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