Ius Novum
2026, vol. 20, no. 3, pp. 82–104

PROTECTION OF PERSONAL DATA IN THE INFORMATION SOCIETY: SELECTED ISSUES

PRZEMYSŁAW SZUSTAKIEWICZ*
MACIEJ KOBAK**

DOI 10.2478/in-2026-0030

Abstract
The article discusses key issues related to the processing of personal data in an era of dynamic technological development. The authors point out that modern societies, characterised by the circulation of information and new media, face a growing threat of surveillance, both by states and by global private entities. The fundamental human right to privacy therefore requires special protection in circumstances in which personal data have become an economic resource of considerable importance. The aim of the article is to identify and analyse the most significant threats to personal data protection in the information society and to assess the adequacy of the existing legal framework. The study applies the dogmatic legal method, involving an analysis of legal acts, case law and legal scholarship, supplemented by elements of the comparative method. The article discusses four main challenges. The first is artificial intelligence, whose development offers innovative potential but also entails the risk of a loss of individual autonomy. The European Union was the first jurisdiction in the world to introduce the AI Act, which lays down rules governing the use of AI systems and their compliance with the GDPR. The second issue is profiling and scoring, namely automated decision-making, often used in finance or insurance, which raises concerns about discrimination and a lack of human oversight. The third challenge is social media, through which users voluntarily share large amounts of data, often unknowingly disclosing sensitive information. The final issue concerns monitoring and the use of biometric devices, which require strict compliance with

* Professor LLD hab., Lazarski University in Warsaw (Poland), Supreme Administrative Court's judge, e-mail: przemyslaw.szustakiewicz@lazarski.edu.pl, ORCID: 0000-0001-9102-9308
** LLD, WSPiA University of Rzeszów (Poland), Voivodeship Administrative Court's judge, e-mail: Maciej.Kobak@wspia.eu, ORCID: 0000-0002-4481-9240

This is an open access article licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) (https://creativecommons.org/licenses/by-nc-sa/4.0/).

the principles of consent, data minimisation and purpose limitation. The analysis leads to the conclusion that effective personal data protection in the information society requires legal regulations, such as the GDPR and the AI Act, to be combined with their effective enforcement in order to maintain a balance between technological development and individual rights.

Keywords: information society, personal data processing, artificial intelligence, GDPR, AI Act

METHODOLOGICAL ASSUMPTIONS

The research question addressed in this article focuses on whether the current legal framework for personal data protection, in particular the GDPR and Regulation (EU) 2024/1689 of the European Parliament and of the Council on artificial intelligence (Artificial Intelligence Act), provides adequate protection for individual rights in the context of the dynamic development of the information society. The primary aim of this study is to identify the most significant threats to the privacy and informational autonomy of natural persons and to assess whether the available legal instruments allow the risks associated with the use of new technologies to be effectively mitigated.

The article primarily employs the dogmatic legal method, comprising an analysis of EU and national law, as well as the case law of the Court of Justice of the European Union and administrative courts. Elements of the comparative method are also used to compare various models of data processing and the corresponding standards of protection. A supplementary analysis of the relevant literature made it possible to situate the discussion within the current state of research and to organise the issues indicated in the title around four areas: artificial intelligence, profiling and scoring, social media, and monitoring and biometric devices.

INFORMATION SOCIETY AND PERSONAL DATA

Contemporary societies in highly developed countries are already 'information societies', i.e. societies whose functioning necessarily entails the collection and circulation of information through highly complex information technologies and devices operating on the basis of those technologies. This type of society should be understood broadly, as it encompasses all people living within the sphere of influence of new media, albeit with varying degrees of intensity and involvement: from computer programmers, through internet users spending many hours in front of a computer monitor, to pensioners who, although they have no computer skills whatsoever, are nevertheless indirectly dependent on computers, for example for the calculation of their pensions by specialised programs used by the relevant institutions.[1]

[1] M. Golka, 'Czym jest społeczeństwo informacyjne', *Ruch Prawniczy, Ekonomiczny i Socjologiczny*, 2005, No. 4, p. 257.

The information society therefore represents a certain stage of social development in which, on the one hand, a system for collecting information and communicating by means of technical devices is an essential element of its organisation, while, on the other hand, remaining outside this system, even where one does not personally use devices operating on the basis of information technologies, is practically impossible. Although the exchange of information has always formed the foundation of human civilisation,[2] since the beginning of the twenty-first century it has effectively become a dominant element of modern societies and the states they have created.

However, it should be pointed out that the progressive integration ('smartification') of technologies suitable for use in surveillance activities and their expansion into ever new spheres of individual and social life are increasingly condemning innocent citizens to a lifelong sentence of electronic surveillance.[3] Hence, the issue of personal data protection is developing in parallel with information technologies. Initially, it was primarily associated with protecting individuals against excessive interference by the state in their privacy, whereas it now increasingly concerns protecting individuals against the excessive collection of information about them by non-state entities, which are often established in countries other than that of the user and conduct business on a global scale. It should be added that the development of new technologies and the new devices operating on their basis is not finite in nature; it is dynamic and, it would appear, unstoppable. This situation raises the question of whether contemporary law and legal protection authorities remain capable of effectively protecting individuals against systems of surveillance operated not only by the state but also, and on a very large scale, by private companies. In this regard, the EU legislature stated in recitals 6 and 7 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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),[4] that:

> 'Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data.' (recital 6),

---

[2] Cf. Y.N. Harari, *Sapiens: od zwierząt do bogów*, trans. Hunia J., Kraków, 2011; the author thoroughly describes the influence of information exchange, including gossip, on the development of culture and, consequently, of society and its structures, as well as on the creation of contemporary civilisation.

[3] K. Michalski, 'Konflikty interesów związane z bezpieczeństwem danych osobowych i ochroną prywatności w społeczeństwie cyfrowym', *Zeszyty Naukowe WSIZiA w Warszawie*, 2017, Vol. 15, No. 3(40), p. 55.

[4] OJ L 119, 4.5.2016, ELI: http://data.europa.eu/eli/reg/2016/679/oj (hereinafter referred to as the 'GDPR').

and that:

> 'Those developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market. Natural persons should have control of their own personal data. Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced' (recital 7).

It was therefore recognised that the GDPR should serve as an instrument that, in an information society in which data relating to natural persons have become an important element of the economy, continues to protect and effectively enforce the human right to the protection of personal data. The dynamic development of information technologies and the emergence of the information society in no way undermine one of the fundamental human rights: the right to privacy, of which the aforementioned protection of personal data is an important component.[5]

Nonetheless, the development of information technologies poses challenges to personal data protection that those involved in this field will face or are already facing. It appears that four issues can currently be identified as posing challenges to personal data protection in connection with the development of new technologies.

LEGAL FRAMEWORK FOR THE FUNCTIONING OF ARTIFICIAL INTELLIGENCE (AI)

The first of these is the use of artificial intelligence in the processing of personal data. In everyday language, 'artificial intelligence' means the ability of advanced information systems to perform certain tasks that require humans to use intelligence, such as learning and recognising shapes or sounds.[6] Artificial intelligence[7] is therefore a type of information technology which, through the use of electronic devices, begins to function like a human being.[8] This technology may be divided into 'weak AI', that is, intelligent decision support systems (IDSS), and 'strong AI'. Both operate autonomously, but strong AI is characterised by self-awareness.[9] Once data have been entered into it, artificial intelligence operates independently of human intervention, autonomously carrying out reasoning processes. At present, successive versions of various AI systems are being used increasingly frequently by both public and private users. In addition, it is clear that, in the information society, AI is a factor transforming both economic and social relations. It may therefore play a role in the

---

[5] For more on this issue, see R. Gellert, 'Understanding the Notion of Risk in the General Data Protection Regulation', *Computer Law & Security Review*, 2018, Vol. 34, No. 2, pp. 279–288.

[6] S. Dubisz (ed.), *Wielki słownik języka polskiego PWN. Tom H–N*, Warszawa, 2018, p. 128.

[7] Hereinafter referred to as 'AI'.

[8] S.J. Russell, P. Norvig, *Artificial Intelligence: A Modern Approach*, 4th edn, Harlow, 2021, passim, provide a comprehensive discussion of the elements comprising the definition of AI.

[9] P. Kłos, 'Inteligentne systemy wspomagania decyzji w procesie podejmowania decyzji prawnych – wybrane zagadnienia z perspektywy teoretycznoprawnej', *Ruch Prawniczy, Ekonomiczny i Socjologiczny*, 2025, Vol. 87, No. 2, p. 41.

economic and social development of the information society comparable to that played by the invention of the steam engine in the development of industrial society in the nineteenth and twentieth centuries. However, in this respect, unregulated AI represents not only an opportunity for further social and economic development but also a challenge and even a threat, because:

> 'Anyone who feels constantly monitored and, at the same time, feels unable to escape intrusions into and interference with their personal life reacts with alienation, is impaired in the development of their personality and is unable to exercise the full range of civil rights and freedoms guaranteed by the constitution, including freedom of belief and association. In this sense, the loss of informational self-determination destroys the basic capacity for social communication and participation in community life. The ideas and talents of such people do not benefit the community and, from the community's perspective, they are lost.'[10]

Uncontrolled AI may therefore lead to individuals losing their autonomy, while a sense of ubiquitous surveillance may deprive them of their freedom. For this reason, the EU legislature was the first in the world to decide to regulate the operation of AI systems by means of a legal act, namely Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).[11] Regulation (EU) 2024/1689 entered into force on 1 August 2024, while the application of its specific provisions was distributed over time. This roadmap was amended by Regulation (EU) 2026/1744 of the European Parliament and of the Council of 8 July 2026 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards the simplification of the implementation of harmonised rules on artificial intelligence,[12] which has applied since 27 July 2026. Following that amendment, the provisions of Chapter III, Sections 1–3, concerning high-risk AI systems apply from 2 December 2027 as regards AI systems classified pursuant to Article 6(2) and Annex III, and from 2 August 2028 as regards AI systems classified pursuant to Article 6(1) and Annex I.

Article 3(1) of the AI Act defines an AI system as

> 'a machine-based system that is 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 legal definition of an AI system therefore identifies two of its fundamental characteristics: learning, which distinguishes it from other electronic collections of

---

10 K. Michalski, 'Konflikty interesów…', op. cit., p. 61.

11 OJ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj (hereinafter referred to as the 'AI Act').

12 OJ L, 2026/1744, 24.7.2026, ELI: http://data.europa.eu/eli/reg/2026/1744/oj.

data and entails the continuous capacity for self-improvement,[13] and the ability to infer, that is, to analyse data and independently synthesise them.

Recital 27 states that the AI Act is designed to ensure implementation of the seven principles set out in the 2019 *Ethics Guidelines for Trustworthy AI*,[14] i.e. (1) human agency and oversight; (2) technical robustness and safety; (3) privacy and data governance; (4) transparency; (5) diversity, non-discrimination and fairness; (6) societal and environmental well-being; and (7) accountability.

With regard to the first principle, it is pointed out that 'The AI Act regulates the use of artificial intelligence through the prism of the human being. This is because all potential consequences of unintended actions by artificial intelligence affect human beings.'[15] The AI Act is human-centric in the sense that its objective, as emphasised in Article 1(1), is to promote the uptake of human-centric and trustworthy AI, that is, AI that respects human dignity and treats the human being not as a 'product' or 'consumer', but as a free individual. Therefore, in order to prevent manipulation by AI, whether carried out by AI itself or by the entities developing it, the Regulation introduces four categories of AI according to the risk of infringement of the humanistic values that form the axiological foundation of the Community. These are:

1. Prohibited systems, including:
   - systems deploying subliminal techniques;
   - systems exploiting any of the vulnerabilities of a natural person or a specific group of persons due to their age, disability or specific social or economic situation, with the objective or effect of materially distorting the behaviour of that person or a person belonging to that group in a manner that causes or is reasonably likely to cause significant harm to that person or another person;
   - systems for scoring citizens based on their behaviour in a different social context or their personal or personality characteristics;
   - systems for profiling a natural person or assessing their personality traits and characteristics to assess the likelihood that they will commit a criminal offence;
   - systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage;
   - AI systems used to monitor natural persons in the workplace or educational institutions by inferring their emotions;
   - biometric categorisation systems that individually categorise natural persons on the basis of their biometric data in order to deduce or infer information

---

[13] Cf. J. Rzymowski, 'Definicja prawnicza sztucznej inteligencji na podstawie rozporządzenia PE i Rady (UE) 2024/1689 w sprawie sztucznej inteligencji', *Przegląd Prawa Publicznego*, 2024, No. 11, pp. 56–63.

[14] High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, Brussels, 2019; https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2019/11-06/Ethics-guidelines-AI_EN.pdf (accessed: 21 July 2026).

[15] K. Palacz, 'Jak inteligentne jest prawo regulujące sztuczną inteligencję? Próba analizy AI Act na podstawie jej ugruntowania w przestrzeni komercyjnego użycia', *Prawo Mediów Elektronicznych*, 2022, No. 1, p. 24.

concerning their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation; this prohibition does not cover the labelling or filtering of lawfully acquired biometric datasets, such as images, on the basis of biometric data, or the categorisation of biometric data in the area of law enforcement.

2. High-risk systems, that is, systems which, under the Regulation, must comply with the requirements laid down therein, particularly those relating to risk management, data use and governance, record-keeping, provision of information to deployers, human oversight, and accuracy, robustness and cybersecurity. Importantly, in addition to imposing the aforementioned requirements on the systems themselves, the Regulation provides for specific obligations to be imposed on their providers, importers, distributors and deployers. A system for the conformity assessment and certification of such systems will be established, together with an EU database containing information on those systems and their operators.[16] This category

> 'entails AI systems used in key areas of human existence, *inter alia*: critical infrastructure (including critical digital infrastructure, road traffic and the supply of utilities), education and vocational training (including systems determining access or admission to educational institutions and assessing learning outcomes), employment and worker management (including the screening of job applicants' CVs and decisions concerning promotion or termination of employment), access to essential private and public services (including assessing eligibility for public healthcare, assessing creditworthiness and determining premiums for health and life insurance), law enforcement, migration, asylum and border control management, the administration of justice and democratic processes (for example, assisting a court in examining the facts and applying the law to those facts, or the vaguely described "AI systems intended to be used to influence the outcome of elections (…) or the voting behaviour of natural persons"). AI systems identified on this basis are subject to registration in an EU database'.[17]

   Systems of this type should be subject to continuous human oversight.
3. Limited-risk systems, also referred to as general-purpose systems, which, under Article 3(63) of the AI Act, means an AI model, including an AI model trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks, regardless of the manner in which the model is placed on the market, and that can be integrated into a variety of downstream systems or applications, with the exception of AI models used for research, development or prototyping activities before they are placed on the market.
4. Systems that do not generate risk, that is, systems which, although they are AI systems, the EU legislator has decided should not be subject to the provisions of the AI Act because of the low risk of infringement of the EU's axiological foundations.

---

[16] P. Burczaniuk, 'Tworzenie prawa sztucznej inteligencji – wyzwania i perspektywy', *Prawo i Więź*, 2024, Vol. 51, No. 3, p. 298.

[17] D. Flisak, *Akt w sprawie sztucznej inteligencji*, LEX/el., 2024.

It is clear that AI systems used by and directed at human beings must process personal data. Otherwise, their usefulness to users would be severely limited. The interaction between the AI Act and the GDPR is crucial for implementing ethical principles of trustworthy AI, such as privacy and data governance, transparency, diversity, non-discrimination and fairness, societal and environmental well-being, and accountability. In this regard, Article 2(7) of the AI Act is of fundamental importance, as, without prejudice to Article 4a and Article 59, the Regulation does not affect the GDPR, Regulation (EU) 2018/1725 or Directives 2002/58/EC and (EU) 2016/680. This means, as emphasised in recital 10 of the AI Act, that the Act does not affect the provisions of the GDPR, including the powers of national supervisory authorities, such as the President of the Personal Data Protection Office. Furthermore, insofar as the design, development or use of AI systems involves the processing of personal data, AI developers and entities using such systems are subject to the obligations imposed on controllers, while data subjects retain all the rights and safeguards granted to them under Union law, including rights relating to solely automated decision-making in individual cases, including profiling. The AI Act is an instrument through which the solutions adopted therein concerning the placing on the market, putting into service and use of AI systems should facilitate effective implementation and enable data subjects to exercise the rights conferred on them by the GDPR. Moreover, as emphasised in recital 69 of the AI Act:

> 'The right to privacy and to the protection of personal data must be guaranteed throughout the entire lifecycle of the AI system. In this regard, the principles of data minimisation and data protection by design and by default, as set out in Union data protection law, are applicable when personal data are processed. Measures taken by providers to ensure compliance with those principles may include not only anonymisation and encryption, but also the use of technology that permits algorithms to be brought to the data and allows AI systems to be trained without the transmission between parties or copying of the raw or structured data themselves, without prejudice to the requirements on data governance provided for in this Regulation.'

Against this background, account must be taken of Article 4a of the AI Act, added by Regulation (EU) 2026/1744. By way of exception and to the extent strictly necessary, that provision permits the processing of special categories of personal data for the purposes of bias detection and correction in AI systems or models. The permissibility of such processing is conditional, in particular, on the fact that bias detection and correction cannot be effectively fulfilled by processing other data, including synthetic or anonymised data; on the application of limitations on the re-use of personal data and security and privacy-preserving measures, including pseudonymisation; on strict controls and documentation of access; on the prohibition of transferring data to other parties; on the deletion of the data once the bias has been corrected or the data have reached the end of their retention period; and on documenting the reasons why the processing is strictly necessary. In addition to providers of high-risk AI systems, this possibility applies to providers and deployers of other AI systems and models and to deployers of high-risk AI systems only where possible biases are likely to affect the health and safety of persons, have a negative impact on fundamental rights or lead to discrimination prohibited

pursuant to Union law. These conditions apply in addition to the provisions set out in the GDPR, Regulation (EU) 2018/1725 and Directive (EU) 2016/680.

The AI Act therefore neither replaces the GDPR nor limits its application.[18] Entities required to comply with the AI Act are, irrespective of the risk analysis and assessment provided for therein and the choice of risk treatment measures, also required to comply with the personal data processing regimes laid down in the GDPR. The requirements imposed on providers and deployers by the AI Act, particularly those concerning documentation intended to ensure transparency, are designed to guarantee that compliance with this requirement can be assessed within the specific context in which AI systems are used to process personal data.[19] Classifying a given AI system as a high-risk system and confirming its compliance with the requirements laid down in the AI Act does not mean that the use of that system is lawful under other acts of Union law or under national law compatible with Union law in the field of personal data protection. Similarly, the *Conformité Européenne* (CE) marking required for high-risk systems does not establish such lawfulness. In each case, the system must be assessed in the light of the principles set out in Article 5 GDPR. The controller, within the meaning of the GDPR, and the deployer (user), within the meaning of the AI Act, will seek guidance on how to bring the use of an AI system into compliance with those regulations.[20] Entities falling within the scope of the AI Act are therefore, in essence, controllers within the meaning of the GDPR. This means that they are fully obliged to comply with the principles of the GDPR, such as:

- lawfulness (Article 5(1)(a) GDPR), which determines the permissible purposes for which personal data may be processed;
- transparency (Article 5(1)(a) GDPR), which requires the controller to formulate information and all communications relating to the processing of personal data in such a way that they are easily accessible and understandable and expressed in clear and plain language;
- purpose limitation (Article 5(1)(b) GDPR), which provides that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes;
- adequacy (Article 5(1)(c) GDPR), under which the data collected must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accuracy (Article 5(1)(d) GDPR), which requires the data collected to be accurate and, where necessary, kept up to date, and obliges the controller to take every reasonable step to ensure that personal data which are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

---

[18] For more on the relationship between the AI Act and the GDPR, see A. Thomaidou, K. Limniotis, 'Navigating Through Human Rights in AI: Exploring the Interplay between GDPR and Fundamental Rights Impact Assessment', *Journal of Cybersecurity and Privacy*, 2025, Vol. 5, Issue 1, article number 7, pp. 1–39.

[19] M. Susałko, 'Podejście oparte na ryzyku w projekcie aktu w sprawie sztucznej inteligencji i RODO', in: Groszkowski J. (ed.), *Projektowanie systemów SI zgodnych z RODO*, Warszawa, 2023, p. 97.

[20] Ibidem, p. 98.

- storage limitation (Article 5(1)(e) GDPR), which means that personal data may not be kept for longer than is necessary for the purposes for which they were collected;
- integrity and confidentiality (Article 5(1)(f) GDPR), which require the controller to store personal data in a manner that ensures protection against unauthorised or unlawful processing and against accidental loss, destruction or damage;
- accountability (Article 5(2) GDPR), under which the controller is responsible for compliance with the provisions of the GDPR and must be able to demonstrate such compliance.

PROFILING AND SCORING

The second issue related to personal data protection and the development of new technologies is profiling (scoring). Recital 71 of the GDPR defines profiling as an activity that:

> 'consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her'.

Scoring consists of two elements: first, the automated processing of a natural person's personal data and, second, the legal effects produced by such processing, because:

> 'The scope of Article 22 [of the Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data] does not cover every process based on automated processing, but only activities that result in a "decision" being made in respect of a natural person – an externally directed, constitutive act resulting from a choice between at least two alternative possibilities.'[21]

Thus, as stated in the judgment of the Court of Justice of the European Union of 7 December 2023 in Case C-634/21:

> 'Article 22(1) of the GDPR must be interpreted as meaning that the automated establishment, by a credit information agency, of a probability value based on personal data relating to a person and concerning his or her ability to meet payment commitments in the future constitutes "automated individual decision-making" within the meaning of that provision, where a third party, to which that probability value is transmitted, draws strongly on that probability value to establish, implement or terminate a contractual relationship with that person.'[22]

---

[21] M. Kupiec, 'Nowe spojrzenie na zautomatyzowane podejmowanie decyzji w rozumieniu art. 22 RODO – glosa do wyroku Trybunału Sprawiedliwości z 7.12.2023 r., C-634/21, OQ przeciwko Land Hessen przy udziale: SCHUFA Holding AG', *Europejski Przegląd Sądowy*, 2024, No. 3, p. 34.

[22] CJEU judgment of 7 December 2023, *OQ v Land Hessen*, C-634/21, ECLI:EU:C:2023:957.

The legal consequences for a natural person are therefore directly dependent on the outcome of the scoring, because:

> 'For the result of automated processing of personal data carried out by an entity other than the final decision-maker to be regarded as a "decision" within the meaning of Article 22 GDPR, the result of such a data-processing operation must have a clear and almost binding influence on the final decision of the controller determining the factual or legal situation of the natural person. Consequently, even where, within the organisation of the controller acting as the decision-maker, the final decision is taken by a human on the basis of the output of a third-party system, the person subject to that decision will still be able to rely on the safeguards laid down in Article 22 GDPR.'[23]

Therefore, even where the result of profiling is approved by a human, this does not exclude the protection of the personal data of the person subjected to such processing. The person profiled may still rely on the protection of their personal data provided for by the GDPR.

It is pointed out that:

> 'Automated decision-making, including profiling, is one of the most controversial issues in personal data protection and, at the same time, one whose role in the information society will continue to grow. It plays a significant role, *inter alia*, in the context of technologies such as Big Data and the Internet of Things. Decisions based on automated data processing, including profiling, are already widely used in areas such as finance, banking, insurance and healthcare.'[24]

Thanks to new technologies such as Big Data, scoring provides information about natural persons essentially without human intervention. The fundamental feature of a Big Data set

> 'is not the breadth of the available information, but the ease with which it can be combined with new resources and the possibility of deriving from it new knowledge that was not the reason for its collection. We are therefore dealing with a combination of information, technology, and process. Data within Big Data are obtained from many different, dispersed datasets and may form a single, large database. They may also form a network of connections between values contained in different databases. The collected data are analysed using complex algorithms, with the resulting knowledge intended to enable accurate decisions to be made quickly and easily'.[25]

Big Data therefore represents an extensive and constantly expanding collection of information from which, through appropriate information technology operations, the data required by users are obtained.

The rules governing profiling are set out in Article 22 GDPR, which establishes the principle that a natural person has the right to refuse to be subject to scoring. There are, however, three exceptions:

---

[23] M. Kupiec, 'Nowe spojrzenie…', op. cit.

[24] M. Czerniawski, 'Artykuł 22', in: Bielak-Jomaa E., Lubasz D. (eds), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa, 2018, p. 561.

[25] C. Zapała, 'Przetwarzanie informacji i danych osobowych w rolnictwie w ramach Big Data', *Studia Iuridica*, 2018, Vol. 78, p. 521.

- profiling is necessary for entering into a contract between the controller and the natural person whose data are processed;
- profiling is authorised by Union law or the law of a Member State to which the controller is subject, and national law lays down suitable measures to safeguard the person being profiled;
- the person subject to scoring has given their explicit consent.

It should be added that, even where there are grounds for profiling, the controller is obliged to implement measures to safeguard the rights, freedoms and legitimate interests of the data subject, including at least the right to obtain human intervention on the part of the controller, to express their point of view and to contest the decision. Accordingly, at the end of such a process there should always be a human being who verifies the outcome of the scoring.

> 'The adoption of this legal structure confirms the legislature's intention not to subject decisions of significance to the data subject entirely to automated processes and to enable the data subject to respond to such actions by the controller. The specification of minimum requirements in this regard means that the controller may also guarantee the data subject other options relating to decision-making in a fully automated procedure.'[26]

It is therefore not permissible, even with the consent of the person being profiled, to create profiling systems that operate solely in an automated manner and exclude any possibility of human verification of the scoring outcome.

Article 22(4) GDPR prohibits the processing of sensitive data in the course of profiling. In accordance with Article 9(1) GDPR, such data include information concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data processed for the purpose of uniquely identifying a natural person, and data concerning a natural person's health, sex life or sexual orientation. This prohibition does not apply where the data subject has given explicit consent to the processing or where the processing is necessary for reasons of substantial public interest and is based on law.

SOCIAL MEDIA

The third challenge for personal data protection concerns the application of the GDPR to social media. It should be noted that, although social media have existed for over 20 years, they remain difficult to define. It is most commonly stated that they comprise three elements: Web 2.0, that is, a subsequent generation of internet services in which the creation of content by users themselves and their mutual interaction play a particular role; content; and the communities that form around

[26] P. Fajgielski, 'Komentarz do rozporządzenia nr 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)', in: Fajgielski P., *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, 2nd edn, Warszawa, 2022.

such services.[27] Social media are a form of Big Data, although their content is primarily the result of the activities of their users. However,

> 'What distinguishes social media from traditional media is primarily:
> 1. Reach: in both cases, the media are capable of reaching a wide audience, even on a global scale. Traditional media are, however, subject to organisational, technological and cost-related limitations, whereas information in social media is, as a rule, decentralised and independent. It may be said that its reach is determined solely by its attractiveness to recipients.
> 2. Accessibility: in traditional media, accessibility is limited by the entities that control them, such as governments or corporations, whereas social media are generally free of charge and accessible to everyone.
> 3. Usability: traditional media require appropriate training and skills, whereas social media rely mainly on what most users are able to do.
> 4. Immediacy: information appears and spreads much more rapidly in social media than in traditional media.
> 5. Persistence: whereas content in traditional media cannot be altered once it has been published, information in social media may be updated on an ongoing basis.'[28]

Social media therefore use the Internet and information technologies to create content that is highly flexible, enabling them to respond to events, whether significant, local or individual, much more rapidly than traditional media.

Social media are interactive platforms on which data in the form of text, photographs, and audio and video recordings are made public. Undoubtedly, each of these media may contain data relating to a specific identified person or to an identifiable person (Article 4(1) GDPR). Given that social media are very often used for self-presentation, there is a high likelihood that personal data will be disclosed on such platforms. Social media users are often unaware of the categories of personal data they publish online. In addition to 'ordinary' data (Article 6 GDPR), they also publish sensitive data (Article 9 GDPR) revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, and data concerning health, sex life or sexual orientation. Textual posts often reveal preferences and affiliations classified as sensitive data; 'about me' sections may indicate political views, religious beliefs or sexual orientation, depending on the privacy settings; photographs and video recordings may reveal data concerning health, such as pregnancy or disability, race, origin or place of residence. In most typical situations, the mere viewing of information constituting the personal data of persons who have disclosed them on social media takes place with their consent. The terms and conditions of social

---

[27] For more, see A.M. Kaplan, M. Haenlein, 'Users of the World, Unite! The Challenges and Opportunities of Social Media', *Business Horizons*, 2010, Vol. 53 No. 1, pp. 59–68; C.T. Carr, R.A. Hayes, 'Social Media: Defining, Developing, and Divining', *Atlantic Journal of Communication*, 2015, Vol. 23, No. 1, pp. 46–65; J.A. Obar, S. Wildman, 'Social Media Definition and the Governance Challenge', *Telecommunications Policy*, 2015, Vol. 39, No. 9, pp. 745–750; M. Popiołek, *Czy można żyć bez Facebooka? Rola serwisów społecznościowych w sieciowym społeczeństwie informacyjnym*, Kraków, 2018, pp. 25 et seq.

[28] A. Szydłowska, 'Charakterystyka mediów społecznościowych jako narzędzia komunikacji firmy z klientem', *Zeszyty Naukowe ZPSB Firma i Rynek*, 2013, Vol. 45, No. 2, pp. 37–38.

networking services state that content posted using their tools may be visible to and used by other users. In this context, by making their personal data public on social media profiles, the data subject consents to their processing. The processing of such personal data may therefore take place on the basis of Article 6(1)(a) GDPR. It should additionally be noted that personal data disclosed on social media may be processed in the course of employment, in which case Article 6(1)(f) GDPR will provide an alternative legal basis for such processing.

A different normative configuration arises where personal data disclosed on social media are published by a third party. Provided that the online publication was lawful, the processing of third-party personal data disclosed in such a publication falls within the scope of the legitimate interest referred to in Article 6(1)(f) GDPR.

The viewing of personal data posted on social networking sites may fall outside the scope of the GDPR, provided that it is carried out by natural persons in the course of a purely personal or household activity, that is, without any connection to a professional or commercial activity. Personal or household activities may include, *inter alia*, correspondence and the holding of addresses, the maintenance of social relationships, and online activity undertaken in the context of such activities (recital 18 and Article 2(2)(c) GDPR). It should be noted, however, that personal data available on social media are increasingly collected by specialised computer programs based on artificial intelligence. Three basic stages of their operation may be distinguished. First, targeting information online, usually through the use of search engines or specialised tools for searching resources. Second, crawling, that is, the systematic searching and downloading of large quantities of data by spider programs (web bots), which visit successive URLs or social networking sites according to an adopted strategy. Third, extraction, that is, the use of tools to extract the information found and stored in a format suitable for further analysis. Web scraping is also distinguished, understood as the automated copying of data and their placement in a centralised database for future analysis; it provides a set of techniques and tools for extracting information from websites.[29] Data obtained in this way may enable automated profiling to assign users to specific groups, for example based on interests, political views or lifestyle; the creation of individual recommendation profiles that tailor content to the user's interests; and the creation of behavioural advertising, involving targeting based on browsing history and activity. Location tracking is also relatively common. The processing of user-generated content (UGC) is particularly far-reaching in the context of personal data protection and involves the processing of photographs, texts, videos and metadata for the purpose of identifying topics, analysing sentiment or identifying individuals. Sharing personal data on social media also entails the risk of fraud, phishing, account takeover, identity theft, data leaks and loss of control over content.

Even a general outline of the issues surrounding the processing of personal data on social media makes it possible to understand the vast area within which conflicts may arise in connection with compliance with the regimes laid down by

[29] R. Poynter, *The Handbook of Online and Social Media Research: Tools and Techniques for Market Researchers*, Chichester, 2010, pp. 223 et seq.

the GDPR. Undoubtedly, this area of judicial protection of individuals is, and will continue to be, a major challenge for the administration of justice, both nationally and internationally. By its nature, the involvement of courts in matters concerning threats associated with the processing of personal data on social media is reactive and subsequent, that is, it comes into play only once such an infringement has actually occurred. For this reason, it is worth referring to the fundamental issues with which courts have had to contend in this area.

In Case C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*,[30] the Court of Justice observed that social networking sites are entities which primarily determine the purposes and means of processing their users' personal data and are therefore controllers within the meaning of Article 4(7) GDPR. It further stated that the mere fact of using a social network such as Facebook does not make a Facebook user jointly responsible for the processing of personal data carried out by that network. The Court noted, however, that the administrator of a fan page hosted on Facebook, by creating such a page, enables Facebook to place cookies on the computer or any other device of a person visiting the fan page, irrespective of whether that person has a Facebook account. Consequently, the Court held that the administrator of a fan page hosted on Facebook bears joint responsibility, at Union level, with Facebook Ireland for the processing of data within the meaning of Article 2(d) of Directive 95/46. The fact that the administrator of a fan page uses the platform offered by Facebook and the services available on it does not release that administrator from its obligations in the field of personal data protection. In those circumstances, recognising the joint responsibility of the operator of the social network and the administrator of a fan page hosted on that network in relation to the processing of the personal data of visitors to that fan page contributes to ensuring more comprehensive protection of the rights enjoyed by persons who visit the fan page.

In Case C-446/21, *Maximilian Schrems v Meta Platforms Ireland Ltd, formerly Facebook Ireland Ltd*,[31] the Court of Justice held that the principle of 'data minimisation' laid down in Article 5(1)(c) GDPR precludes all personal data obtained by a controller, such as the operator of an online social networking platform, from the data subject or from third parties and collected both on and outside that platform from being aggregated, analysed and processed for the purposes of targeted advertising without any temporal limitation and without regard to the nature of those data. The Court also held that Article 9(2)(e) GDPR must be interpreted as meaning that the fact that a person has made a statement concerning their sexual orientation during a panel discussion open to the public does not authorise the operator of an online social networking platform to process other data concerning that person's sexual orientation, obtained, as the case may be, outside that platform through third-party websites and applications, with a view to aggregating and analysing those data in order to offer that person personalised advertising.

---

[30] CJEU judgment of 5 June 2018, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH*, C-210/16, ECLI:EU:C:2018:388.

[31] CJEU judgment of 4 October 2024, *Maximilian Schrems v Meta Platforms Ireland Ltd, formerly Facebook Ireland Ltd*, C-446/21, ECLI:EU:C:2024:834.

Relying on analogous reasoning, the Court of Justice ruled in Case C-252/21, *Meta Platforms Inc., formerly Facebook Inc., and Others v Bundeskartellamt*.[32] The Court proceeded on the basis that, under the first subparagraph of Article 6(1)(b) GDPR, the processing of personal data by the operator of an online social network, consisting in the collection of data concerning users of that network from other services of the group to which that operator belongs or from visits by those users to third-party websites or applications, the linking of those data to the users' social network accounts and the use of those data, may be regarded as necessary for the performance of a contract to which the data subjects are parties only where that processing is objectively indispensable for a purpose forming an integral part of the contractual performance intended for those users, with the result that the main purpose of the contract could not be achieved without that processing. The Court also pointed out that, where a user of an online social network visits websites or applications relating to one or more of the categories referred to in Article 9(1) GDPR, that user does not manifestly make public, within the meaning of Article 9(2)(e) GDPR, the data concerning those visits collected by the operator of that online social network by means of cookies or similar recording technologies. However, where such a user enters data on those websites or in those applications, or activates buttons integrated into them, such as 'Like' or 'Share' buttons, or buttons enabling the user to identify themselves on those websites or in those applications by using login credentials linked to their online social network account, telephone number or email address, the user manifestly makes public, within the meaning of Article 9(2)(e) GDPR, the data entered in that manner or resulting from the activation of those buttons only where the user has previously and explicitly chosen, where appropriate by individually configuring the relevant settings with full knowledge of the facts, to make the data concerning them publicly accessible to an unlimited number of persons. The collection of data should therefore, first, be transparent, in the sense that the data subject is aware of the processing and its scope; second, have a lawful basis; and third, be carried out in circumstances in which the controller is able to demonstrate that its actions do not infringe the rights and freedoms of the data subject.

Moreover, the use of social media also gives rise to obligations concerning the application of the GDPR to its users. This applies to entities that use social media for commercial purposes by posting links through which their products may be purchased, since a website operator

> 'that embeds on that website a social plugin causing the browser of a visitor to that website to request content from the provider of that plugin and, to that end, to transmit personal data of the visitor can be considered to be a controller, within the meaning of Article 2(d) of Directive 95/46. That liability is, however, limited to the operation or set of operations involving the processing of personal data in respect of which it actually determines the purposes and means, that is to say, the collection and disclosure by transmission of the data at issue'.[33]

---

[32] CJEU judgment of 4 July 2023, *Meta Platforms Inc., formerly Facebook Inc., and Others v Bundeskartellamt*, C-252/21, ECLI:EU:C:2023:537.

[33] CJEU judgment of 29 July 2019, *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV*, C-40/17, ECLI:EU:C:2019:629.

An entity using social media for commercial purposes is therefore a controller of personal data, but only of the data obtained in the course of its activities, and the processing of those data should comply with the principle of lawfulness laid down in Article 5(1)(a) GDPR, that is, it must have a lawful basis.

The Supreme Administrative Court considered a particularly important issue in its judgment of 16 October 2024 in Case III OSK 4984/21. The Court pointed out that the GDPR may apply where a natural person publishes data concerning another natural person on social media. According to the Supreme Administrative Court:

> 'As a rule, content published on social networking sites by natural persons does not fall within the scope of the GDPR, provided that the activity is not professional or commercial in nature and that access to the content is limited to persons selected by the individual making it available. In other words, where the processing extends, even partially, into the public sphere and is therefore directed beyond the private sphere of the person carrying out the processing, it should not be regarded as an activity of a purely "personal or household nature" […]. Of fundamental importance is whether the complainant's data made available on the participant's profile were disclosed in an "open" manner, enabling any person, including persons not authorised by the participant, to access the content posted there.'[34]

Therefore, where a natural person's data are published without their consent on social media profiles that allow any user to access them, that person is entitled to request that the controller cease such practices. It should be noted, however, that not every publication of information on social media without the consent of the person concerned justifies reliance on the protection afforded by the GDPR. Such intervention will be possible only in respect of data that enable the person concerned to be identified; otherwise, there are no grounds for the removal of those data.[35]

MONITORING AND PHYSICAL PROTECTION DEVICES

The fourth issue related to the use of new technologies and the protection of personal data is the processing of personal data in connection with advanced technical devices designed to protect persons or property. In this regard, the judgment of the Supreme Administrative Court of 10 October 2024 in Case III OSK 4804/21[36] provides some guidance on the principles governing the processing of personal data necessary for the use of such devices. The case concerned a processing by a school of a child's fingerprint as biometric data to enable access to the school canteen. The Supreme Administrative Court indicated that, in this regard, the GDPR does not preclude the processing of biometric data by a non-public entity. In addition, the

---

[34] LEX No. 3774694.

[35] Cf. judgment of the Voivodeship Administrative Court in Warsaw of 21 February 2025, II SA/Wa 1253/24, LEX No. 3884766, in which it was held that the administrator of a social media platform is not required to remove a photograph of a person from the website where it is impossible to determine who is actually depicted therein.

[36] CBOSA.

court of cassation identified two basic conditions under which the processing of such data is permitted.

First, consent must be given by the data subject or, in the case of minors, by their legal representatives, since

> 'A systematic analysis of Article 6(1) and Article 9(1) and (2) GDPR has shown that the purpose of processing personal data on the basis of the data subject's consent does not have to arise from provisions of law. This is expressly confirmed by Article 6(3) GDPR, which provides that only the conditions for processing specified in Article 6(1)(c) and (e) must be laid down by Union law or the law of the Member State to which the controller is subject.'

Consent therefore does not have to relate solely to the processing of data which the controller is legally obliged to process. The purpose of the processing must, however, be clearly and lawfully justified.

Second,

> 'There is a strong normative correlation between the principle of purpose limitation (Article 5(1)(b) GDPR) and the concept of consent to the processing of personal data. Giving consent to the processing of personal data the characteristics required by the GDPR – namely, that it be freely given, specific, informed and unambiguous (Article 4(11)) – has the same effect as determining the purpose of that processing in a specified, explicit and legitimate manner (Article 5(1)(b)). Where the personal data controller, in fulfilling the information obligation imposed on it under Article 13(1) GDPR, informs the data subject, at the latest when the personal data are collected, of the purpose of the processing, the scope of the data processed, the method of processing, and the period for which the data will be processed, and that person freely consents to such processing, it must be assumed that the principle of purpose limitation has been observed. The conditions described above for implementing the principle of purpose limitation and the characteristics that consent to data processing must possess are of fundamental importance in determining the scope of application and operation of the principle of data minimisation. In the view of the Supreme Administrative Court, consent to the processing of personal data given in accordance with the requirements laid down in the GDPR defines the limits of the personal data controller's permissible activities, which, by definition, cannot infringe the principle of data minimisation. By giving consenting to the processing of personal data, no later than when the controller begins collecting those data, the data subject accepts the purpose of the processing, the type and scope of the data processed, the quantity of data processed, the method of processing and the period for which the data will be processed. Consent to the processing of personal data therefore is a form of agreement between the data controller and the data subject, the substance of which is their shared assessment that, in order to achieve the purpose accepted by both parties, the best solution is to process personal data of a specified scope and quantity, in the agreed manner and for the necessary period. The parties involved in the data-processing operation – the controller and the data subject – jointly form the subjective assessment that the processing will comply, *inter alia*, with the principle of data minimisation.'

Consent to the processing of personal data given by a natural person should, of course, be freely given and unambiguous, but its content is also important in this regard. The person giving consent should clearly understand the specific actions by the controller concerning the processing of their personal data to which they

are consenting. Such consent, in turn, defines the framework within which the controller may act and beyond which it may not operate.

In various factual and legal contexts, the case law of the courts addresses the processing of personal data obtained through monitoring. From the perspective of the GDPR, three situations may generally be distinguished, each of which is subject to a different legal classification. The first is where monitoring is used on private property and does not extend to neighbouring property that is publicly accessible or owned by third parties. The second is where monitoring is used in the course of a specific commercial or public activity. The third is where monitoring is applied to an employee.

The general framework governing the permissibility of monitoring on private property was outlined by the Court of Justice in its judgment of 11 December 2014 in Case C-212/13, *František Ryneš v Úřad pro ochranu osobních údajů*.[37] Although that judgment was delivered under Directive 95/46/EC, it remains fully relevant because the solutions adopted in the GDPR are identical. The Court pointed out that the use of a camera system which continuously records images of persons and stores them on recording equipment, such as a hard disk drive, and which is installed by a natural person on their family home for the purpose of protecting the property, health and life of the homeowners, but which also monitors a public space, does not represent the processing of data in the course of a purely personal or household activity – currently Article 2(2)(c) of the GDPR. Conversely, it should therefore be assumed that monitoring installed on private property for the purpose of protecting the occupants and their property, and which does not extend to neighbouring properties, is a purely personal or household activity and is therefore excluded from the scope of the GDPR under Article 2(2)(c). It should be added that the Court did not rule out the possibility that the processing of personal data obtained through a domestic monitoring system covering a public space may be justified by the legitimate interests pursued by the data controller, which include, in particular, the protection of the property, health and life of the controller and their family – Article 6(1)(f) of the GDPR. The Court of Justice returned to this issue in Case C-708/18, *TK v Asociaţia de Proprietari bloc M5A-ScaraA*,[38] in which it considered the permissibility of installing a video monitoring system in the common areas of a building. The Court concluded that the 'legitimate interest' within the meaning of Article 7(1)(f) of Directive 95/46/EC (currently Article 6(1)(f) GDPR) constitutes grounds for the processing of personal data obtained through such monitoring. The Court stipulated, however, that it must be examined in each case whether the legitimate interests pursued through the processing of data by a video monitoring system, consisting in ensuring the security of property and individuals and preventing crime, could be achieved just as effectively by other means that interfere to a lesser extent with the fundamental rights and freedoms of data subjects. The Court thus

[37] CJEU judgment of 11 December 2014, *František Ryneš v Úřad pro ochranu osobních údajů*, C-212/13, ECLI:EU:C:2014:2428.

[38] CJEU judgment of 11 December 2019, *TK v Asociaţia de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064.

emphasised the requirement that the processing of personal data obtained through video surveillance be necessary. It also drew attention to the need to comply with the principle of data minimisation, under which consideration must be given to whether it would be sufficient for the surveillance system to operate only at night or outside normal working hours, and whether access to the images should be blocked or the images obscured in areas where surveillance is unnecessary.

The processing of personal data by businesses does not, by definition, represent an activity of a purely personal or household nature. The installation of surveillance systems on properties or in buildings where commercial activities are conducted may be justified under Article 6(1)(f) GDPR by demonstrating a legitimate interest. It must be remembered, however, that in such circumstances the scope of the data processed must be necessary and adequate for the achievement of the purposes associated with that interest.

Administrative courts have resolved a number of disputes concerning the permissibility of processing employees' personal data obtained through video surveillance conducted by employers. It should be noted that Article 88(1) GDPR permits Member States, by law or by collective agreements, to provide for more specific rules than those laid down in the GDPR itself to protect employees' rights and freedoms with regard to the processing of their personal data in the employment context. Such a solution has been adopted in Articles 22^2 and 22^3 of the Labour Code.[39] In their judgments, the courts have pointed out that the lawfulness of installing monitoring systems in or around the workplace depends on demonstrating that this is necessary to ensure employee safety, protect property, control production or preserve the confidentiality of information whose disclosure could expose the employer to damage (Article 22^2 § 1 of the Labour Code). An employer may retain recordings for no longer than three months and may process the recorded images solely for the purposes for which they were recorded (Article 22^2 § 3 of the Labour Code). The courts have strongly emphasised that the lawfulness of processing personal data obtained through monitoring depends on the employer's proper fulfilment of the information obligation[40] (Article 22^2 § 7 and § 8 of the Labour Code and Articles 12 and 13 GDPR in conjunction with Article 22^2 § 9 of the Labour Code).

It may be expected that the future will bring numerous scenarios involving the monitoring of natural persons, the legal assessment of which will require new approaches and unconventional analyses. In the approaching age of artificial intelligence, threats associated with surveillance, identity theft and the creation of false content using images obtained through monitoring systems appear inevitable.

---

[39] Act of 26 June 1974, Employment Code, Journal of Laws 2025, item 277, as amended (hereinafter referred to as the 'EC').

[40] Judgments of the Supreme Administrative Court of 19 September 2024, III OSK 4707/21, and of 20 March 2025, III OSK 6858/21 and III OSK 1340/22; on the admissibility of covert monitoring of employees, see also LEX No. 2418052.

CONCLUSIONS

The dynamic development of information technologies is redefining the conditions in which individuals and institutions operate, but it does not abrogate the fundamental human right to privacy or the obligation to protect personal data. The analysis conducted in this article has shown that the principal challenges arise in four areas: artificial intelligence, profiling and scoring, social media, and monitoring and biometric devices. In each of these areas, the tension between innovation and individual informational autonomy requires a precise legal framework and effective enforcement of the GDPR principles of lawfulness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and accountability.

The Artificial Intelligence Act adopted by the European Union structures the relevant risks by affirming human-centricity and human oversight, while at the same time not replacing the GDPR regime; the provisions of both acts must be applied cumulatively when designing, deploying and using AI systems. Data protection must encompass the entire lifecycle of a system, taking into account data protection by design and by default. Article 4a of the AI Act, as added, provides for a strictly limited possibility of processing special categories of personal data for the purposes of bias detection and correction. Compliance with the AI Act, including the marking or registration of high-risk systems, does not remove the need for a separate assessment of the lawfulness of processing under the GDPR.

The case law of the Court of Justice of the European Union and national courts has clarified the limits of permissible profiling and the standards applicable to processing on social media and through monitoring systems. It has emphasised the importance of consent, where it constitutes the legal basis for processing, transparency, the genuine possibility of human intervention, and the prohibition of excessive aggregation of data, particularly sensitive data. In the workplace and in common areas, monitoring may be based on a legitimate interest only where it is necessary, proportionate and appropriately limited.

Consequently, effective data protection in the information society requires not only the continued refinement of legislation, including the GDPR and the AI Act, but also its consistent enforcement, strong accountability mechanisms for controllers and system providers, the implementation of data protection by design and by default, and greater user awareness. Only the synergy of law, technology and organisational practice can maintain a balance between digital development and respect for individual dignity and freedom.

BIBLIOGRAPHY

Burczaniuk P., 'Tworzenie prawa sztucznej inteligencji – wyzwania i perspektywy', *Prawo i Więź*, 2024, Vol. 51, No. 4.

Carr C.T., Hayes R.A., 'Social Media: Defining, Developing, and Divining', *Atlantic Journal of Communication*, 2015, Vol. 23, No. 1.

Czerniawski M., 'Artykuł 22', in: Bielak-Jomaa E., Lubasz D. (eds), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa, 2018.

Dubisz S. (ed.), *Wielki słownik języka polskiego PWN. Tom H–N*, Warszawa, 2018.

Fajgielski P., 'Komentarz do rozporządzenia nr 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)', in: Fajgielski P., *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, 2nd edn, Warszawa, 2022.

Flisak D., *Akt w sprawie sztucznej inteligencji*, LEX/el., 2024.

Gellert R., 'Understanding the Notion of Risk in the General Data Protection Regulation', *Computer Law & Security Review*, 2018, Vol. 34, No. 2.

Golka M., 'Czym jest społeczeństwo informacyjne', *Ruch Prawniczy, Ekonomiczny i Socjologiczny*, 2005, Vol. 67, No. 4.

Harari Y.N., *Sapiens: od zwierząt do bogów*, trans. Hunia J., Kraków, 2017.

High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, Brussels, 2019; https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2019/11-06/Ethics-guidelines-AI_EN.pdf (accessed: 21 July 2026).

Kaplan A.M., Haenlein M., 'Users of the World, Unite! The Challenges and Opportunities of Social Media', *Business Horizons*, 2010, Vol. 53, No. 1.

Kłos P., 'Inteligentne systemy wspomagania decyzji w procesie podejmowania decyzji prawnych – wybrane zagadnienia z perspektywy teoretycznoprawnej', *Ruch Prawniczy, Ekonomiczny i Socjologiczny*, 2025, Vol. 87, No. 2.

Kupiec M., 'Nowe spojrzenie na zautomatyzowane podejmowanie decyzji w rozumieniu art. 22 RODO – glosa do wyroku Trybunału Sprawiedliwości z 7.12.2023 r., C-634/21, OQ przeciwko Land Hessen przy udziale: SCHUFA Holding AG', *Europejski Przegląd Sądowy*, 2024, No. 3.

Michalski K., 'Konflikty interesów związane z bezpieczeństwem danych osobowych i ochroną prywatności w społeczeństwie cyfrowym', *Zeszyty Naukowe WSIZiA w Warszawie*, 2017, Vol. 15, No. 3(40).

Obar J.A., Wildman S., 'Social Media Definition and the Governance Challenge', *Telecommunications Policy*, 2015, Vol. 39, No. 9.

Palacz K., 'Jak inteligentne jest prawo regulujące sztuczną inteligencję? Próba analizy AI Act na podstawie jej ugruntowania w przestrzeni komercyjnego użycia', *Prawo Mediów Elektronicznych*, 2022, No. 1.

Popiołek M., *Czy można żyć bez Facebooka? Rola serwisów społecznościowych w sieciowym społeczeństwie informacyjnym*, Kraków, 2018.

Poynter R., *The Handbook of Online and Social Media Research: Tools and Techniques for Market Researchers*, Chichester, 2010.

Russell S.J., Norvig P., *Artificial Intelligence: A Modern Approach*, 4th edn, Harlow, 2021.

Rzymowski J., 'Definicja prawnicza sztucznej inteligencji na podstawie rozporządzenia PE i Rady (UE) 2024/1689 w sprawie sztucznej inteligencji', *Przegląd Prawa Publicznego*, 2024, No. 11.

Susałko M., 'Podejście oparte na ryzyku w projekcie aktu w sprawie sztucznej inteligencji i RODO', in: Groszkowski J. (ed.), *Projektowanie systemów SI zgodnych z RODO*, Warszawa, 2023.

Szydłowska A., 'Charakterystyka mediów społecznościowych jako narzędzia komunikacji firmy z klientem', *Zeszyty Naukowe ZPSB Firma i Rynek*, 2013, Vol. 45, No. 2.

Thomaidou A., Limniotis K., 'Navigating Through Human Rights in AI: Exploring the Interplay between GDPR and Fundamental Rights Impact Assessment', *Journal of Cybersecurity and Privacy*, 2025, Vol. 5, Issue 1, article number 7.

Zapała C., 'Przetwarzanie informacji i danych osobowych w rolnictwie w ramach Big Data', *Studia Iuridica*, 2018, Vol. 78.

Cite as:

Szustakiewicz P., Kobak M. (2026), *Protection of Personal Data in the Information Society: Selected Issues*, Ius Novum (Vol. 20) 3, 82–104. DOI 10.2478/in-2026-0030