills directly into the legal system, in addition to previously provided written forms of will (attested or holographic wills). This article presents a brief historical outline of the regulation of electronic wills in Nevada, as well as the practice related to their preparation, or rather the lack thereof, and the reasons for this lack for many years after this form of will was introduced into law. The experience of Nevada and the conclusions drawn from it are worth taking into account by other legislatures, including European ones, that want to incorporate new technologies into their regulations regarding the form of wills.

1. The introduction of electronic wills in Nevada

Electronic wills were introduced in Nevada by an amendment to the Nevada Revised Statutes (NRS) of 6 June 2001 (effective from 1 October 2001). It took into account changes in society, and aimed at the convenience of citizens and meeting the

needs of the part of society familiar with new technologies. In this way, Nevada was to become a leader in the field of implementing new technologies in law and legal transactions (Beyer & Hargrove, 2007, pp. 890). The legislature expressly stated that 'an electronic will is valid and has the same force and effect as if formally executed [in written not electronic form]'. Moreover, it 'may be made in or out of this state' (Sec. 9(3) = NRS 133.085(3)). The requirements of this form were specified in Sec. 9 = NRS 133.085 as follows:

1. An electronic will is a will of a testator that:
   (a) Is written, created and stored in an electronic record;
   (b) Contains the date and the electronic signature of the testator and which includes, without limitation, at least one authentication characteristic of the testator; and
   (c) Is created and stored in such a manner that:
      (1) Only one authoritative copy exists;
      (2) The authoritative copy is maintained and controlled by the testator or a custodian designated by the testator in the electronic will;
      (3) Any attempted alteration of the authoritative copy is readily identifiable; and
      (4) Each copy of the authoritative copy is readily identifiable as a copy that is not the authoritative copy.

Accordingly, an electronic will is a will written, created and stored in a record created, generated or stored by electronic (not written) means (Sec. 3 = NRS 132.117). It must be dated and signed by the testator electronically. 'Electronic signature' means an electronic sound, symbol or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record (Sec. 4 = NRS 132.118). In addition, it should contain the authentication characteristic of the testator; these are defined in Sec. 9(6)(a) = NRS 133.085(6)(a) as a characteristic of a certain person that is unique to that person and that is capable of measurement and recognition in an electronic record as a biological aspect of or physical act performed by that person. Such a characteristic may consist of a fingerprint, a retinal scan, voice recognition, facial recognition, a digitized signature or other authentication using a unique characteristic of the person. A 'digitized signature' means a graphical image of a handwritten signature that is created, generated or stored by electronic means.

The next requirements concern the manner of the will's preparation and storage. It should be prepared in one authoritative version and maintained and controlled by the testator or a custodian designated by them in the electronic will, in such a way that any attempted alteration of the authoritative version is readily identifiable. Any copy of the electronic will should be identifiable as a copy that is not the authoritative copy. Moreover, an electronic will should be maintained by a custodian designated in

the electronic will or by the testator at their place of business or residence in Nevada (Sec. 9(4) = NRS 133.085(4)).

At first glance, the above requirements, although specified not in one but in several provisions, seem to be understandable to comply with. However, the problem lies in the details, especially the technical ones, which in the provisions have been specified generally and in a scattered manner, without indicating specific means and technologies that meet the requirements of the law and at the same time give the testator a sense of a properly and validly made will (Grant, 2008, pp. 124–125; Kucia, 2016, p. 113). As a result, the testator has to consider each time whether the chosen means meet the requirements of the law, which entails the risk of a court finding that these requirements have not been met (Langbein, 2017, p. 11) and therefore that the will is invalid. It should be remembered that we are dealing with a will – an act *mortis causa*, which the testator will not be able to correct after death in order to meet the formal requirements of the law, if it turns out that they have not all been fulfilled.

How then should we understand that 'electronic record' means 'a record created, generated or stored by electronic means'? What is this electronic means? What is an 'electronic signature' that is 'an electronic sound, symbol or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record'? How should it be recorded? Using what technology and in what format? Although in Sec. 6 'record' is defined as 'information that is inscribed on a tangible medium, or that is stored in an electronic medium and is retrievable in perceivable form', this definition does not provide an unequivocal answer. Similar questions could be asked in relation to the 'authentication characteristic'.

Finally, given the electronic format of the will and the easy ability to copy electronic files, how can it be ensured that there is only one authoritative copy? How can the requirement that the will be maintained at a place of business or residence in Nevada be understood? Does it have to be saved and stored on a data carrier such as a hard drive, a pen drive, or in phone memory? Could it be stored in the cloud? In the latter case, the user does not necessarily know where the collected data is physically stored.

2. Practical problems in implementing electronic wills in Nevada

The requirements for electronic wills, and the technical solutions included in them, introduced in Nevada in 2001 were very avant-garde, and at the same time not fully accessible. While work on biometric authentication, a kind of equivalent to a testator's signature on a paper will, was already advanced, there was a lack of software that could ensure that there is only one authoritative copy of the will and that any copies and changes to the original are readily identifiable. For this reason, for many years the regulation introducing electronic wills was in force in Nevada but was not applied (Beyer & Hargrove, 2007, pp. 890–891). There were also opinions that the

solution to the problem of the one authoritative copy could be the use of Digital Estate Planning (DEP) services:

> The authoritative copy would be the copy held by the DEP service. It would be alterable only by the testator, but the DEP service would record any changes made and keep copies of previous versions in case a dispute arose later. Commodity consumer electronics hardware and software can already perform many of the authentication techniques mentioned in the Nevada statute, including voice recognition, face recognition, fingerprints, and digitized signatures. (Roy, 2011, pp. 415–416)

Moreover, it was pointed out that hardware and software are often modified and updated, due to incredibly rapid technological progress, as a result of which there is a risk that there will be no hardware or software that would allow access to an electronic will prepared by the testator many years before his or her death. In addition, there were risks related to the ageing of hardware, in particular hard drives or portable data carriers such as pen drives or CD-ROMs, which over the years results in the loss of data stored on them, which may also apply to electronic wills (Beyer & Hargrove, 2007, pp. 893–895). There is also a risk that a company storing wills might go bankrupt or be hacked (Hirsch, 2020, pp. 862–863).

Another noted risk raised in connection with the electronic form of a will is related to its revocation through physical destruction. There is always a risk that, even if the testator intends to revoke his or her will and deletes the file from the computer's hard drive (or other storage medium), this file will be restored against their wishes (Langbein, 2017, p. 11). Suspicion of such action may pose many evidentiary problems that would not arise in the case of physical destruction of a written will. On the other hand, this disadvantage could be an advantage in certain cases, because if a written will is destroyed (e.g. burned) by an unauthorized person or accidentally by the testator him – or herself, without the testator wishing to revoke it, then its content cannot always be entirely recreated; thus such an unrevoked but physically non-existent will cannot be executed. Meanwhile, if someone (including the testator) accidentally or intentionally deletes the electronic will from the medium's memory (without destroying the medium itself) against the testator's will, there is a chance of recovering it entirely.

The fact that the older part of the population is not familiar with new technologies and is therefore distrustful of them, which is why they are not interested in using such legal innovations as electronic wills, was raised as a social barrier to implementing electronic wills (Beyer & Hargrove, 2007, pp. 891–892). On the contrary, society is accustomed to a tangible written document that is easy to read (Banks, 2015, pp. 298–299), and as a result, testators choose the traditional, written form of a will. This is true, but it should be noted that another, younger part of society is in the exact opposite situation: they use only electronic means of communication and make declarations of their will on a daily basis, and treat traditional written forms as outdated and inconvenient.

Another barrier raised was the costs associated with the technology (devices, software, and also training in their use) necessary to prepare an electronic will (Beyer & Hargrove, 2007, p. 892). However, taking into account rapid technological progress, mass implementation of new technologies and their availability, it seems that this obstacle has lost its significance. On the contrary, the implementation of secure methods of authorization and recognition of a person may make an electronic will safer than a written one, as it is more difficult to introduce unauthorized changes (not made by the testator) or to forge them. More advanced technologies (which is still a future prospect) could additionally verify whether there are any defects in the declaration of will when preparing an electronic will, e.g. a state of lack of awareness (cf. Melnychuk, 2014, p. 41).

It seems that a very important reason for the lack of interest in electronic wills in Nevada was the lack of measurable benefits from their use. Even with the availability of technology, fulfilling all the requirements would mean taking care of a number of details that the average person is not able to remember (and is also a matter of knowledge of the law), let alone be sure that they have completed correctly and therefore that they have definitely drawn up a valid will. It is certainly easier to ensure that all the requirements of a written will (attested or holographic) are met, which is still an acceptable and more accessible form of will, with a lower risk of failure to meet the requirements for validity (Boddery, 2012, pp. 200–201). An electronic will does not bring any measurable added value, nor has there been a real need to introduce it.

3. Amendments to the Nevada Revised Statutes regarding electronic wills

The above problems, and above all the lack of technological solutions ensuring the existence of only one authoritative copy, resulted in the fact that, despite the passage of time, electronic wills have not been drawn up in practice (Beyer & Peters, 2019, p. 2). As a result, the legislature decided to introduce changes to the existing regulation. The amendment to the Nevada Revised Statutes of 9 June 2017 (effective from 1 July 2017) was intended to correct the imperfections of the original regulation regarding electronic wills and to allow their preparation. It improved the definition of 'electronic will' (Sec. 8 = NRS 132.119) and clarified the meaning of the terms 'electronic record' (Sec. 7 = NRS 132.117) and 'authentication characteristic' (Sec. 19 = NRS 133.085(5)(a)). At the same time, the requirements for its validity were changed, and allowed, as an alternative to the authentication characteristic of the testator, its confirmation by the signature and electronic seal of an electronic notary public or the electronic signatures of two or more attesting witnesses, placed thereon in the presence of the testator and in whose presence the testator placed his or her electronic signature (Sec. 19 = NRS 133.085(1)). Moreover, according to this regulation it is not necessary for the testator to be present

in Nevada at the time of execution; it is sufficient that a notary public or attesting witnesses be present there and that they communicate with each other by means of audiovisual communication (Millonig, 2018, p. 29).

Above all, however, the provisions concerning the requirement of the existence and storage of one authoritative copy, which in practice constituted an obstacle preventing the preparation of electronic wills, were removed from the requirements for validity. In their place appeared an extensive regulation (over six typewritten pages) concerning a qualified custodian of the electronic record of the will, the participation of an electronic notary in the preparation of the will, and declarations or affidavits of the witnesses and qualified custodians necessary for the execution of the will (Sec. 10–18). So once again, no specific technological solutions for storing an electronic will were indicated, but instead obligations were imposed on the qualified custodian, and guidelines were provided as to how to handle the electronic will during the life of the testator and after their death (Krueger, 2019, pp. 993–994), while declarations or affidavits submitted by the qualified custodian and other persons are to ensure the authenticity of the electronic will. As a result, although it has become possible to apply the regulation concerning electronic wills, it has been further expanded, which in practice does not facilitate its application.

The situation in this respect was not changed by the next amendment, of 29 May 2021, which did not introduce fundamental changes to the regulation on electronic wills but was of a regulatory nature. It systemically unified the definition of 'electronic record' and 'electronic signature' by referring to the definitions of these concepts included in Chapter 719 concerning 'electronic transactions' in general, and also simplified the definition of 'electronic wills'. In addition, among other things, the methods for revoking an electronic will (Sec. 9 = NRS 133.120) and the methods of appointing a qualified custodian and their duties (Sec. 10–14 = NRS 133.300–133.340) were clarified.

4. Subsequent electronic will regulations

Apart from in Nevada, which was the pioneer of electronic wills, electronic wills have been regulated by the laws of only three states: Indiana from 1 July 2018, Arizona from 1 July 2019 (Beyer & Peters, 2019, pp. 3–11) and Florida from 6 June 2019 (Krueger, 2019, pp. 1018–1023). In July 2019, the Uniform Law Commission (Electronic Wills Committee) completed work on the framework for the Uniform Electronic Wills Act (UEWA), which can be easily adopted by all states:

> Under the UEWA, an electronic will must be 'a record that is readable as text at the time of signing', signed by the testator, and either signed by two witnesses or acknowledged before a notary. […] The UEWA also allows for the possibility of remote, electronic witnessing and notarization, providing optional

> language depending upon the state's preference. […] Notably absent from the provisions of the UEWA are any provisions related to qualified custodians. (Krueger, 2019, pp. 1023–1025)

The Uniform Electronic Wills Act includes the basic regulations necessary for the preparation of electronic wills, omitting the more controversial and extensive ones found in the Nevada Revised Statutes and leaving states free to choose some of the proposed solutions.

The approval of the Uniform Electronic Wills Act and the emergence of the COVID-19 pandemic and the associated isolation undoubtedly contributed to the increased interest of state legislatures in electronic wills, as well as the acceleration of work on the related legislation. The possibility of witnesses participating in the preparation of a will without being personally present but with remote attestation using audiovisual communication turned out to be particularly attractive (Storrow, 2022, pp. 857–860). This turned out to be a way to meet the need for making testaments during isolation. Therefore some states, such as Utah and Washington, DC, soon began to adopt them, although in the case of the latter, on the provision that only when the mayor has declared a public health emergency may electronic wills be electronically witnessed (Visconti, 2021, pp. 964–968).

The list of states directly regulating a form of electronic wills has begun to grow, so that in 2023, six states (Nevada, Indiana, Arizona, Florida, Maryland and Illinois) had their own regulations, and seven (Colorado, North Dakota, Utah, Washington, Idaho, Minnesota and Washington, DC) adopted the Uniform Electronic Wills Act with greater or fewer changes (Carson, 2023; Hirsch, 2021, pp. 165–166). Work is currently underway to introduce electronic wills in other states; at the same time, there are mentions of the first electronic wills being prepared. As Jeffrey Dible rightly notes, 'we won't know how many there are until people start dying' (quoted in Carson, 2023), which means that we have to wait a few years for more reliable statistics. On the other hand, most US states still lack regulations that allow for the preparation of an electronic will.

Conclusions

Dynamic technological progress and, as a result, changes in society are slowly creating a need to introduce electronic wills into law. The development of technology and the COVID-19 pandemic have accelerated the legislative process in this area in the US, and at the same time have increased social acceptance of remote forms of preparing wills. However, testators should have the choice of whether to make a will in a traditional or an electronic form. At least as long as people who were born and learned about the world in analogue times are alive, legislatures should retain the traditional forms of wills. This does not exclude the possibility of allowing electronic wills, while at the same time regulating their form in an unambiguous and possi-

bly concise manner, and where appropriate technical support is provided. Just as for many years a written will has been accessible to everyone for obvious reasons (lack of illiteracy, easy access to writing materials), and therefore in practice it has been the basic form of making a will, an electronic will may already be becoming a more accessible and secure form for younger generations. It is worth noting that none of the currently available forms of will is free from defects or completely safe (Kucia, 2017, p. 1192, n. 78). Considering the fact that many young people already find it easier to write using electronic devices (which among other things automatically check spelling), and only write by hand when they have no choice, it is worth European legislatures, including the Polish one, considering creating such an opportunity for them. It is also worth considering issuing a framework regulation at the European Union level, similar to the Uniform Electronic Wills Act.

An electronic will with appropriately balanced requirements can be a very convenient and useful form of a last will, especially in exceptional situations where using other forms would be difficult or even impossible, while today almost everyone carries a smartphone. Although no work is underway in Poland on its introduction yet, there is a government draft amendment to the Civil Code (UD30 of 2024) providing for the possibility of making an oral audiovisual will without the participation of witnesses, as a special form. Using it could be easier; sometimes such a special form may be the only possible way of making a will, as happened on 8 June 1948 to Cecil George Harris, who, after being crushed by a tractor and fearing he may not survive, without a piece of paper and a pen, used his pocket knife to scratch his will onto the tractor's fender (Brown, 2013).

Drawing up a will in electronic form, as the latest regulations show, does not have to involve additional costs, assuming that its preparation requires only the hardware and software that is used on a daily basis by most people. Moreover, it may in practice be easier for the testator to make changes to the content of electronic wills, without the risk of making them illegible, which may happen in the case of many changes made to a holographic will (Banks, 2015, p. 298).

REFERENCES

Banks, J. (2015). Turning a won't into a will: Revisiting will formalities and e-filing as permissible solutions for electronic wills in Texas. *Estate Planning and Community Property Law Journal*, *8*, 291–316.

Beyer, G. W., & Hargrove, C. G. (2007). Digital wills: Has the time come for wills to join the digital revolution? *Ohio Northern University Law Review*, *33*(3), 865–902.

Beyer, G. W., & Peters, K. V. (2019). *Sign on the [electronic] dotted line: The rise of the electronic will*. https://ssrn.com/abstract=3278363

Boddery, S. S. (2012). Electronic wills: Drawing a line in the sand against their validity. *Real Property, Trust and Estate Law Journal*, *47*(1), 197–212.

Brown, J. (2013, 25 October). *Dying Saskatchewan farmer's will goes down in history*. Global News. https://globalnews.ca/news/926746/dying-sk-farmers-will-goes-down-in-history/

Carson, D. (2023, 2 August). *Electronic wills off to slow start in Indiana: State law updated in 2021 to allow for remote witnessing, but demand remains low*. The Indiana Lawyer. https://www.theindianalawyer.com/articles/electronic-wills-off-to-slow-start-in-indiana-state-law-updated-in-2021-to-allow-for-remote-witnessing-but-demand-remains-low

Grant, J. K. (2008). Shattering and moving beyond the Gutenberg paradigm: The dawn of the electronic will. *University of Michigan Journal of Law Reform*, *42*(1), 105–139.

Hirsch, A. J. (2020). Technology adrift: In search of a role for electronic wills. *Boston College Law Review*, *61*(3), 827–903.

Hirsch, A. J. (2021). Models of electronic-will legislation. *Real Property, Trust and Estate Law Journal*, *56*(2), 163–235.

Krueger, N. (2019). Life, death, and revival of electronic wills regulation in 2016 through 2019. *Drake Law Review*, *67*, 983–1035.

Kucia, B. (2016). *Forma testamentu w systemach common law*. C.H. Beck.

Kucia, B. (2017). Testament elektroniczny – aktualne tendencje w wybranych systemach prawnych. In M. Pazdan, M. Jagielska, E. Rott-Pietrzyk, & M. Szpunar (Eds.), *Rozprawy z prawa prywatnego. Księga jubileuszowa dedykowana Profesorowi Wojciechowi Popiołkowi* (pp. 1177–1192). Wolters Kluwer.

Langbein, J. H. (2017). Absorbing South Australia's Wills Act dispensing power in the United States: Emulation, resistance, expansion. *Adelaide Law Review*, *38*, 1–11.

Melnychuk, K. (2014). One click away: The prospect of electronic wills in Saskatchewan. *Saskatchewan Law Review*, *77*, 27–43.

Millonig, M. J. (2018). Electronic wills: Evolving convenience or lurking trouble? *Estate Planning*, *45*(6), 27–38.

Osajda, K. (2010). Wpływ rozwoju techniki na uregulowanie formy testamentu – rozważania *de lege ferenda*. *Rejent*, *5*(229), 50–67.

Roy, M. D. (2011). Beyond the digital asset dilemma: Will online services revolutionize estate planning?. *Quinnipiac Probate Law Journal*, *24*(4), 376–417.

Storrow, R. F. (2022). Legacies of a pandemic: Remote attestation and electronic wills. *Mitchell Hamline Law Review*, *48*(4), 826–862.

Świrgoń-Skok, R. (2019). Wpływ nowych technologii na zagadnienie formy testamentu w polskim prawie spadkowym. *Zeszyty Prawnicze*, *19*(1), 135–151.

Visconti, O. (2021). The wills of COVID-19: The technological push for change in New York trusts and estates law. *St. John's Law Review*, *95*(3), 951–975.

Załucki, M. (2017). Kierunek zmian przepisów o formie testamentu w dobie nowych technologii na przykładzie Szwajcarii. *Białostockie Studia Prawnicze*, *30*(1), 15–25.

Załucki, M. (2018). *Videotestament. Prawo spadkowe wobec nowych technologii*. C.H. Beck.

Załucki, M. (2021). *Wills formalities versus testator's intention: Functional model of effective testation for informal wills*. Nomos.

Bialystok Legal Studies
Białostockie Studia Prawnicze
2025 vol. 30 no. 4

sciendo

DOI: 10.15290/bsp.2025.30.04.14

Received: 01.04.2025
Accepted: 10.09.2025

Łukasz Augustyniak
Wrocław University of Science and Technology, Poland
lukasz.augustyniak@pwr.edu.pl
ORCID ID: 0000–0002–4090–4480

Michał Bernaczyk
University of Wrocław, Poland
michal.bernaczyk@uwr.edu.pl
ORCID ID: 0000–0001–7683–8852

Berenika Kaczmarek-Templin
Wrocław University of Science and Technology, Poland
berenika.kaczmarek@pwr.edu.pl
ORCID ID: 0000–0003–2731–7430

Unseen Influence: Computational Propaganda, Free Elections, and the Reluctance to Seek Judicial Remedies in Poland. Evidence from AI-Assisted Case Law Analysis

Abstract: The Polish electoral system adheres to the principle of free and fair elections. This principle has a defined content, and its backbone remains access to truthful information and the free shaping of opinions about a candidate or an issue put to a referendum. However, the enormous increase in computational power and the associated development of artificial intelligence have caused electoral competition to become highly aggressive; it no longer avoids false information, messages appealing to negative emotions, or calls for violence. Very Large Online Platforms' predictable abdication of their role as moderators of public debate leads to the question: How can or should public authorities protect integrity and freedom of participation from abuse in the era of digital constitutionalism? Should we rely on a litigation system where the initiative comes solely from the participant in the electoral process, or should we also include the regulatory power of the electoral administration? What picture of electoral campaigns is provided by Polish jurisprudence concerning electoral disputes?

Keywords: artificial intelligence, digital constitutionalism, Digital Services Act, Very Large Online Platforms, political advertisement, Digital Services Coordinator

Introduction

Discussion of the advantages and disadvantages of new technologies in the electoral process inevitably leads to the hotly debated issue of freedom of expression and the classic counterargument regarding the restriction of free speech through spending limits (both financial and material). This is particularly evident in the United States, which on the one hand has created the economic conditions for the development of information technologies and artificial intelligence, while on the other it has adopted First Amendment dogma followed by a restrictive approach to state or federal attempts to limit election campaigning (de Gregorio, 2022, p. 24; Urofsky, 2020, pp. 182–183 on McCutcheon v. Federal Election Commission, 572 US 185 (2014)). European constitutionalism is therefore faced with an interesting problem: political competition methods in EU countries are using tools from technological giants which have developed them without the legal restrictions typical of the European model of protecting freedom of speech or privacy. The European approach to the issue of free campaigning is thus a consequence of a belated conclusion that Very Large Online Platforms (VLOPs) and other digital market giants have built such a strong position that their relationship with the individual (user and potential voter) has begun to resemble the relations of power exercised by the state over an individual. At the same time, it should not be expected that with their increasing influence in the digital environment, large technological entities will take responsibility for the social, political, and economic effects of that influence. The enthusiasm at the end of the first decade of the 21st century that accompanied the inauguration of large platforms faded along with naive belief in self-regulation; this happened even before the reporting of another 'AI spring' in 2018 by the Artificial Intelligence Index (an initiative of Stanford University). Ironically, in 2019, Facebook's vice president of global affairs and communications, Nick Clegg, welcomed public regulations on content moderation with a slight rhetorical enthusiasm: 'Why should a private company decide who is or isn't a legitimate participant in an election?' (Sky News, 2019). This is a fundamental shift in narrative, considering that just a year earlier, Mark Zuckerberg had said, '[i]n a lot of ways Facebook is more like government than a traditional company' (Foer, 2017). Clegg, however, showed no courtesy towards European legislatures, but merely acknowledged the state of play in the European Union, as Member States had already begun to regain control over their citizens from online platforms.[1] Giovanni

1 A turning point is considered to be the Judgment of the Court of Justice of the European Union, 2014. The issues that supported the qualification of Google as a data controller (and not a data processor) – which can be easily nuanced in the areas of civil and administrative law as a technical-legal thread – fall under typically 'constitutional' arguments, rooted in the essence of public authority: 'The Court has already held that the provisions of Directive 95/46, in so far as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must necessarily be interpreted in the light of fundamental rights, which, accord-

de Gregorio (2022, pp. 20–24) has argued that the current shape of EU secondary law concerning digital services is a consequence of the 'reclaiming of state authority' by EU Member States through the European Union law oriented to the protection of human dignity. This began in the area of personal data protection with the adoption of the now obsolete Directive 95/46/EC, and accelerated with the entry into force of the Lisbon Treaty and the granting of binding status to the EU Charter of Fundamental Rights. Leading this trend were France, which experienced failed foreign interference in the 2017 French presidential elections ('#Macron Leaks'), and Germany, which adopted the 'Netzwerkdurchsetzungsgesetz' on 1 September 2017. The culmination of this process was the entry into force of the Digital Services Act (DSA), Regulation (EU) 2022/2065, which establishes rules for online platforms, content moderation, and intermediary liability, and applies to providers of digital services, including VLOPs.[2] The DSA affects electoral law primarily by imposing obligations on online platforms to combat disinformation, enhance transparency in political advertising, and mitigate risks to democratic processes. However, it should be noted that the effectiveness of the regulation will depend on the introduction at the national level of mechanisms for flagging and assessing illegal content, in accordance with electoral law. The DSA does not establish self-standing criteria for assessing what constitutes, for example, illegal or covert campaigning (Article 3(h)), nor does it impose general obligations to monitor the transmission or storage of information by providers of intermediary services. More importantly, it does not impose general obligations on such providers to seek facts or circumstances indicating illegal activity (Article 8). This means that the DSA should not be overestimated as a tool for protecting the integrity of the electoral system unless an effective system for safeguarding fair electoral competition is first established at the national level, adapted to mass, machine-driven, microtargeted political advertising, disinformation, or other harmful content that disrupts the electoral process.

The issue is significant for Poland, as in the area of electoral law, it denied this regulatory trend through an amendment to the Electoral Code in 2018 (Sejm of Poland, 2018), despite the risk of foreign interference (Bernaczyk, 2020, pp.).[3] From the perspective of 2025, it can be concluded that the 2018 amendments were done for short-term political goals (to conceal the transfer of public funds to the campaigns of the then ruling right-wing majority), but third-party campaign deregulation, for example, came at the cost of increased national security threats (allowing agitation

ing to settled case-law, form an integral part of the general principles of law whose observance the Court ensures and which are now set out in the Charter' (§68).

2 The Digital Services Act (DSA) entered into force on 1 November 2022. However, the full application of its provisions began on 17 February 2024, due to a transitional period for platforms to adapt to the new requirements.

3 The legal framework of campaigning is shaped primarily by Section I Chapter 12 Section IX of the Electoral Code of 2011 (Sejm of Poland, 2011).

funded by unknown sources and origins). The Polish Electoral Code of 2011 did not recognize the peculiarities of electoral campaigning on the internet, nor did it foresee the development of large platforms or campaigning supported by algorithms. This is surprising, because constitutional standards do not allow for the assumption that competition in an election campaign should be based on the exercise of freedom of expression entirely free from intervention by public authorities. In 2009, a judgment by the Polish Constitutional Tribunal (2008, section III(3) of the legal reasoning) ruled that the rule-of-law clause implies the state's positive obligation to create conditions conducive to the fair and safe exercise of freedom of political expression:

> Article 2 of the Constitution implies, among other things, the legislature's duty to establish regulations that ensure a fair electoral campaign, allowing citizens access to truthful information about public affairs and candidates. The electoral campaign should facilitate the free formation of the voter's will and the making of decisions expressed through the act of voting.

This view was not new, as the Court had already outlined the essential components of free elections in 2008, including (i) 'genuine freedom of expression and assembly', (ii) 'the overall media order in the state', (iii) accessibility to the local media market, (iv) transparent procedures for obtaining the necessary financial resources for campaigning, and (v) adequate and effective guarantees for the protection of electoral rights (Judgment of the Polish Constitutional Tribunal, 2006). A distinctive feature of this reasoning is the connection between freedom of expression and the fundamental principles of the political system. There is a resemblance to the reasoning in the Romanian Constitutional Court's judgment no. 32 of 6 December 2024, on the annulment of the electoral process for the election of the president of Romania that year.[4] The Romanian court ordered the entire electoral process be repeated, deriving this conclusion primarily from the principle of national sovereignty (Article 2 of the Constitution of Romania), making Romania the first country in Europe to respond so decisively to computational propaganda deployed in national elections.[5]

Polish electoral law remains at the stage of diagnosis established relatively early in 2018, rather than of the implementation of practical solutions. The Polish National Electoral Committee (Państwowa Komisja Wyborcza) (NEC) voiced concerns regarding the electoral system on 26 September 2018, by publishing a document en-

4 In the reasons for its judgment, the Court stated that the electoral process for the presidential election in 2024 fell victim to 'the manipulation of electors' votes and the distortion of the equality of opportunity for the electoral competitors, through the non-transparent use of digital technologies and artificial intelligence in the electoral campaign, in violation of electoral legislation, and through funding from unreported sources in the electoral campaign, including the online one' (§11).

5 Samuel C. Woolley and Philip N. Howard (2016) define computational propaganda as the combination of social media platforms, independent intermediaries, algorithms, and big data technology implemented to manipulate public opinion.

titled 'The National Electoral Committee's position on the principles of conducting and financing an electoral campaign on the internet' (Państwowa Komisja Wyborcza, 2018). The NEC's communication completely departed from broadcasts on radio and television, and for the first time in Polish history, focused exclusively on the topic of electoral agitation conducted on the internet, placing the manner in which it is carried out in a rather pejorative context.[6] This allegation fell on deaf ears, which was easy to explain on a political level. The United Right (Zjednoczona Prawica, the political alliance in power from the 2015 elections until its defeat in 2023) showed no willingness to strengthen the transparency of electoral campaigns nor to adapt them to modern requirements. This does not change the constitutional paradigm, in which the Electoral Code must provide effective legal remedies against 'electoral materials, particularly posters, leaflets, and slogans, as well as statements or other forms of electoral propaganda containing false information' (Article 111 §1 of the Electoral Code).

This article aims to examine the image of electoral campaigns based on disputes conducted under Article 111 of the Electoral Code. The latter introduced a specific expedited procedure for claims in Polish law, somewhat resembling the protection against violations of personal rights but granted exclusively to candidates or authorized representatives of an interested electoral committee. We are interested in the scale of applications filed against various forms of digital campaigning, based on the reasoning of court rulings published in the Portal of Common Courts' Decisions. We believe that examining over 400,000 disclosed cases will help to answer the question of how many disputes related to digital election campaigning actually reach the courts. The use of an AI model allowed us to determine, first, what plaintiffs challenge in court as false election campaigning; second, how much digital content is contested in this manner; and finally, what the number of such cases tells us about the tendency of voters and political actors to compete in a legal way. A working hypothesis assumed that the Polish ecosystem of social and 'traditional' media (radio and linear television) has created two separate worlds, one in which election disputes are addressed by individuals and committees in courts of law, and one where there is an all-out war on social media, where the sheer speed and scale of blows exchanged between opponents make correcting misinformation through electoral procedures futile (the need for a symmetrical response outweighs the truth and accountability expected from a court's decision). We will first examine the key foundations of litigation in election-related cases; we will then provide the results of a machine-based

6 The NEC explicitly described the practice of 'political parties, election committees, candidates, and other entities participating in public life' as conducted by 'means commonly considered unethical and sometimes illegal'. The communication gives several examples of 'all kinds of messages' classified as electoral material, e.g. on websites used by electoral committees to conduct electoral agitation, but also disseminated in another form, including in the form of messages 'multiplied by persons or by automated systems on behalf of a committee' (Państwowa Komisja Wyborcza, 2018, p. 2).

analysis of Polish case law related to these matters. In the subsequent section, we will attempt to explain how the pseudo-anonymity of the digital environment may discourage the resolution of such cases in courts of law and what alternatives may be provided in the foreseeable future under national and EU law.

1. Legal proceedings against the dissemination of false information in electoral campaigns

The freedom to express opinions is linked to responsibility for both the opinions themselves and the manner in which they are expressed. Legal provisions must create the necessary conditions for this, in the interests both of those who wish to exercise their freedom of expression and of those who may be affected by it due to its content or form. Article 111 of the Electoral Code provides candidates or the official representative of an electoral committee with the ability to combat false information in electoral materials. The legal protection measures specified in Article 111, although undoubtedly the fastest, do not constitute the only legal avenue for candidates to assert their rights in court. Other available legal remedies include the right of rectification, regulated by Articles 31a–33 and 39 of the Press Law Act, as well as lawsuits for the protection of personal rights under Articles 23–24 and 448 of the Civil Code. All these proceedings are conducted under the provisions of the Code of Civil Procedure.

Court cases initiated under Article 111 of the Electoral Code are civil cases in a formal sense (Article 1 of the Code of Civil Procedure). Under the Electoral Code, their examination is subject to the provisions of the Code of Civil Procedure governing non-contentious proceedings, which means that the regulations set out in Articles 506–525 of the Code of Civil Procedure apply. However, the Electoral Code modifies the general rules, particularly concerning the timeframe of the proceedings. According to Article 111 §§2–3 of the Electoral Code, a district court examines the application within 24 hours. A district court decision may be appealed to a court of appeal within 24 hours, and the court of appeal must resolve the appeal within the same timeframe. No cassation appeal is allowed against the decision of the court of appeal, and the decision is subject to immediate enforcement. This means that from the moment of filing the application to the execution of the decision, no more than 72 hours should pass.

The extremely short timeframes for handling cases in the first and second instance aim to ensure that, on the one hand, voters can familiarize themselves with the court's findings before election day, and on the other, that the pre-election debate remains fair and free from false information (Judgment of the Constitutional Tribunal, 2008). Expedited proceedings in electoral matters come with a trade-off: a narrow list of plaintiffs (limited to a 'candidate or the election representative of the concerned electoral committee') may seek remedies for infringements not caused by the proliferation of 'any information' but only by such information that constitutes 'electoral materials, in particular posters, leaflets, and slogans, as well as statements or other

forms of electoral campaigning'. Unlike the general term 'information', a claim may concern only three types of harmful objects: electoral materials, statements, or other forms of electoral campaigning (Article 111 §2 of the Electoral Code).

'Electoral material' is not an open-ended legal term, nor is 'electioneering': both of these phrases have been defined in the Electoral Code. Electoral material is any publicly disseminated and recorded message originating from an electoral committee that is related to the announced elections (Article 109 §1 of the Electoral Code). Electioneering is the public encouragement to vote in a particular way, especially for a candidate of a specific electoral committee. Thus 'other forms of electoral campaigning' may cover third-party campaigning conducted without the consent of electoral committees, regardless of its domestic or foreign origin. This controversial issue has been raised in Poland since 2020 by the Organization for Security and Co-operation in Europe (ODIHR, 2020, p. 3), as third parties are not required to label their physical or digital forms of campaigning, which makes them difficult to identify for the purpose of expedited proceedings in electoral matters.

Another issue concerns the very concept of electioneering, which requires public encouragement, raising problems in the case of microtargeting. Microtargeting can be so sophisticated that electioneering loses the characteristics of a mass, identical ('public') message, making it difficult to classify as action falling under the traditional rules on electioneering. Last but not least, electioneering does not have to target a candidate personally, nor their electoral programme; instead, it can, for example, discourage people from voting, thereby manipulating voter turnout. This in turn can be concealed within forms of expression that blend into the general entertainment content of social media platforms, such as fostering a general aversion to the state, promoting the boycott of any civic engagement, or instilling in the audience the feeling that their civic participation is meaningless. Due to the cost of and barriers to accessing private telecommunications data, it is doubtful that electoral committees would be able to monitor the scale of such information operations.

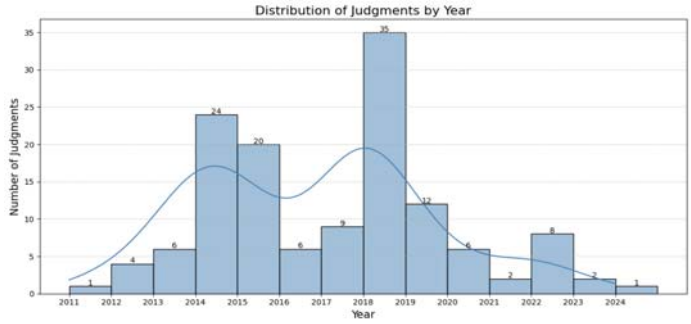
2. What does the courts' practice tell us about the nature of election-related disputes?

From the technological perspective, our examination of case law was conducted using state-of-the-art Natural Language Processing techniques and Human-In-The-Loop open-source software, developed within the JuDDGES: Judicial Decision Data Gathering, Encoding, and Sharing project.[7] The team examined Article 111 disputes re-

7 The work was partially supported by the JuDDGES project (Judicial Decision Data Gathering, Encoding and Sharing), funded by the National Science Centre (NCN), Poland, under the CHIST-ERA programme (project number 2022/04/Y/ST6/00183). Additional support was provided by the Department of Artificial Intelligence at Wroclaw University of Science and Technology.

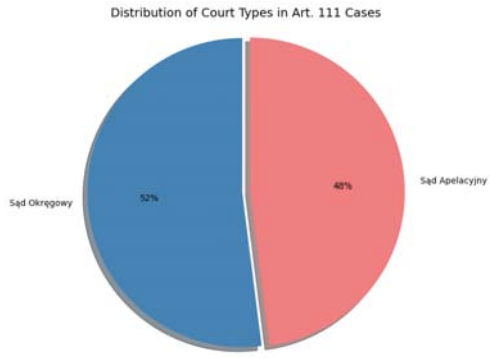
garding online campaign materials by querying over 2 million judicial decisions. After refining our search, we found 136 cases related to digital electioneering. A histogram (Figure 1) revealed the sparse number of cases, with clusters in 2014 and 2018 coinciding with local elections. Moreover, in 2015, following a few elections, we observed that the rulings within the judicial system were still for the 2014 local elections. Only two cases have been related to presidential elections. In conclusion, despite millions of rulings published and available in our internal search database, only a little more than 100 judgments have covered this topic in the past decade. This could mean that our estimates of the impact of third-party campaigning on elections might be less accurate than expected; while everyone discusses it, few take the step to file a case.

Figure 1. Number of judgments, 2011–2025.



Our research team found that judgments related to digital electioneering disputes were distributed across various courts, with 52% of the decisions coming from district courts (Sąd Okręgowy) and 48% from appellate courts (Sąd Apelacyjny) (see Figure 2). These findings underscore the involvement of various judicial levels in addressing the challenges presented by online campaign materials.

Figure 2. Type of court.



3. The problem of identifying wrongdoers on the internet

One of the most essential requirements is the identification of the parties, including their names or legal entities, and their legal representatives and attorneys, as well as their addresses (Piesiewicz & Piaskowska, 2018). Since a court is not authorized to proceed with a case without this information, an applicant seeking claims under Article 111 of the Electoral Code must identify the person engaged in an action that constitutes a violation and must demonstrate that this person engaged in the alleged conduct. The legislature has not modified the rules when the contested action in the application occurred on the internet, a VLOP, etc. Therefore the applicant must designate the participant at the stage of submitting the application, specify the unlawful action attributed to them, and subsequently prove the truthfulness of their claims before the court. The verification of the applicant's claims does not involve actions aimed at determining the identity of individuals who posted false or unlawful information on the internet, but rather whether the alleged perpetrator is indeed the one involved, as the request in the application pertains to them.

In cases of online violations, a candidate (or the electoral committee's representative) may face difficulties in determining the identity of the individual responsible, especially within the timeframe required for this specific procedure. The ECHR's position in *Staniszewski v. Poland* increases the burden put on the applicant: while the swift resolution of election-related disputes may be desirable, it should not lead to an excessive limitation of procedural guarantees granted to the parties to such proceedings, particularly the defendants.

A candidate (or an election committee representative) seeking protection for his/her rights which have been violated on the internet must apply the general rules of civil procedure. These require an entity to be identified by first name and surname (Kaczmarek-Templin, 2014); furthermore, the law imposes an obligation on the party initiating the proceedings to provide the defendant's place of residence or registered office and address (Articles 126 §1 and 187 §1, in conjunction with Article 13 §2 of the Code of Civil Procedure). The absence of this information in the application will result in the return of the statement of claim (Article 130 of the Code of Civil Procedure). Information on who specifically can be held responsible for disseminating false information during an election campaign should be obtained before the proceedings are initiated.

The Supreme Court of Poland's judgment of 6 August 2020, addressed cases involving the violation of personal rights, but the issue analysed was a more universal problem related to the identification of the party violating the rights of an injured party on the internet, which is worth examining in more detail. The Court took the position that obtaining information about the perpetrator's identity can be based on

the rules on the seizure of evidence (Articles 310 of the Civil Procedure Code).[8] In the Court's view, these provisions should allow the contact details of the potential infringer to be secured, if those details are known to a third party. This view seems to contradict the general rules related to civil procedure, namely the principle that the court cannot assist a party in actions related to determining the procedural legitimacy of the parties. The provisions on securing evidence concern assistance in determining specific circumstances from which a party derives legal consequences, rather than providing a basis for identifying the entity that should be a party in the case. Identifying the party cannot be qualified as evidence in the proceedings. Therefore the court's stance may seem to be an expression of activism, in light of the lack of legislative response to conflicts in the digital environment.

4. Blind lawsuits and forgotten expeditious examinations of election-related disputes

For years, the challenge of identifying entities acting online has been a topic of legal debate (Pązik, 2022; Wybrańczyk, 2023), leading to the emergence of the so-called 'blind lawsuit' concept, which aims to enable victims to pursue legal claims for personal rights violations even when the wrongdoer's identity cannot be determined. The first attempt to translate the concept into law came in 2017, when a draft parliamentary bill amending the Civil Procedure Code and the Telecommunications Law was submitted, but which was rejected at first reading. This draft proposed allowing the filing of a lawsuit for the violation of personal rights against a person unidentified by name, with the burden of identifying the defendant placed on the court (Sejm of Poland, 2017).

In 2024, with the submission of another parliamentary bill amending the Civil Procedure Code, the idea of the so-called 'blind lawsuit' targeted at an unknown person resurfaced (Sejm of Poland, 2024). This bill introduces a separate procedure in cases of the protection of personal rights against individuals of unknown identity. Although the draft moved away from the anachronistic (and narrow) language of the 2017 proposal, which referred to 'violations on the internet', in favour of a broader concept of 'violations through means of electronic communication', the issue for participants in electoral campaigns remains the exclusivity of this procedure. According to the proposed Article 505 §40 of the Civil Procedure Code, the provisions would apply to cases concerning the protection of personal rights if the violation occurred electronically and the plaintiff does not know the first name, surname, or address or registered office of the defendant who violated their personal rights. Upon the plaintiff's request, the court will

8 According to this regulation, even before the initiation of proceedings, the court may, at the request of the interested party, secure evidence if there is a concern that its collection will become impossible or excessively difficult, or when there is a need to confirm the existing state of affairs for other reasons.

oblige the service provider through whom the violation of personal rights occurred to send all the data it holds about the defendant, under the penalty of a fine (proposed Article 505 §42(1) of the Civil Procedure Code). However, as indicated by the aforementioned provisions, the methods of determining the identity of the violator will apply only to proceedings concerning violations of personal rights and, by analogy, cannot be applied to proceedings initiated under Article 111 of the Electoral Code, despite their similar nature. This means that even if the provisions in the so-called 'blind lawsuit' are enacted, they will be completely useless in expeditious electoral procedures. In the case of the spread of false information in electoral materials on the internet, the only way to eliminate it will be a case for the violation of personal rights, which will not have the characteristics of an expedited procedure as defined in the provisions concerning electoral campaigns. Under the general rules of procedure, it would take years for the court to issue a verdict, which contradicts the fairness of the electoral process. Given, for example, the mass automated mechanism of attacks during a campaign, an applicant would be unable to respond quickly and fight directly with the unknown violator or, more importantly, to present to the intermediary digital platforms a judgment obtained through an expeditious procedure.

Although the electoral procedure cannot be applied, the proposed amendment should be viewed positively, as the injured party will ultimately be able to pursue their rights through legal action. However, the legislative process is still pending, so we cannot yet determine whether the issue of fair electoral competition will be ignored.

Conclusions

In a situation where election materials containing false information are disseminated on the internet, the right to a court trial based on Article 111 of the Electoral Code is essentially illusory. In such a case, the possibility of initiating legal proceedings arises only from the formal right to a court (Florczak-Wątor, 2016). However, the possibility of effectively obtaining legal protection remains questionable; in fact, one could consider whether this constitutes a violation of the constitutional right to a court (Zalewski & Zdanowicz, 2025). While a rights-holder may pursue claims for the infringement of personal rights, even a favourable verdict would be futile, as it would inevitably come post-election. The analysis of case law available in the Case Law Portal supports this conclusion. The number of judgments issued under Article 111 is relatively small, and observation of internet users' activity in the pre-election period suggests that there are significantly more violations which never reach court. Thus the quantitative analysis of election disputes recorded in the official repository confirms the validity of our hypothesis that an anachronistic law, tailored to campaigns in the bygone era of analogue media (radio, linear television, physical billboards in the public space), has created two separate worlds: one in which election

disputes are addressed by individuals and committees in a court of law, and the other as all-out war on social media platforms, where no one intends to resolve conflicts in a civilized manner but rather seeks to overwhelm the opponent with aggressive and abusive messaging. The Polish framework, which fails to align with the digital environment of voter activity, cannot be reduced to a matter of mere political discretion, for electoral law that does not provide sufficient safeguards for the fairness of the electoral process falls short of a constitutional imperative.

However, there is light at the end of the tunnel, if we take into consideration the entry into force on 10 October 2025 of Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the Transparency and Targeting of Political Advertising. Publishers of political advertising will be under an obligation to label political advertisements, including (but not limited to) transparency regarding the use of microtargeting and AI systems, and to maintain records documenting the financial trail from sponsors to the final communication (see Articles 9–12 of Regulation 2024/900).[9] It should be added that political advertising disseminated by VLOPs is already subject to the transparency obligation laid down in Article 39 DSA (Jabłonowska, 2024). No less important – and indeed of primary relevance in the context of this paper – is the horizontal right of access to information (Article 17 of Regulation 2024/900) concerning political advertising granted to interested entities (vetted researchers, members of civil society organizations, political actors, national and international election observers, and journalists). Regulation 2024/900 may enhance the chances of identifying the defendant in an electoral dispute, and on top of that, it attempts to address the problem we have described concerning hostile actors, whereas these actors, by default, pursue ways to outmanoeuvre legal constraints and to blend into the political campaign ecosystem. While the Regulation adopts a solution similar to that of the Polish Electoral Code, namely by excluding from its scope political expressions made in a 'personal capacity' (Article 2 §2 of Regulation 2024/900, similar to third-party campaigning in Poland conducted outside the structures of an electoral committee), it nevertheless establishes a mechanism for detecting, inter alia, political advertisements which are suspected of concealing a professional, paid information operation disguised as grassroots campaigning (Chapters 22 and 23 of Regulation 2024/900).

Another element in safeguarding the integrity of the electoral system may be the notice-and-action mechanism provided for in Article 16 DSA. It must be stressed, however, that Regulation (EU) 2022/2065 does not contain provisions empowering platforms or public authorities to remove or block political advertising, as defined under national electoral law. Nevertheless, it does establish rules enabling the removal or dis-

9 Publishers of political advertising are defined as providers of political advertising services, usually at the end of the chain of service providers, who publish, deliver, or disseminate political advertising by broadcasting, making it available through an interface, or otherwise making it available to the public.

abling of access to such content, which in specific circumstances may overlap with the notion of electoral campaigning under Polish law or may produce equivalent campaign effects (for instance, the dissemination of the stolen internal correspondence of electoral committees, as in the Macron Leaks incident, or the 2021 hack-and-leak scandal involving the disclosure of 60,000 emails from the head of the Polish prime minister's office, Michał Dworczyk). In practice, the procedure under Article 16 DSA will be most effective where the applicant can demonstrate the unlawfulness of the content on the basis of a judicial determination rendered in expedited electoral proceedings. However, the latter is not required by the DSA, and the classification of information as illegal (including false information) may result from an autonomous legal assessment of the entity hosting the disputed information or activity (Article 16 §4 DSA).

Failure to comply with the DSA's notice-and-action procedure may result in a complaint to the president of the Office of Electronic Communications (Prezes Urzędu Komunikacji Elektronicznej), who serves in Poland as the Digital Services Coordinator. This means that this president should enjoy guarantees of independence similar to those of the supervisory authority under the GDPR, albeit less firmly anchored in EU law, since the independence of data protection supervisory authorities is based directly on the EU Charter of Fundamental Rights. National coordinators must nevertheless be granted a comparable status under domestic law by means of so-called guarantees of functional independence, which should shield them from political pressure through the manner of their appointment, fixed terms of office, and protection against removal (Łakomiec, 2024). This also gives rise to an interesting constellation in Polish constitutional law, insofar as the competence envisaged for the president of the Office of Electronic Communications to exercise authoritative powers against unlawful digital content of a political nature and/or which qualifies as electoral campaigning shall entail his/her inclusion within the broadly conceived category of the electoral administration system (Gąsior, 2015). Similarly, albeit on a narrower scale, the institutional position of the president of the Personal Data Protection Office within the constitutional framework may be assessed, as this authority is empowered to intervene in cases of the unlawful processing of personal data – for example, the public disclosure of personal data by candidates in the course of electoral campaigning, as indeed occurred during the rivalry between Nawrocki and Trzaskowski in the 2025 presidential election campaign. It should be borne in mind, however, that these are instruments of public supervision and ought to complement, rather than replace, an effective system of judicial protection through expedited electoral litigation. Nevertheless, the anachronistic character of Polish electoral law may, over time, awaken political actors' interest in the administrative powers of the president of the Office of Electronic Communications. Our analysis has confirmed that the system of judicial protection attracts only negligible interest in the context of digital campaigns – and it is these campaigns that will constitute the future of political marketing.

The absence of statutory provisions in Polish electoral law that specifically address digital election campaigning also reveals an interesting paradox: while the European Union is under constant pressure and criticism as a supranational institution that allegedly restricts the sovereignty of its Member States, it is in fact the Union that adopts measures aimed at safeguarding the integrity of the democratic electoral process against covert intervention by foreign actors and sponsors – interventions that strike at the very principle of a Member State's national sovereignty.

REFERENCES

Bernaczyk, M. (2020). Polski kodeks wyborczy wobec manipulacji i innych form propagandy obliczeniowej. In M. Bernaczyk, T. Gąsior, J. Misiuna, & M. Serowaniec (Eds.), *Znaczenie nowych technologii dla jakości systemu politycznego: ujęcie politologiczne, prawne i socjologiczne* (pp. 83–87). Uniwersytet Mikołaja Kopernika w Toruniu Wydawnictwo Naukowe.

de Gregorio, G. (2022). *Digital constitutionalism in Europe: Reframing rights and powers in the algorithmic society*. Cambridge University Press.

European Parliament and European Council. (1995, 24 October.) Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (O. J. L 281, 23.11.1995).

European Parliament and European Council. (2022, 19 October) Regulation (EU) 2022/2065 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act) (O. J. L 277).

European Parliament and European Council. (2024, 13 March). Regulation (EU) 2024/900 on the Transparency and Targeting of Political Advertising (O. J. L 2024/900, 20.03.2024).

European Union. (2000). Charter of Fundamental Rights of the European Union of 7 December 2000 (O. J. C 202, 2016).

European Union. (2007, 13 December). The Treaty of Lisbon amending the Treaty on European Union and the Treaty Establishing the European Community of 13 December 2007 (O. J. C 306).

Florczak-Wątor, M. (2016). Prawo do sądu jako prawo jednostki i jako gwarancja horyzontalnego działania praw i wolności. *Przegląd Prawa Konstytucyjnego*, *3*, 47–66.

Foer, F. (2017, 19 September), Facebook's war on free will. *The Guardian*. https://www.theguardian.com/technology/2017/sep/19/facebooks-war-on-free-will

Gąsior, T. (2015). *Kontrola finansowania komitetów Wyborczych. Zagadnienia administracyjnoprawne*, Wydawnictwo Sejmowe, Warszawa, 2015.

Jabłonowska, A. (2024). Commentary on Article 39 of the Digital Services Act (Regulation (EU) 2022/2065 of the European Parliament and of the Council. In M. Grochowski (Ed.), *Rynek Cyfrowy. Komentarz* (pp. 358–363). Wydawnictwo C.H. Beck, Warszawa.

Judgment of the Court of Justice of the European Union of 13 May 2014 on the case of *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), M. C. González*, C 131/12.

Judgment of the European Court of Human Rights of 14 October 2021 on the case of *Staniszewski v. Poland*, application no. 20422/15.

Judgment of the Polish Constitutional Tribunal of 3 November 2006, K 31/06, OTK-A 2006, no. 10, item 1.

Judgment of the Polish Constitutional Tribunal of 21 July 2008, K 7/09, OTK-A 2009, no. 7, item 113.

Judgment of the Polish Supreme Court of 6 August 2020, case no. III CZP 78/19. https://www.sn.pl/sites/orzecznictwo/OrzeczeniaHTML/iii%20czp%2078–19.docx.html

Judgment of the Romanian Constitutional Court of 6 December 2024, no. 32.

Kaczmarek-Templin, B. (2014). Odpowiedzialność administratora portalu. In M. Małek, K. Serafin, & E. Mazurek (Eds.), *Etyka i technika. Społeczne i etyczne aspekty działalności inżynierskiej* (pp. 119–126). Studium Nauk Humanistycznych i Społecznych Politechniki Wrocławskiej, Wrocław.

Łakomiec, K. (2024). Commentary on Article 50 of the Digital Services Act (Regulation (EU) 2022/2065 of the European Parliament and of the Council. In M. Grochowski (Ed.), *Rynek Cyfrowy. Komentarz* (pp. 421–424). Wydawnictwo C.H. Beck, Warszawa.

Office for Democratic Institutions and Human Rights. (2020, 23 September). *Republic of Poland: Presidential election, 28 June and 12 July 2020. ODIHR Special election assessment mission final report*. https://www.osce.org/files/f/documents/6/2/464601.pdf

Państwowa Komisja Wyborcza. (2018). National Electoral Committee's position on the rules for conducting and financing an electoral campaign on the internet of 26 September 2018 (ZKF-811–850/18), op. https://pkw.gov.pl/uploaded_files/1537988216_1–50-18.pdf

Pązik, A. (2022). Ślepy pozew i krótkowzroczny ustawodawca': uwagi na marginesie projektu ustawy o wolności słowa w Internecie. In B. Fischer, A. Pązik, & M. Świerczyński (Eds.), *Prawo sztucznej inteligencji i nowych technologii* (pp. 367–397). Wolters Kluwer.

Piesiewicz, P., & Piaskowska, O. (2020). Ustalenie danych osobowych sprawcy naruszenia dóbr osobistych w Internecie celem dochodzenia ich ochrony w postępowaniu cywilnym. *Zeszyty Naukowe Katolickiego Uniwersytetu Lubelskiego Jana Pawła II*, *61*(2), 277–289. https://doi.org/10.31743/zn.2018.61.2.277–289.

Sejm of Poland. (2018). Act of 11 January 2018 Amending Certain Acts in Order to Increase Citizens' Participation in the Process of Election, Functioning and Control of Certain Public Bodies (Journal of Laws of 2018, item 130).

Sejm of Poland. (2024). Parliamentary Bill no. 728 Amending the Code of Civil Procedure Act and Certain Other Laws.

Sky News. (2019, 25 June), *Sir Nick Clegg: Facebook welcomes government regulation*. https://news.sky.com/story/sir-nick-clegg-link-between-social-media-and-mental-health-problems-not-proven-11748174

Urofsky, M. I. (2020). *The campaign finance cases:* Buckley*,* McConnell*,* Citizens United *and* McCutcheon. University Press of Kansas.

Woolley, S. C., & Howard, P. N. (2016). Political communication, computational propaganda, and autonomous agents. *International Journal of Communication*, *10*, 4886.

Wybrańczyk, D. (2023). Propozycja wprowadzenia do procedury cywilnej tzw. ślepych pozwów. *Zeszyty Prawnicze Biura Analiz Sejmowych Kancelarii Sejmu*, *1*, 159–173.

Zalewski, M., & Zdanowicz, U. (2025). Realność ochrony dóbr osobistych naruszonych za pośrednictwem internetu a konstytucyjna gwarancja prawa do sądu. *Palestra*, *1*, 176–191.

Bialystok Legal Studies
Białostockie Studia Prawnicze
2025 vol. 30 no. 4

sciendo

DOI: 10.15290/bsp.2025.30.04.15

Received: 23.03.2025
Accepted: 26.09.2025

Tomasz Szanciło
Europejska Wyższa Szkoła Prawa i Administracji, Polska
tszancilo@ewspa.edu.pl
ORCID ID: 0000–0001–6015–6769

Jawność postępowania gospodarczego a elektronizacja procesu cywilnego

The Openness of Commercial Proceedings and the Digitisation of Civil Proceedings

Abstract: The principle of openness is a guiding principle of the organisation of justice; the right to an open hearing of a case, inter alia a civil case, is a human right, although not an absolute one. Therefore the digitisation of the civil process should not affect this right. All forms of digitisation are in practice really concerned with the technical and not the substantive aspects of the proceedings. Technical innovations aimed at improving the civil process should be introduced primarily in commercial cases; in the digital age, this does not infringe on the right to a court. Before attempting to apply artificial intelligence to the adjudication of court cases (if that is really possible), it would be advisable first to completely digitise the civil process, especially commercial proceedings.

Key words: commercial proceedings, openness of proceedings, digitisation, artificial intelligence, ICT systems, electronic delivery
Słowa kluczowe: postępowanie gospodarcze, jawność postępowania, elektronizacja, sztuczna inteligencja, system teleinformatyczny, doręczenia elektroniczne

Wprowadzenie

Zasada jawności jest naczelną zasadą organizacji wymiaru sprawiedliwości, wynikającą nie tylko z międzynarodowych aktów prawnych, w szczególności art. 6 ust. 1 EKPC (Rada Europy, 1950), lecz także z najwyższej rangi prawa krajowego (art. 45 Konstytucji RP). Prawo do jawnego (publicznego) rozpoznania sprawy, m.in. cywilnej, jest prawem człowieka i stanowi jeden z elementów prawa do sądu, do rzetelnego procesu sądowego ustanowionego w tych przepisach. W założeniu postępowanie przed sądem ma być jawne, a ograniczenia w tej materii powinny mieć uzasadnienie.

W związku z tym elektronizacja (cyfryzacja) procesu cywilnego nie powinna mieć wpływu na to uprawnienie stron.

Można postawić hipotezę, że chociaż modne jest aktualnie pojęcie „e-sąd", to elektronizacja procesu cywilnego jest dopiero na początkowym etapie, dotyczy tak naprawdę technicznych, a nie merytorycznych aspektów i nie jest wykorzystywana nawet w ramach postępowania gospodarczego, które powinno być w jak największej mierze zelektronizowane, a jednocześnie nie wpływa na zasadę jawności. W tej materii powinna nastąpić jak najszybsza intensyfikacja prac. Chodzi przede wszystkim o wnoszenie pism procesowych, doręczenia, przeprowadzenie odmiejscowionej rozprawy itp., a nie o realny wpływ nowinek technicznych na merytoryczne rozstrzygnięcie sprawy. Istotne znaczenie miała w tej materii epidemia COVID-19 i rozwiązania zawarte w ustawie COVID-19 (Sejm RP, 2020b). Zmiana aspektów technicznych jest związana przede wszystkim z odpowiednimi nakładami finansowymi i rzeczowymi na sądownictwo.

Stosując metodę dogmatyczno-prawną, która pozwala przeanalizować ustawowe rozwiązania w omawianej materii, trzeba podkreślić, że celem opracowania nie jest opisanie technicznych ich aspektów, ale ich analiza w kontekście zasady jawności postępowania. Innymi słowy, należy ustalić, czy elektronizacja postępowania cywilnego (w tym wypadku postępowania gospodarczego) ma istotny wpływ na tę zasadę. Pominięto przy tym potencjalne (bo jak na razie nierealne) możliwości związane z wykorzystaniem AI do merytorycznego rozpoznania różnych kategorii spraw cywilnych, co było przedmiotem innego opracowania (Szanciło, 2024, s. 7 i nast.). Generalnie, chociaż toczy się dyskusja na temat zastosowania AI do rozpoznawania spraw, to należałoby zacząć od zelektronizowania postępowania cywilnego, w tym w szczególności postępowania gospodarczego, a więc od czegoś, co jawi się jako znacznie łatwiejsze, a w praktyce nadal jest dalekie od wykonania (chociażby w tak prozaicznej materii, jaką jest digitalizacja akt sądowych).

1. Ograniczenia zasady jawności

Zasada jawności stanowi jedną z gwarancji bezstronności sędziego i rzetelności procesu (Łazarska, 2012, s. 46 i nast.). Podkreśla się jej wymiar społeczny, gdyż jawny przebieg postępowania pełni funkcje edukacyjną i wychowawczą, przyczyniając się do zwiększenia zaufania społeczeństwa do wymiaru sprawiedliwości (Rylski, Zembrzuski, 2006, s. 84). Ma na celu również zmobilizowanie sądu do jak największej staranności i sumienności przy dokonywaniu czynności procesowych, w tym w szczególności przy merytorycznym rozpoznaniu sprawy. Jeżeli strona ma możliwość obecności na rozprawie, zapoznawania się na bieżąco z czynnościami w sprawie, posiada realną możliwość realizacji swoich praw procesowych. Dzięki temu

strona zyskuje również przeświadczenie, że dotyczące jej postępowanie jest zrozumiałe i sprawiedliwe (Góra-Błaszczykowska, 2008, s. 131).

Ograniczenia zasady jawności wynikają z art. 6 ust. 1 EKPC i art. 45 ust. 2 Konstytucji RP, a dotyczą aspektów związanych z porządkiem publicznym, bezpieczeństwem państwa, dobrem małoletnich, ochroną życia prywatnego stron albo okoliczności szczególnych, w granicach uznanych przez sąd za bezwzględnie konieczne, kiedy jawność mogłaby przynieść szkodę interesom wymiaru sprawiedliwości. Są to oczywiście pojęcia nieostre (niedookreślone), przenoszone do ustawodawstw krajowych, a następnie każdorazowo stosowane w realiach konkretnej sprawy przez sądy krajowe, przy czym standard konwencyjny musi przynajmniej zostać zachowany (ustawodawca krajowy nie może wprowadzić dalej idących ograniczeń).

Z art. 9 § 1 zd. 1 k.p.c. wynika, że rozpoznawanie spraw odbywa się jawnie, chyba że przepis szczególny stanowi inaczej. Analogicznie, zgodnie z art. 42 § 2 i 3 u.s.p. (Sejm RP, 2001), sądy rozpoznają i rozstrzygają sprawy w postępowaniu jawnym, a rozpoznanie sprawy w postępowaniu niejawnym lub wyłączenie jawności postępowania jest dopuszczalne jedynie na podstawie przepisów ustaw.

Nie powinno zatem dojść do ograniczenia – ponad niezbędne minimum – tzw. jawności zewnętrznej, gdyż tylko tej mogą one dotyczyć – w wyniku tego rozprawa lub jej część zostaje przeprowadzona przy drzwiach zamkniętych (w procesie art. 153–154, 427 k.p.c.). Jawność zewnętrzna (zwana publicznością postępowania) wzmacnia gwarancje transparentności poczynań sądu i jego publiczną kontrolę przez dostępność posiedzeń sądowych dla opinii publicznej, w tym osób trzecich (mediów), a także możności wysłuchania wyroku (Gołąb, 2024, Komentarz do art. 9, Nt 3), nawet jeżeli cała rozprawa odbyła się przy drzwiach zamkniętych. Jawne posiedzenia stanowią dla osób trzecich źródło informacji o sprawie i przebiegu postępowania cywilnego, gdyż nie mają one – w przeciwieństwie do stron tego postępowania – nieograniczonego dostępu do akt sprawy. W postępowaniu procesowym tylko strony mają prawo przeglądać akta sprawy i otrzymywać odpisy, kopie lub wyciągi z tych akt (art. 9 § 1 zd. 2 k.p.c.), a skuteczność żądania ich wydania jest uzależniona wyłącznie od uiszczenia opłaty kancelaryjnej (Postanowienie Sądu Najwyższego, 1997). Jedynie na podstawie przepisu szczególnego ten dostęp może zostać ograniczony, np. w przypadku tajemnicy przedsiębiorstwa lub innej tajemnicy podlegającej ochronie na podstawie odrębnych przepisów – w sprawach antymonopolowych (art. 479^{33} k.p.c.) czy w sprawach z zakresu telekomunikacji i poczty (art. 479^{66a} k.p.c.). Nie ma tu zastosowania art. 525 k.p.c., dotyczący postępowania nieprocesowego, przewidujący szerszy dostęp do akt sprawy.

Trybunał strasburski przyjmuje, że wyłączenie jawności postępowania musi spełniać wymogi proporcjonalności – jest zatem dopuszczalne, gdy wyłączenie to rzeczywiście służy celom wynikającym z art. 6 ust. 1 zd. 2 EKPC, nie jest możliwe zrealizowanie tych celów w inny sposób niż przez wyłączenie jawności postępowania i istnieje odpowiedni stosunek między wskazanymi w tym przepisie podstawami wy-

łączenia jawności a interesem przemawiającym za jawnością postępowania (Hofmański & Wróbel, 2010, s. 363–364). Nie ma natomiast możliwości wyłączenia czy nawet ograniczenia tzw. jawności wewnętrznej, która dotyczy stron procesu, gdyż nawet w przypadku zarządzenia przez sąd (postanowieniem) posiedzenia przy drzwiach zamkniętych mogą być obecni na sali m.in. strony, ich przedstawiciele ustawowi i pełnomocnicy oraz osoby zaufania po dwie z każdej strony (art. 154 § 1 zd. 1 k.p.c.). Ograniczenie jawności wewnętrznej, a tym bardziej jej wyłączenie, może prowadzić do nieważności postępowania z uwagi na pozbawienie strony możności obrony jej praw (art. 379 pkt 5 k.p.c.) i stanowić podstawę wznowienia postępowania (art. 401 pkt 2 k.p.c.). Jawność wewnętrzna stanowi bowiem podstawowy element sprawiedliwości proceduralnej i prawa do sądu (Wyroki Trybunału Konstytucyjnego, 2002, 2006, 2007, 2010). Przejawia się ona w prawie strony do wysłuchania, udziału w postępowaniu sądowym, zapoznania się ze stanowiskiem strony przeciwnej i dostępie do akt sądowych. Strona powinna być informowana w szczególności o czynnościach sądu (przewodniczącego), posiedzeniach sądowych, czynnościach strony przeciwnej. Prawo do wysłuchania polega na możliwości przedstawiania swojego stanowiska w sprawie w formie ustnej lub pisemnej. Może to nastąpić ustnie na posiedzeniach sądowych (jawnych lub wyznaczonych na rozprawę) lub pisemnie poza nimi (Ereciński & Weitz, 2010, s. 53). Oczywiście, zgodnie z zasadą dyspozytywności, to od strony procesu zależy, czy korzysta z przysługujących jej praw, ale nie może zostać pozbawiona takiej możliwości.

O ile zatem załatwienie sprawy sądowej na publicznej rozprawie jest najbardziej pożądanym konstytucyjnie rozwiązaniem (Wyrok Trybunału Konstytucyjnego, 20 listopada 2007) i w świetle art. 148 § 1 k.p.c. stanowi podstawowe rozwiązanie w procesie, o tyle, jeżeli sąd orzeknie na posiedzeniu niejawnym, samo w sobie nie oznacza to pozbawienia strony prawa do wysłuchania. Taka możliwość została przewidziana w art. 148^1 § 1 k.p.c. (w I instancji) i art. 374 zd. 1 k.p.c. (w II instancji). Ma to na celu przyśpieszenie rozpoznania sprawy, a dotyczy sytuacji, w których wyznaczenie rozprawy jest zbędne. Pomimo tego zostało to obwarowane przede wszystkim brakiem wniosku o przeprowadzenie rozprawy (przy czym możliwe jest zrzeczenia się przez stronę prawa do jawnego rozpatrzenia sprawy – wyroki Europejskiego Trybunału Praw Człowieka, 1993, 1997, 2006). Jak się słusznie wskazuje, istotne jest, czy przed posiedzeniem niejawnym strona miała możliwość przedstawienia stanowiska w formie pisemnej (Wyroki Trybunału Konstytucyjnego, 3 lipca 2007, 19 września 2007); ponadto trzeba pamiętać o możliwości wysłuchania na dalszym etapie postępowania w wyniku zaskarżenia orzeczenia zapadłego na posiedzeniu niejawnym (Wyrok Trybunału Konstytucyjnego, 2011; odmiennie wyrok Trybunału Konstytucyjnego, 20 listopada 2007). Oczywiste jest przy tym, że w kwestiach formalnych wymagania dotyczące wyznaczenia rozprawy nie mogą być tak restrykcyjne, czego wynikiem jest zasada, że sąd może wydać postanowienie na posiedzeniu niejawnym (art. 148 § 3 k.p.c.).

Podkreśla się przy tym, że jeżeli sprawa jest rozpoznawana w postępowaniu pisemnym, strona powinna mieć prawną możliwość, aby na dalszym etapie lub w kolejnej fazie postępowania zostać wysłuchana na rozprawie (Gołąb, 2020, s. 100 i nast.). Spełnia zatem standard z art. 6 ust. 1 EKPC odstąpienie od przeprowadzenia rozprawy w postępowaniu wywołanym wniesieniem środka zaskarżenia, jeżeli to prawo zostało zrealizowane w pierwszej instancji, i przeprowadzenie rozprawy dopiero na etapie postępowania apelacyjnego, jeżeli wcześniej strona nie została na niej wysłuchana (Wyroki Europejskiego Trybunału Praw Człowieka, 1990, 2000, 2003, 2005; Mayer, 2022, s. 180–181). W związku z tym ten standard spełnia postępowanie w przedmiocie wydania nakazu zapłaty w postępowaniu upominawczym lub nakazowym, gdyż wniesienie środka zaskarżenia – odpowiednio sprzeciwu lub zarzutów – umożliwia przeprowadzenie rozprawy z udziałem strony procesu. Jeżeli natomiast sprawa jest rozpoznawana tylko w jednej instancji, prawo do „publicznego wysłuchania" obejmuje prawo do „ustnego wysłuchania", chyba że istnieją wyjątkowe okoliczności uzasadniające odstąpienie od takiego wysłuchania, przy czym takie odstępstwo nie powinno dotyczyć roztrząsania dowodów w celu ustalenia podstawy faktycznej (Wyroki Europejskiego Trybunału Praw Człowieka, 1994, 1998 i powołane tam orzecznictwo). W konsekwencji decyzja ustawodawcy dotycząca tego, czy sprawa ma być załatwiana na publicznej rozprawie, posiedzeniu jawnym lub posiedzeniu niejawnym, powinna uwzględniać m.in. przedmiot sprawy, charakter postępowania, cel i etap postępowania oraz zakres kognicji sądu (Grzegorczyk & Weitz, 2016, s. 1135).

2. Aspekty elektronizacji postępowania gospodarczego

2.1. Postępowanie gospodarcze jako pole dla „eksperymentów"

Powyższe unormowania powinny oddziaływać na szczegółowe rozwiązania zawarte w ustawach procesowych, w tym związane z zastosowaniem nowych technologii, aby przyśpieszyć rozpoznawanie spraw, gdyż taki powinien być cel wprowadzenia do postępowania sądowego (nie tylko cywilnego) nowych rozwiązań. Dotyczy to również postępowania gospodarczego, które zostało wyodrębnione właśnie w celu przyśpieszenia rozpoznawania spraw, nawet kosztem pewnych ograniczeń co do przedmiotowego i podmiotowego zakresu postępowania (np. w odniesieniu do zmian przedmiotowych i podmiotowych, wnoszenia pozwu wzajemnego), czy postępowania dowodowego (w szczególności co do prekluzji dowodowej). Ponieważ jest to jedno z odrębnych postępowań procesowych, w pierwszej kolejności zastosowanie mają przepisy szczególne, którymi są art. 458^1 i n. k.p.c., a w kwestiach nieuregulowanych – przepisy ogólne postępowania cywilnego (procesowego). W związku z tym nawet jeżeli konkretne rozwiązanie nie zostało (lub nie zostałoby) zawarte w przepisach ogólnych, a więc dotyczących wszystkich postępowań cywilnych, to nic nie stoi

na przeszkodzie, aby zawrzeć takie rozwiązanie właśnie w przepisach regulujących postępowanie odrębne w sprawach gospodarczych.

Sprawy gospodarcze można podzielić na sprawy gospodarcze *sensu stricto* (związane z działalnością gospodarczą prowadzoną przez strony będące przedsiębiorcami) oraz sprawy gospodarcze *sensu largo* (niezwiązane z działalnością gospodarczą prowadzoną przez obie strony, ale co do których ustawodawca uznał, że powinny być rozpatrywane w postępowaniu odrębnym w sprawach gospodarczych z uwagi na swoją specyfikę). Są to więc sprawy gospodarcze w znaczeniu materialnym oraz formalnym (szerzej: Szanciło, 2023, s. 1957).

Jedną z kluczowych kwestii jest elektronizacja postępowania, w tym postępowania gospodarczego, już na etapie komunikacji z sądem. Do tego nie są potrzebne AI ani szczególnie wyszukane rozwiązania prawne. Warunkiem wszczęcia postępowania sądowego, ale również odwoławczego i kasacyjnego, jest skuteczne wniesienie do sądu stosownego pisma procesowego. Zasadą jest wniesienie pisma w tradycyjnej formie pisemnej – bezpośrednio w siedzibie sądu (w biurze podawczym), za pośrednictwem określonego operatora pocztowego (art. 165 § 2 k.p.c.) albo za pośrednictwem dowództwa jednostki wojskowej, administracji zakładu karnego lub kapitana statku (art. 165 § 3 k.p.c.). Inna forma powinna wynikać z przepisu szczególnego, przy czym wyjątków od ogólnej zasady wnoszenia pism procesowych nie można interpretować rozszerzająco.

Dla rozwiązania problemu komunikacji z sądem prawidłowy kierunek (aczkolwiek nieprawidłowo sformułowany) wyznaczał art. 458^3 k.p.c., który wszedł w życie 7 listopada 2019 r. (Sejm RP, 2019), a został uchylony 1 lipca 2023 r. (Sejm RP, 2023b). W tym przepisie pojawiło się *novum* w polskiej procedurze cywilnej, którym był obowiązek wskazania przez strony (w pierwszym piśmie procesowym) adresu poczty elektronicznej strony (e-maila) lub złożenia oświadczenia, że takiego adresu nie posiada. Był to bardzo dobry kierunek, gdyż tego typu rozwiązanie, niewątpliwie, ułatwia kontakt ze stronami postępowania gospodarczego (Szczurowski, 2019, s. 42). Chodzi przede wszystkim o doręczenia w formie elektronicznej (nie tylko w ramach systemu teleinformatycznego), co w oczywisty sposób przyspiesza postępowanie. Tego rodzaju obowiązek (wskazanie adresu poczty elektronicznej) w praktyce nie stanowi problemu szczególnie dla osób prowadzących działalność gospodarczą, a wręcz nie jest możliwe prowadzenie takiej działalności bez posiadania adresu poczty elektronicznej. Adres poczty elektronicznej strony, o którym stanowił art. 458^3 § 1 i 2 k.p.c., służył jednak tak naprawdę wyłącznie doręczeniu stronie przez sąd w formie elektronicznej pouczeń wymienionych w art. 458^4 § 1 k.p.c., nie uregulowano bowiem innej funkcji adresu poczty elektronicznej właściwej dla przebiegu postępowania w sprawach gospodarczych (Feliga, 2024, Komentarz do art. 458^3, Nt 17). Problem był zatem taki, że ta regulacja nie służyła upowszechnieniu doręczeń za pośrednictwem poczty elektronicznej, co było tym dziwniejsze, że niewskazanie przez stronę adresu poczty elektronicznej lub niezłożenie oświadczenia, że takiego adresu

nie posiada, stanowiło brak formalny złożonego pisma procesowego uniemożliwiający nadanie mu biegu. Co więcej, ustawodawca nie przewidział żadnych negatywnych konsekwencji, jeżeli strona nie wskazała adresu e-mail, składając oświadczenie, że takiego nie posiada – to oświadczenie nie podlegało bowiem żadnej weryfikacji.

W art. 458^3 § 1 i 2 k.p.c. nie zrealizowano zatem idei komunikacji elektronicznej z sądem poza systemem teleinformatycznym. O ile oczywiste jest, że nie wszystkie sprawy wymienione w art. 458^2 § 1 k.p.c. są związane z prowadzoną działalności gospodarczą, jak również, że nie każdy musi posiadać adres poczty elektronicznej, o tyle obecnie nie stanowi to żadnego problemu, szczególnie w przypadku przedsiębiorców. Nie można również zapominać, że w sprawach gospodarczych strony są zwykle reprezentowane przez profesjonalnych (zawodowych) pełnomocników. Można przyjąć, że postępowanie w sprawach gospodarcze stanowi idealne pole do wprowadzenia wszelkich zmian dotyczących prowadzenia postępowania w formie elektronicznej. Tymczasem ustawodawca zamiast znowelizować art. 458^3 k.p.c. we właściwym kierunku, uchylił go, nie wprowadzając w to miejsce żadnego tego typu rozwiązania. Do postępowania gospodarczego mają zastosowanie zasady ogólne, które w praktyce w znacznej mierze nie funkcjonują (o czym będzie mowa poniżej). Wskazanie adresu poczty elektronicznej w tych postępowaniach powinno być obligatoryjne i za pośrednictwem tego adresu powinny być dokonywane wszelkie doręczenia, niezależnie, czy strona jest reprezentowana przez profesjonalnego pełnomocnika.

Podobne rozwiązanie zawarto w nieobowiązującym art. $15zzs^9$ ustawy COVID-19 (zob. Sejm RP, 2023a), zgodnie z którym w okresie obowiązywania stanu zagrożenia epidemicznego albo stanu epidemii ogłoszonego z powodu COVID-19 oraz w ciągu roku od odwołania ostatniego z nich, w sprawach prowadzonych przy użyciu urządzeń technicznych umożliwiających przeprowadzenie rozprawy lub posiedzenia na odległość, w pierwszym piśmie procesowym wnoszonym przez adwokata, radcę prawnego, rzecznika patentowego lub Prokuratorię Generalną Rzeczypospolitej Polskiej podawało się adres poczty elektronicznej i numer telefonu przeznaczone do kontaktu z sądem, a niewykonanie tego obowiązku stanowiło brak formalny pisma.

2.2. System teleinformatyczny

Przepisem szczególnym dotyczącym formy pism procesowych jest art. 125 § 2^1 zd. 1 k.p.c., zgodnie z którym takie pisma wnosi się do sądu za pośrednictwem systemu teleinformatycznego, jeżeli przepis szczególny tak stanowi albo dokonano wyboru wnoszenia pism procesowych za pośrednictwem takiego systemu. Wprowadzenie pisma do systemu teleinformatycznego jest równoznaczne z wniesieniem pisma do sądu (art. 165 § 4 k.p.c.). Podstawowe znaczenie mają tu rozporządzenia wykonawcze (Minister Sprawiedliwości, 2015, 2021). Ten system został stworzony i ustanowiony *stricte* do obsługi postępowania sądowego, a więc nie służy jedynie porozumiewaniu się z sądem.

Jak podkreślono w orzecznictwie, w przepisach regulujących postępowanie cywilne – jako drogę kontaktowania się stron z sądem w postępowaniu sądowym – nie przewidziano ani poczty mailowej, ani Platformy Usług Administracji Publicznej e-PUAP, służącej do komunikacji obywateli z jednostkami administracji publicznej. Pismo procesowe złożone w postaci elektronicznej – w zakresie nieunormowanym szczególnymi przepisami – nie wywołuje skutków prawnych, które ustawa wiąże z jego złożeniem, przy czym nie chodzi o brak formalny pisma, lecz o jego pierwotny, nieusuwalny brak skuteczności spowodowany użyciem nieautoryzowanej techniki. Uzupełnianie tej luki prawnej za pomocą wykładni rozszerzającej przepisów o charakterze formalnym nie jest dopuszczalne i może prowadzić do negatywnych skutków. Dopóki zatem ustawodawca nie otworzy szerszej, uwzględniającej rozwój technologii, drogi wnoszenia pism procesowych, przesłanie pisma do sądu mailem czy też za pośrednictwem platformy e-PUAP nie wywołuje skutków procesowych i nie wymaga podjęcia przez sąd czynności o charakterze faktycznym (wydrukowanie załącznika do maila) i procesowym (usunięcia braków formalnych jako pisma procesowego, którym nie jest). Strona powinna natomiast zostać poinformowana o bezskuteczności tej czynności w trybie pozaprocesowym (Postanowienie Sądu Najwyższego, 29 marca 2023). Ten pogląd, zgodny z obowiązującymi przepisami, pokazuje, w jakim miejscu znajduje się polskie prawo, jeżeli chodzi o omawianą materię.

Zgodnie z art. 3 pkt 3 ustawy z 2005 r. (Sejm RP, 2005) system teleinformatyczny jest zespołem współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniającym przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy – Prawo komunikacji elektronicznej (Sejm RP, 2024). System teleinformatyczny w postępowaniu gospodarczym nie ma obligatoryjnego zastosowania, a ogólnie w procesie – jest to wyjątek, gdyż dotyczy tylko elektronicznego postępowania upominawczego (EPU; art. 505^{28} i nast.), z tym że jest to obligatoryjne tylko dla powoda, a pozwany może wybrać wnoszenie pism procesowych za pośrednictwem systemu teleinformatycznego (art. 505^{31} § 1 i 2 k.p.c.).

W art. 125 § 2^1 i 2^{1a} k.p.c. ustawodawca poszerzył zaś możliwość korzystania przez strony z systemu teleinformatycznego w każdym postępowaniu sądowym, gdyż strony mogą wybrać wnoszenie pism procesowych za pośrednictwem tego systemu – wówczas wniesienie pisma w ten sposób staje się obligatoryjne. Oświadczenie zarówno o wyborze, jak i rezygnacji z wyboru wnoszenia pism procesowych za pośrednictwem systemu teleinformatycznego powinno być złożone poprzez ten system, w przeciwnym razie będzie bezskuteczne. Takie oświadczenie wiąże tylko osobę składającą, a więc nie czyni tego wobec przeciwnika procesowego (innych uczestników postępowania). Żadnego z tych oświadczeń nie trzeba uzasadniać, nie są to bowiem oświadczenia woli.

Warunkiem jest jednak to, aby z przyczyn technicznych leżących po stronie sądu było to możliwe. Jest to spowodowane aktualnym niedostosowaniem systemów sądowych (i samych sądów) do możliwości wnoszenia pism procesowych w każdej sprawie tą drogą. Ustawodawca uzależnił więc możliwość skorzystania przez strony z systemu teleinformatycznego w zależności od możliwości technicznych i przestawienia się sądów na informatyczny obieg dokumentów w sprawie cywilnej. Jest to związane z nakładami na sądownictwo. Tak naprawdę możliwość wyboru skorzystania z systemu teleinformatycznego jest w praktyce iluzoryczna, chociaż stan taki miał trwać (pierwotnie) nie dłużej niż przez 3 lata, licząc od 8 września 2016 r. (zob. art. 20 Sejm RP, 2015, uchylony Sejm RP, 2019; postanowienie Sądu Apelacyjnego w Katowicach, 27 lutego 2017). Na chwilę obecną taki wybór jest niemożliwy z uwagi na techniczne braki systemów teleinformatycznych obsługujących postępowania sądowe w procesowych sprawach cywilnych inne niż EPU. W konsekwencji także ze strony sądu nie może mieć miejsca odstępstwo od doręczeń przez operatora pocztowego, osoby zatrudnione w sądzie lub sądową służbę doręczeniową, ewentualnie przez komornika, Policję lub Żandarmerię Wojskową (art. 131 § 1 i 1^1 k.p.c.). Jedynie bowiem, gdy strona wniosła (obligatoryjnie) pismo za pośrednictwem systemu teleinformatycznego albo dokonała wyboru wnoszenia pism za pośrednictwem tego systemu (fakultatywnie), sąd również dokonuje doręczeń za pośrednictwem systemu teleinformatycznego (art. 131^1 § 1 k.p.c.). Nie jest to zatem problem wyłącznie postępowania gospodarczego, w którym korzystanie z systemu teleinformatycznego powinno być obligatoryjne (dla obu stron, bez względu na to, czy są one reprezentowane przez profesjonalnego pełnomocnika), ale całego postępowania cywilnego.

2.3. Inne doręczenia elektroniczne

Ustawą o doręczeniach elektronicznych (Sejm RP, 2020a; dalej: u.d.e.) wprowadzono prawne ramy dla doręczeń elektronicznych nie tylko w postępowaniu cywilnym (i nie tylko w ramach systemu teleinformatycznego w powyższym rozumieniu), lecz także w ogóle w usługach publicznych. W przypadku postępowania cywilnego kluczowy jest art. 131^2 § 1 k.p.c., który uzależnia możliwość dokonywania doręczeń na adres do doręczeń elektronicznych, o którym mowa w art. 2 pkt 1 u.d.e., wpisany do bazy adresów elektronicznych, o której mowa w art. 25 tej ustawy, zaś w przypadku braku takiego adresu – na adres do doręczeń elektronicznych powiązany z kwalifikowaną usługą rejestrowanego doręczenia elektronicznego, z którego adresat wniósł pismo – „jeżeli warunki techniczne i organizacyjne sądu to umożliwiają" (podobnie art. 125 § 5 k.p.c.). Co więcej, w przypadku osoby fizycznej będącej stroną (za wyjątkiem przedsiębiorców wpisanych do Centralnej Ewidencji i Informacji o Działalności Gospodarczej) takiego doręczenia można dokonać tylko wtedy, gdy wniosła ona pismo z adresu do doręczeń elektronicznych albo wskazała ten adres jako adres do doręczeń.

Zgodnie z Komunikatem Ministra Cyfryzacji z dnia 29 maja 2023 r. pierwotny termin wdrożenia rozwiązań technicznych niezbędnych do doręczania korespondencji z wykorzystaniem publicznej usługi rejestrowanego doręczenia elektronicznego lub publicznej usługi hybrydowej oraz udostępnienia w systemie teleinformatycznym punktu dostępu do usług rejestrowanego doręczenia elektronicznego w ruchu transgranicznym określono na 10 grudnia 2023 r. Aktualnie jest to 1 stycznia 2025 r. Termin ten nie został dochowany.

Powyższe zadania częściowo spełnia Portal Informacyjny Sądów Powszechnych, który funkcjonuje od kilku lat (podstawę prawną do doręczeń elektronicznych pism sądowych za pośrednictwem tego portalu wprowadziła ustawa z dnia 28 maja 2021 r.), przy czym słusznie wskazuje się, że ustawodawca nie był w stanie stworzyć odpowiedniego systemu teleinformatycznego, dlatego wykorzystano już istniejący Portal Informacyjny, co naturalnie było dotknięte problemami i niedostatkami (Cygan, 2025, s. 247). Swoiste *novum* stanowi art. 131^{1a} § 1 k.p.c., który wszedł w życie 14 marca 2024 r. (zob. art. 1 pkt 2 i art. 40 ustawy z dnia 7 lipca 2023 r.) i stanowi powtórzenie (z rozszerzonym zakresem podmiotowym) nieobowiązującego już art. $15zzs^{9}$ § 2 ustawy COVID-19. Zgodnie z art. 39 ust. 3 ustawy z dnia 7 lipca 2023 r. czynności dokonane przed dniem wejścia w życie tej ustawy zgodnie z art. $15zzs^{9}$ ustawy COVID-19 uważa się za czynności dokonane zgodnie z art. 131^{1a} k.p.c. Przepis kodeksowy reguluje doręczanie przez sąd pism sądowych (o ile nie istnieje możność doręczenia za pośrednictwem systemu teleinformatycznego) profesjonalnym pełnomocnikom (adwokatom, radcom prawnym, rzecznikom patentowym), Prokuratorii Generalnej Rzeczypospolitej Polskiej, prokuratorowi i organowi emerytalnemu określonemu przez ministra właściwego do spraw wewnętrznych wyłącznie przez umieszczenie ich treści w portalu informacyjnym w sposób umożliwiający uzyskanie przez odbiorcę dokumentu potwierdzającego doręczenie. Ogólną normę w tym przedmiocie stanowi art. 53e § 1 u.s.p.

Doręczenie w trybie art. 131^{1a} § 1 k.p.c. jest obligatoryjne (zob. postanowienia Sądu Najwyższego, 2022, 31 stycznia 2023, wydane na tle art. $15zzs^{9}$ ustawy COVID-19), przy czym nie dotyczy to pism, które podlegają doręczeniu wraz z odpisami pism procesowych stron lub innymi dokumentami niepochodzącymi od sądu, chyba że sąd dysponuje ich kopią utrwaloną w postaci elektronicznej. Ponieważ sąd bardzo rzadko dysponuje elektroniczną kopią pisma pochodzącego od strony lub osoby trzeciej, w praktyce tą drogą są doręczane pisma pochodzące od sądu (w szczególności zarządzenia oraz orzeczenia i ich uzasadnienia). Nie jest przy tym wykluczone utworzenie takiej kopii przez sąd, zwłaszcza że dopuszczono możliwość przedstawienia akt sprawy w postaci ich kopii biegłemu sądowemu za pośrednictwem portalu informacyjnego (art. 284 § 2 k.p.c.; zob. Wolwiak, 2024, Komentarz do art. 131^{1a}, Nt 38). Za pośrednictwem portalu informacyjnego można też informować strony i ich pełnomocników o czynnościach podejmowanych w sprawie, co wynika z art. 53e § 1 zd. 2 u.s.p. Oczywiste jest przy tym, że niektóre pisma z sądu nie mogą być doręczone

za pośrednictwem portalu, np. uwierzytelniony odpis orzeczenia, odpis orzeczenia ze stwierdzeniem prawomocności czy tytuł wykonawczy.

Jeżeli nie zachodzi ustawowy wyjątek od doręczenia za pośrednictwem portalu informacyjnego, takie doręczenie jest skuteczne (Postanowienie Sądu Najwyższego, 31 stycznia 2023). Zgodzić się przy tym należy z poglądem, że obecny rozwój komunikacji elektronicznej i powszechna dostępność urządzeń telekomunikacyjnych determinuje konieczność uznania, że potwierdzone – w myśl art. 131^{1a} § 1 i 2 k.p.c. (wcześniej art. $15zzs^{9}$ ustawy COVID-19) – przez pełnomocnika strony zapoznanie się z dokumentem przesłanym przez sąd w postaci cyfrowej (elektronicznej) nie narusza norm konstytucyjnych ani międzynarodowych (Postanowienie Sądu Najwyższego, 2024).

Ponieważ system teleinformatyczny w zasadzie nie działa, w postępowaniu gospodarczym szersze zastosowanie powinien mieć przynajmniej portal informacyjny, który powinien dotyczyć nie tylko profesjonalnych pełnomocników, lecz także stron niereprezentowanych przez takich pełnomocników. Dostęp do takiego portalu nie powinien stanowić żadnego problemu dla stron postępowania gospodarczego.

2.4. Posiedzenia odmiejscowione

Można z dużą dozą prawdopodobieństwa przyjąć, że gdyby nie epidemia COVID-19, przeprowadzenie posiedzenia zdalnego – tzw. odmiejscowione posiedzenie/rozprawa (takim pojęciem posługuje się doktryna; zob. np. Gołaczyński & Zalesińska, 2020, s. 637) pozostawałoby jedynie teoretyczną możliwością. Chociaż art. 151 § 2 k.p.c., przewidujący możliwość zarządzenia przeprowadzenia posiedzenia jawnego na odległość przy użyciu urządzeń technicznych, został wprowadzony już 8 września 2016 r. (Sejm RP, 2015), to przepis ten w praktyce pozostawał martwy. Nie można jednak nie zauważyć, że w pierwotnej wersji zakładał, że jeżeli przewodniczący zarządził przeprowadzenie takiego posiedzenia, to jego uczestnicy mogli brać udział w posiedzeniu sądowym, gdy przebywali w budynku innego sądu, i tam dokonywać czynności procesowych (od 1 stycznia 2023 r. rozszerzono to na uczestników postępowania pozbawionych wolności – transmisja odbywała się z zakładu karnego lub aresztu śledczego, w którym taka osoba przebywała).

Rewolucję przyniosło jednak dopiero rozwiązanie zawarte w art. $15zzs^{1}$ ust. 1 pkt 1 ustawy COVID-19 (Gołaczyński & Dymitruk, 2021, s. 685), zgodnie z którym w okresie obowiązywania stanu zagrożenia epidemicznego albo stanu epidemii ogłoszonego z powodu COVID-19 oraz w ciągu roku od odwołania ostatniego z nich w sprawach cywilnych rozprawę lub posiedzenie jawne przeprowadzało się przy użyciu urządzeń technicznych umożliwiających przeprowadzenie ich na odległość z jednoczesnym bezpośrednim przekazem obrazu i dźwięku, z tym że osoby w nich uczestniczące nie musiały przebywać w budynku sądu. W art. 151 § 2 k.p.c. w aktualnym brzmieniu również wskazano, że w przypadku przeprowadzenia posiedzenia zdalnego na sali sądowej przebywają sąd i protokolant, a pozostałe osoby uczestniczące w posiedzeniu nie muszą przebywać w budynku sądu prowadzącego postępo-

wanie (przy czym zgodnie z § 3 zd. 3 przewodniczący może zastrzec, że określona osoba weźmie udział w posiedzeniu zdalnym poza budynkiem sądu prowadzącego postępowanie, jeżeli będzie przebywać w budynku innego sądu). Co prawda osoba biorąca udział w posiedzeniu zdalnym przebywająca poza budynkiem sądu jest zobowiązana poinformować sąd o miejscu, w którym przebywa, oraz dołożyć wszelkich starań, aby warunki w miejscu jej pobytu licowały z powagą sądu i nie stanowiły przeszkody do dokonania czynności procesowych z jej udziałem (art. 151 § 8 zd. 1 k.p.c.), jednak może przebywać w zasadzie gdziekolwiek chce. Takie rozwiązanie może zostać wykorzystane szczególnie, gdy zachodzi konieczność przesłuchania strony lub świadka przebywających w znacznej odległości od sądu (zob. Parafianowicz, 2024, s. 416), z ograniczeniem wynikającym z art. 263^1 k.p.c. Może być ono stosowane nawet, gdy sprawa jest rozpatrywana przy drzwiach zamkniętych, o ile wszyscy uczestnicy czynności przebywają w budynkach sądowych (art. 154 § 1 zd. 2 k.p.c.), co w sprawach gospodarczych ma znaczenie, chociażby z uwagi na treść art. 153 § 1^1 k.p.c., gdyż niejednokrotnie zdarza się przeprowadzenie posiedzenia lub jego części przy drzwiach zamkniętych z uwagi na możliwość ujawnienia okoliczności stanowiących tajemnicę przedsiębiorstwa strony.

W praktyce art. 151 § 2 k.p.c. daje stronom i ich pełnomocnikom dużą swobodę, co jest szczególnie cenne również w postępowaniu odwoławczym, gdy sąd nie przeprowadza uzupełniającego postępowania dowodowego. Mimo że problemy techniczne czasem powodują odraczanie rozpraw odmiejscowionych (szerzej Fruk, 2024, s. 538–539), to jednak pozytywnych aspektów spotkań zdalnych jest zdecydowanie więcej niż negatywnych. Należałoby stworzyć jednolite oprogramowanie, służące sądownictwu do prowadzenia takich posiedzeń, ale wymagałoby to, niewątpliwie, dużych nakładów finansowych i rzeczowych.

Podsumowanie

Jeżeli rozważać wzajemną relację elektronizacji procesu cywilnego i zasady jawności, to nabiera ona znaczenia tylko w aspektach związanych z przeprowadzeniem rozprawy, reszta dotyczy tak naprawdę doręczeń, wymiany pism procesowych itp. Informatyzacja w tym zakresie nie narusza w żaden sposób tej zasady. Podobnie jest w przypadku digitalizacji akt sądowych oraz możliwość wnoszenia i doręczania niemal pism, w tym wszczynających postępowanie drogą elektroniczną. Istotne jest przy tym, że postępowanie gospodarcze, które stanowi bardzo dobre pole do wprowadzania nowinek technologicznych, nie jest w ogóle wykorzystywane w tej materii. Nie sposób bowiem nie zauważyć, że ustawodawca wprowadza ogólne przepisy w omawianym zakresie dla postępowania cywilnego, które z różnych względów (finansowych, technicznych itp.) nie funkcjonują, a zasadne byłoby ich przetestowanie w jednym postępowaniu. Choć nie wszystkie sprawy prowadzone w postępowaniu go-

spodarczym dotyczą przedsiębiorców, to tzw. wykluczenie cyfrowe nie wydaje się być argumentem przemawiającym za zastosowaniem do niego ogólnych zasad, a więc stosowanych w przypadku każdej innej sprawy cywilnej. *De lege ferenda* należy postulować, aby w postępowanich gospodarczych został wprowadzony obowiązek dokonywania wszelkich doręczeń (z sądu i do sądu) elektronicznie, nawet mailowo, a przynajmniej przez portal informacyjny, bez względu na to, czy strony są reprezentowane przez profesjonalnych pełnomocników. Nie byłaby wówczas potrzebna nawet digitalizacja. Nie sposób uznać, aby w aktualnym stanie cyfryzacji naruszało to prawo do sądu. Rozwiązania, które wprowadzono lub się rozwinęły podczas epidemii COVID-19, takie jak posiedzenie zdalne bez konieczności bytności w innym sądzie czy portal informacyjny, dotyczą wszystkich postępowań cywilnych i mają ograniczony zasięg podmiotowy.

Jeżeli chodzi o postępowanie odwoławcze, zasadą powinno być posiedzenie niejawne, nawet jeżeli w pierwszej instancji wydano wyrok na posiedzeniu niejawnym. Rozprawa powinna mieć miejsce tylko wówczas, gdyby zaszła potrzeba przeprowadzenia postępowania dowodowego z osobowych źródeł lub ze względu na charakter sprawy sąd uznałby konieczność przeprowadzenia rozprawy. Powinny zatem zostać zmodyfikowane art. 374 i 375 k.p.c. Sędzia powinien być przygotowany i w takiej sytuacji rozprawa niczego nie wnosi, gdyż strony przedstawiły swoje stanowiska w pismach procesowych. W wielu sprawach (w tym również gospodarczych) całkowicie wystarczające są stanowiska stron wyrażone na piśmie. Wówczas wszystkie czynności sąd mógłby wykonać drogą elektroniczną.

BIBLIOGRAFIA

Cygan, R. (2025). Sądownictwo w dobie nowoczesnych technologii, *Palestra*, *1*, 241–254.

Ereciński, T. & Weitz, K. (2010). Prawda i równość stron w postępowaniu cywilnym a orzecznictwo Trybunału Konstytucyjnego. w: T. Ereciński & K. Weitz (red.), *Orzecznictwo Trybunału Konstytucyjnego a Kodeks postępowania cywilnego. Materiały Ogólnopolskiego Zjazdu Katedr i Zakładów Postępowania Cywilnego*. 17–62. Wolters Kluwer Polska.

Feliga P., (2024). Komentarz do art. 458[3]. w: P. Rylski (red. nacz.) & A. Olaś (red. cz. III), *Kodeks postępowania cywilnego. Komentarz*. Legalis.

Fruk, A. (2024). E-rozprawa w postępowaniu cywilnym – standaryzacja czy destabilizacja? Dekalog zmian art. 151 KPC wprowadzonych nowelizacją z 2024 r., *Monitor Prawniczy*, *9*, s. 529–543.

Gołaczyński, J. & Dymitruk, M. (2021). Rozprawa zdalna i doręczenia elektroniczne w dobie pandemii COVID-19 po wejściu w życie nowelizacji z 28.5.2021 r., *Monitor Prawniczy*, *13*, 685–697.

Gołaczyński, J. & Zalesińska, A. (2020). Nowe technologie w sądach na przykładzie wideokonferencji i składania pism procesowych i doręczeń elektronicznych w dobie pandemii COVID-19, *Monitor Prawniczy*, *12*, 637–643.

Gołąb, A. (2020). Wybrane aspekty zasady jawności w świetle nowelizacji Kodeksu postępowania cywilnego z 4.7.2019 r. w: P. Rylski (red.), *Reforma czy kolejna nowelizacja? Uwagi na tle ustawy z 4.7.2019 r. zmieniającej k.p.c.* 95–129. Wydawnictwo C.H.Beck.

Gołąb, A. (2024). Komentarz do art. 9. w: P. Rylski (red. nacz.) & A. Olaś (red. cz. III), *Kodeks postępowania cywilnego. Komentarz*. Legalis.

Góra-Błaszczykowska, A. (2008). *Zasada równości stron w procesie*. Wydawnictwo C.H.Beck.

Grzegorczyk, P. & Weitz, K. (2016). Komentarz do art. 45. w: M. Safjan & L. Bosek (red.), *Konstytucja RP. Komentarz*. Tom I. Art. 1–86, 1086–1152. Wydawnictwo C.H. Beck.

Hofmański, P., & Wróbel, A. (2010). Komentarz do art. 6. w: L. Garlicki (red.), *Konwencja o ochronie praw człowieka i podstawowych wolności*. Tom I. Komentarz do art. 1–18, 246–461. Wydawnictwo C.H. Beck.

Łazarska, A. (2012). *Rzetelny proces cywilny*. Wolters Kluwer Polska.

Mayer, F. C. (2022). Art. 6 EMRK. w: U. Karpenstein, F. C. Mayer (red.), *Konvention zum Schutz der Menschenrechte und Grundfreiheiten*: EMRK, 171–302. C.H. Beck.

Minister Cyfryzacji. (2023). Komunikat z dnia 29 maja 2023 r. w sprawie określenia terminu wdrożenia rozwiązań technicznych niezbędnych do doręczania korespondencji z wykorzystaniem publicznej usługi rejestrowanego doręczenia elektronicznego lub publicznej usługi hybrydowej oraz udostępnienia w systemie teleinformatycznym punktu dostępu do usług rejestrowanego doręczenia elektronicznego w ruchu transgranicznym (Dz.U. 2023, poz. 1077, ze zm.).

Minister Sprawiedliwości. (2015). Rozporządzenie z dnia 20 października 2015 r. w sprawie sposobu wnoszenia pism procesowych za pośrednictwem systemu teleinformatycznego obsługującego postępowanie sądowe (t.j. z 2023, poz. 540).

Minister Sprawiedliwości. (2021). Rozporządzenie z dnia z 30 listopada 2021 r. w sprawie konta w systemie teleinformatycznym obsługującym postępowanie sądowe (Dz.U. 2021, poz. 2204, ze zm.).

Parafianowicz, J. (2024). Komentarz do art. 151. w: O. M. Piaskowska (red.), *Kodeks postępowania cywilnego. Komentarz*. Tom I. Art. 1–505[39], 415–417. Wolters Kluwer Polska.

Postanowienie Sądu Apelacyjnego w Katowicach z dnia 27 lutego 2017 r., sygn. akt V ACz 171/17, OSA/Kat. 2017, nr 1, poz. 3.

Postanowienie Sądu Najwyższego z dnia 11 kwietnia 2024 r., sygn. akt II UZ 3/24.

Postanowienie Sądu Najwyższego z dnia 12 stycznia 2022 r., III CZ 37/22.

Postanowienie Sądu Najwyższego z dnia 25 listopada 1997 r., sygn. akt I CZ 142/97.

Postanowienie Sądu Najwyższego z dnia 29 marca 2023 r., sygn. akt III CZ 427/22, OSNC 2023, nr 9, poz. 93.

Postanowienie Sądu Najwyższego z dnia 31 stycznia 2023 r., III CZP 369/23.

Rada Europy. (1950). Konwencja o ochronie praw człowieka i podstawowych wolności, sporządzona w Rzymie w dniu 4 listopada 1950 r. (Dz.U. 1993, nr 61, poz. 284, ze zm.).

Rylski, P., Zembrzuski, T. (2006). Rozpoznanie spraw cywilnych na posiedzeniu niejawnym. *Przegląd Sądowy*, *6*, 83–106.

Sejm Rzeczypospolitej Polskiej. (2001). Ustawa z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych (t.j. z 2024, poz. 334, ze zm.).

Sejm Rzeczypospolitej Polskiej. (2005). Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. z 2024, poz. 1557, ze zm.).

Sejm Rzeczypospolitej Polskiej. (2015). Ustawa z dnia 10 lipca 2015 r. o zmianie ustawy – Kodeks cywilny, ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw (Dz.U. 2015, poz. 1311, ze zm.).

Sejm Rzeczypospolitej Polskiej. (2019). Ustawa z dnia 4 lipca 2019 r. o zmianie ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw (Dz.U. 2019, poz. 1469, ze zm.).

Sejm Rzeczypospolitej Polskiej. (2020a). Ustawa z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (t.j. z 2024, poz. 1045, ze zm.).

Sejm Rzeczypospolitej Polskiej. (2020b). Ustawa z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (t.j. z 2024, poz. 340, ze zm.).

Sejm Rzeczypospolitej Polskiej. (2021). Ustawa z dnia 28 maja 2021 r. o zmianie ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw (Dz.U. 2021, poz. 1090).

Sejm Rzeczypospolitej Polskiej. (2023a). Ustawa z dnia 7 lipca 2023 r. o zmianie ustawy – Kodeks postępowania cywilnego, ustawy – Prawo o ustroju sądów powszechnych, ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw (Dz.U. 2023, poz. 1860, ze zm.).

Sejm Rzeczypospolitej Polskiej. (2023b). Ustawa z dnia 9 marca 2023 r. o zmianie ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw (Dz.U. 2023, poz. 614).

Sejm Rzeczypospolitej Polskiej. (2024). Ustawa z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej (Dz.U. 2024, poz. 1221, ze zm.).

Szanciło, T. (2023). Komentarz do art. 458^{2}. w: T. Szanciło (red.), *Kodeks postępowania cywilnego. Komentarz*. Tom I. Art. $1–458^{16}$, 1956–1969. Wydawnictwo C.H. Beck.

Szanciło, T. (2024). Artificial intelligence and case categories in civil proceeding. *Studia Iuridica*, *103*, 7–22.

Szczurowski, T. (2019). Specyfika nowego postępowania odrębnego w sprawach gospodarczych. *Przegląd Ustawodawstwa Gospodarczego*, *11*, 41–47.

Wolwiak, I. (2024). Komentarz do art. 131^{1a}. w: P. Rylski (red. nacz.) & A. Olaś (red. cz. III), *Kodeks postępowania cywilnego. Komentarz*. Legalis.

Wyrok Europejskiego Trybunału Praw Człowieka z dnia 1 marca 2006 r. w sprawie *Sejdovic v. Włochy*, nr wniosku 56581/00.

Wyrok Europejskiego Trybunału Praw Człowieka z dnia 14 listopada 2000 r. w sprawie *Riepan v. Austria*, nr wniosku 35115/97.

Wyrok Europejskiego Trybunału Praw Człowieka z dnia 19 lutego 1998 r. w sprawie *Jacobsson v. Szwecja*, nr wniosku 16970/90.

Wyrok Europejskiego Trybunału Praw Człowieka z dnia 20 listopada 2003 r. w sprawie *Faugel v. Austria*, nr wniosków 58647/00 i 58649/00.

Wyrok Europejskiego Trybunału Praw Człowieka z dnia 22 maja 1990 r. w sprawie *Weber v. Szwajcaria*, nr wniosku 11034/84.

Wyrok Europejskiego Trybunału Praw Człowieka z dnia 23 lutego 1994 r. w sprawie *Fredin v. Szwecja*, nr wniosku 18928/91.

Wyrok Europejskiego Trybunału Praw Człowieka z dnia 24 czerwca 1993 r. w sprawie *Schuler-Zgraggen v. Szwajcaria*, nr wniosku 14518/89.

Wyrok Europejskiego Trybunału Praw Człowieka z dnia 28 maja 1997 r. w sprawie *Pauger v. Austria*, nr wniosku 16717/90.

Wyrok Europejskiego Trybunału Praw Człowieka z dnia z 8 lutego 2005 r. w sprawie *Miller v. Szwecja*, nr wniosku 55853/00.

Wyrok Trybunału Konstytucyjnego z dnia 11 czerwca 2002 r., sygn. akt SK 5/02, OTK-A 2002, nr 4, poz. 41.

Wyrok Trybunału Konstytucyjnego z dnia 16 listopada 2011 r., SK 45/09, OTK-A 2011, nr 9, poz. 97.

Wyrok Trybunału Konstytucyjnego z dnia 19 września 2007 r., sygn. akt SK 4/06, OTK-A 2007, nr 8, poz. 98.

Wyrok Trybunału Konstytucyjnego z dnia 3 lipca 2007 r., sygn. akt SK 1/06, OTK-A 2007, nr 7, poz. 73.

Wyrok Trybunału Konstytucyjnego z dnia z 2 października 2006 r., sygn. akt SK 34/06, OTK-A 2006, nr 9, poz. 118.

Wyrok Trybunału Konstytucyjnego z dnia z 20 listopada 2007 r., sygn. akt SK 57/05, OTK-A 2007, nr 10, poz. 125.

Wyrok Trybunału Konstytucyjnego z dnia z 20 października 2010 r., sygn. akt P 37/09, OTK-A 2010, nr 8, poz. 79.

List of the Reviewers in 2025

Adrych-Brzezińska Izabela, University of Gdansk, Poland

Alfano Roberta, University of Naples, Italy

Bagan-Kurluta Katarzyna, University of Białystok, Poland

Barczak-Oplustil Agnieszka, Jagiellonian University in Cracow, Poland

Bączyk-Rozwadowska Kinga, Nicolaus Copernicus University in Torun, Poland

Bernaczyk Michał, University of Wroclaw, Poland

Bień-Kacała Agnieszka, University of Szczecin, Poland

Bieranowski Adam, Warmia and Mazury University, Poland

Bilewska Katarzyna, University of Warsaw, Poland

Bożek Wojciech, University of Szczecin, Poland

Bugajski Błażej, Cracow University of Economics, Poland

Cani Eralda, University of Tirana, Albania

Czaplicki Paweł, University of Bialystok, Poland

Daniluk Paweł, Polish Academy of Sciences, Poland

de Angelis Monica, Marche Polytechnic University, Italy

Demendecki Tomasz, Maria Curie-Skłodowska University Lublin, Poland

Doliwa Adam, University of Białystok, Poland

Drozdowska Urszula, University of Białystok, Poland

Filipkowski Wojciech, University of Bialystok, Poland

Flaga-Gieruszynska Kinga, University of Szczecin, Poland

Florczak-Wątor Monika, Jagiellonian University in Cracow, Poland

Gąsior Tomasz, Kujawy and Pomorze University in Bydgoszcz, Poland

Górski Adam, Medical University of Bialystok, Jagiellonian University in Cracow, Poland

Grądalski Tomasz, Andrzej Frycz Modrzewski University in Krakow, Poland

Grochowski Mateusz, Tulane University School of Law, USA

Grzelak Agnieszka, Kozminski University, Poland

Habdas Magdalena, University of Silesia in Katowice, Poland

Haberko Joanna, Adam Mickiewicz University in Poznan, Poland

Haczkowska Monika, Opole University of Technology, Poland

Jabłonski Mariusz, University of Wroclaw, Poland

Jacuński Michał, University of Wroclaw, Poland

Jagielska Monika, University of Silesia in Katowice, Poland

Janovec Michal, Masaryk University, Czechia

Jóźwicki Władysław, Adam Mickiewicz University in Poznan, Poland

Kanarek-Równicka Anna, Uniwersytet Jana Kochanowskiego w Kielcach, Poland

Kancik-Kołtun Ewelina, Maria Curie-Skłodowska University Lublin, Poland

Kapsa Izabela, Kazimierz Wielki University in Bydgoszcz, Poland

Karczewska-Kamińska Natalia, Nicolaus Copernicus University in Torun, Poland

Kawałko Agnieszka, John Paul II Catholic University of Lublin, Poland

Kmieciak Błażej, Medical University of Lodz, Poland

Knapp Magdalena, University of Warsaw, Poland

Kosinska Anna, University of Szczecin, Poland

Kossoń Dariusz, Medical University of Warsaw, Poland

Kowalewska Ewa, University of Szczecin, Poland

Kubiak Rafał, University of Lodz, Medical University of Lodz, Poland

Kucia Bartosz, University of Silesia in Katowice, Poland

Kuczma Paweł, University of Zielona Gora, Poland

Kuklo Marta, University of Białystok, Poland

Kuźnicka-Błaszkowska Dominika, University of Wroclaw, Poland

Lach Arkadiusz, Nicolaus Copernicus University in Torun, Poland

Lach Daniel, Adam Mickiewicz University in Poznan, Poland

Latos-Miłkowska Monika, Kozminski University, Poland

Lupano Matteo, University of Turin, Itlay

Łakomiec Katarzyna, Polish Academy of Sciences, Poland

Łukasiewicz Jakub, University of Rzeszow, Poland

Łukasiewicz Rafał, University of Rzeszow, Poland

Maceratini Arianna, University of Macerata, Italy

Malarewicz-Jakubów Agnieszka, University of Białystok, Poland

Małozięć Cezary, SWPS University, Poland

Mamak Kamil, Jagiellonian University in Cracow, Poland

Mariański Michał, Warmia and Mazury University, Poland

Marzęda-Młynarska Katarzyna, Maria Curie-Skłodowska University Lublin, Poland

Masłowski Michał, Warsaw University of Technology, Poland

Mędrzycki Radosław, Cardinal Stefan Wyszyński University, Poland

Miaskowska-Daszkiewicz Katarzyna, John Paul II Catholic University of Lublin, Poland

Michalski Marek, Cardinal Stefan Wyszyński University, Poland

Michałowska Kinga, Cracow University of Economics, Poland

Milczarek Ewa, University of Szczecin, Poland

Milinkovic Igor, Uniwersytet Banjaluka, Bosnia and Herzegovina

Moszyńska Anna, Nicolaus Copernicus University in Torun, Poland

Mucha Ariel, Jagiellonian University in Cracow, Poland

Oplustil Krzysztof, Jagiellonian University in Cracow, Poland

Ożóg Michał, University of Bialystok, Poland

Pacian Joanna, Medical University of Lublin , Poland

Parente Salvatore Antonello, University of Bari, Italy

Passaglia Paolo, University of Pisa, Italy

Pązik Adam, Cracow University of Economics, Poland

Piech Krzysztof, Warsaw School of Economics, Poland

Piszcz Anna, University of Białystok, Poland

Pogorelcnik Neza, University of Ljublana, Slovenia

Południak-Gierz Katarzyna, Jagiellonian University in Cracow, Poland

Puchta Radosław, University of Bialystok, Poland

Rzewuska Magdalena, Warmia and Mazury University, Poland

Rzewuski Maciej, Warmia and Mazury University, Poland

Sakowska-Baryła Marlena, University of Lodz, Poland

Schweigl Johan, Masaryk University, Czechia

Selicato Gianluca, University of Bari, Italy

Sienczyło-Chlabicz Joanna, University of Bialystok, Poland

Skóra Agnieszka, Warmia and Mazury University, Poland

Skórzewska-Amberg Małgorzata, Kozminski University, Poland

Skuza Sebastian, University of Warsaw, Poland

Sobiecki Grzegorz, Warsaw School of Economics, Poland

Sroka Tomasz, Jagiellonian University in Cracow, Poland

Stawarska-Rippel Anna, University of Silesia in Katowice, Poland

Stec Piotr, University of Opole, Poland

Stępień-Załucka Beata, University of Rzeszow, Poland

Suwaj Patrycja, Jacob of Paradies University, Poland

Sylwestrzak Anna, University of Gdansk, Poland

Szanciło Tomasz, European School of Law and Administration, Poland

Szaraniec Monika, Cracow University of Economics, Poland

Szczerbowski Jakub, University of Lodz, Poland

Ślęzak Emil, Warsaw School of Economics, Poland

Świderska Małgorzata, University of Business and Administration in Gdynia, Poland

Świerczyński Marek, Cardinal Stefan Wyszyński University, Poland

Świrgon-Skok Renata, University of Rzeszow, Poland

Tomaszuk Mariusz, Warsaw University of Technology, Poland

Tomczak Łukasz, University of Szczecin, Poland

Urbaniak Monika, Poznan University of Medical Sciences, Poland

van der Hoeven Just, University of Amsterdam, Netherlands

Verdoodt Valerie, University of Ghent, Belgium

Villaplana Jiménez Francisco Ramón, University of Valencia, Spain

Walczuk Konrad, War Studies University, Poland

Waszkiewicz Paweł, University of Warsaw, Poland

Weber Anne-Marie, University of Warsaw, Poland

Witoszko Wioletta, University of Bialystok, Poland

Wnukiewicz-Kozłowska Agata, University of Wroclaw, Poland

Wojciechowski Bartosz, University of Lodz, Poland

Wowerka Arkadiusz, University of Gdansk, Poland

Woźniak Rafał, Kozminski University, Poland

Wrzecionek Rafał, University of Zielona Gora, Poland

Wyżykowski Bartosz, University of Warsaw, Poland

Zabłocki Jan, Cardinal Stefan Wyszyński University, Poland

Zacharzewski Konrad, Kozminski University, Poland

Zajączkowska Renata, University of Rzeszow, Poland

Zalcewicz Anna, Warsaw University of Technology, Poland

Załucki Mariusz, Andrzej Frycz Modrzewski University in Krakow, Poland

Zawadzka Patrycja, University of Wroclaw, Poland

Zięty Jakub, Warmia and Mazury University, Poland