Z Problematyki Prawa Pracy i Polityki Socjalnej
T. 6(23). Katowice 2025. ISSN: 2719-3462
https://doi.org/10.31261/zpppips.2025.23.04

CC BY SA

Edyta Bielak-Jomaa
University of Lodz
https://www.orcid.org/0000-0002-9217-7959

The use of modern technologies in employment and the protection of personal data – selected issues

Summary

Modern technology and artificial intelligence are increasingly being used in labour relations. Technological solutions support employers in managing the organisation, reduce the cost of supervising the work process, and enable easier and faster control of employees' work. However, the use of technology, especially without sufficient human supervision, raises risks in the area of employees' right to privacy and data protection. Not only can it risk violating data protection laws and lead to violations of employee privacy, discrimination or even dehumanising working conditions. The article aims to identify the potential risks to the protection of employees' personal data in connection with the use of high-tech solutions and artificial intelligence in labour relations, and the obligations of the employer of data processing, in accordance with the principles set forth by the RODO.

Keywords: new technologies, artificial intelligence, personal data, processing of employees' personal data, principles of personal data processing, modern technologies in employment

1. Introduction

Employers are increasingly turning to digital tools to help them modernise and streamline their organization's management model. The implementation of new technologies makes it possible to automate business processes, streamline, accelerate and increase the quality of activities performed by the employees. Used properly, the tools allow to improve the efficiency of operations, optimise costs, and thus increase the competitiveness of companies. However, new technologies also create new tasks for employees. New occupations and job titles, new specialised activities and jobs are being created, in which la-

bour has a relative competitive advantage in relation to capital[1]. Thus, it should be emphasised that the development of technology and artificial intelligence is extremely important, and its use can bring significant benefits to its creators, employees and employers themselves.

At the same time, the use of new technologies may involve certain risks and challenges for employers, such as violation of labour laws, liability to employees and third parties when their rights and freedoms are threatened. Employees, in turn, do not have sufficient knowledge about the proper use of new technologies and the responsibilities for their misuse[2]. Taking into account the ever-increasing processing capabilities, the ever-faster and cheaper flow of data, the possibilities of combining them, the ease of manipulation and the asymmetries of information, it becomes increasingly important to protect personal data. This is because the introduction of advanced technologies may involve threats to the organization's cyber security and the risk of data loss.

2. Modern technologies in employment

A variety of technological solutions are being used in labour relations: process automation, Internet of Things (IoT), Cloud Computing, Big Data, biotechnology, robotics, augmented and virtual reality[3]. Artificial intelligence is also growing in importance in labour relations. It has a growing range of applications, from relatively simple Chatbot used for customer service to more complex analytical solutions based on deep learning[4]. An extremely important element of high-tech, system-based artificial intelligence is the use of data processing technology (including personal data), the ability of systems to make decisions or perform specific tasks with at least a partial representation of human intelligence, as well as the ability to learn and improve on

[1] Ł. Arendt, E. Kwiatkowski: *Kontrowersje wokół wpływu nowoczesnych technologii na zatrudnienie i bezrobocie*. "Ekonomista" 2023, no. 2, p. 199.

[2] N. Bender: *Prywatność pracowników vs. nowoczesne technologie*. "Monitor Prawa Pracy" 2020, no. 4, p. 24.

[3] K. Piwowarska: *Czy nowe technologie zrewolucjonizują rynek pracy?* "Studia Prawnicze. Rozprawy i Materiały" 2018, no. 2(23), pp. 36–147.

[4] J. Vrbka, E. Nica, I. Podhorská: "Equilibrium" 2019, vol. 14, no. 4, p. 739.

the basis of collected information, generate results and provide predictions related to labour relations tasks[5].

Technology is used throughout the hiring cycle and at every stage. In the recruitment process, employers use systems and tools that automate recruitment activities and improve its efficiency. The systems and applications allow to control every stage of the process, from the preparation and publication of an ad in multiple portals simultaneously, and facilitate contact with applicants. Voicebot and Chatbot, which are used during recruitment, make it possible to ask candidates questions (about language skills, education) and verify this information in real time. With the use of artificial intelligence, employers will be able to use video platforms equipped with software to analyse the facial expressions and behaviour of a job candidate and, based on this, create further data determining the suitability of a person for the employer[6]. Technology and algorithms are used when assigning tasks to an employee, evaluating performance, and making decisions about continued employment or its termination[7].

Modern technologies also help in organising and conducting training, developing criteria for selecting employees for layoffs, establishing criteria for acquiring key – from the employer's point of view – skills, calculating salaries, talent acquisition and management. They are also used for evaluating employees, forecasting work performance and determining employee involvement in work processes, employee productivity and their suitability for the employer.

The literature indicates that the changes in labour relations associated with the use of modern technology will be manifold – both in the area of health and safety, the right to privacy (for example, in the context of monitoring the workplace and monitoring the activities of the employee), the organisation of working time and many other areas[8].

[5] P. Nowik: *Definicja sztucznej inteligencji w nauce prawa pracy*. "Praca i Zabezpieczenie Społeczne" 2023, no. 9, p. 7.

[6] *Nowe technologie w HR. Raport*, https://mycompanypolska.pl/artykul/nowe-technologie-w-hr-raport/10919 (Accessed: 12.02.2024).

[7] Ł. Pisarczyk: *Stosunek pracy wobec zmian technologicznych*. In: *Prawo pracy i prawo socjalne: teraźniejszość i przyszłość. Księga jubileuszowa dedykowana Profesorowi Herbertowi Szurgaczowi*. Eds. R. Babińska-Górecka, A. Przybyłowicz, K. Stopka, A. Tomanek. Wrocław 2021, p. 155.

[8] See: M. Madej-Kaleta: *Nowoczesne technologie w gospodarce a ochrona pracowników w prawie pracy*. In: *Prawo pracy. Między gospodarką a ochrona pracy. Księga Jubileuszowa*

The management of the work process and the control or supervision of the work and the worker are carried out through the use of digital tools that can be managed by different entities and, increasingly, through automated systems that are even beyond the control of the employer.

With the development of new technologies, one of the most important challenges facing employers is the protection and security of personal data, processed by the employer (data controller), especially with the use of such technologies as background screening, acquisition and use of biometric data, data from various forms of monitoring, radio-frequency identification (RFID), streamlining organisational processes or employee control by implanting subcutaneous microchips.

Indeed, these solutions can be based on technologies that collect and store data, but also on algorithmic solutions that allow their collation, modification, transmission, i.e. technologies that "feed on data" and can create new personal data, often without human involvement. The methods of analysis can be more (complex biometric technologies) or less intrusive (such as simple counting algorithms). An example of this is employee monitoring. It allows to ensure the safety and security of property (premises and equipment) or detect any kind of violation of the obligation to keep confidential information that is part of the employer's capital[9], and for this purpose it records and stores the record, but at the same time it can offer many additional "amenities", such as the ability to locate the whereabouts of the employee, to control and monitor his activity or business mail[10]. Software that is used, for example, to identify, recognise and analyse faces works differently depending on the age, gender and ethnicity of the person being identified. Algorithms operate based on varying demographics, so facial recognition biases risk exacerbating prejudice among the public[11].

Profesora Ludwika Florka. Eds. M. Latos-Miłkowska, Ł. Pisarczyk. Warszawa 2016, pp. 252–262.

[9] M. Barański, M. Giermak: *Przetwarzanie danych osobowych w kontekście zatrudnienia pracowniczego (uwagi de lege ferenda)*. "Państwo i Prawo" 2017, no. 9, pp. 90–91.

[10] D. Dörre-Kolasa: *Monitoring w miejscu pracy a prawo do prywatności*. "Praca i Zabezpieczenie Społeczne" 2004, no. 9, pp. 10–12.

[11] *Guidelines 3/2019 on the processing of personal data by video devices Version 2.0*, adopted on January 29, 2020, pp. 5–6.

3. The concept of personal data

From the point of view of the issue under analysis, the concept of personal data is of key importance. The legal definition of personal data is contained in Article 4 § 1 of the General Data Protection Regulation (GDPR)[12]. According to it, personal data is any information about an identified or identifiable natural person ("data subject"). Personal data is information of a personal nature, which includes data with characteristics that directly or indirectly identify a person, related to the identifier used, such as name, identification number, but also e.g. date of birth, address of residence and other factors such as gender, eye colour, weight, height or other biometric data indicating biological characteristics. These are, thus, factors of a physical and physiological nature, but also information regarding views, beliefs, statements, information regarding the genetic, psychological, cultural, social, as well as economic identity of the natural person[13]. These factors, therefore, include not only information of a personal nature, but also property, content strictly of a person's private and family life, as well as information about any activity, professional relationship or economic or social behaviour, regardless of the position taken, the characteristics of objectivity or truthfulness, as long as they make it possible to meet the premise of connection and identify person, but also information about any activity, professional relationship, or economic or social behaviour, regardless of position, the characteristics of objectivity or truthfulness, as long as they make it possible to meet the condition of relationship and identifiability of the natural person to whom they relate[14].

The phrase "any information" indicates that this concept is open-ended. It can also include hitherto unknown categories of data[15], any

[12] 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), Official Journal of the European Union, L 119/1.

[13] D. Lubasz: *Komentarz do art. 4 RODO*. In: *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*. Eds. E. Bielak-Jomaa, D. Lubasz. Wolters Kluwer 2018, p. 171.

[14] Ibidem, pp. 171–172, CJEU, Judgement of 20 December 2017, No. C-434/16, Peter Nowak vs. Data Protection Commissioner, ECLI:EU:C:2017:994.

[15] P. Fajgielski: *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*. Warszawa 2022, p. 106; CJEU, 9 November 2010, Joined cases C-92/09 and C-93/09, Volker und Markus Schecke GbR and Hartmut Eifert vs. Land Hessen, ECLI:EU:C:2010:662.

statements about a person, including subjective opinions and assessments, and even false or unverified information, regardless of the form in which it is presented, which concerns an identified or identifiable person (that is, not necessarily identifying data), if it relates to the identity, characteristics or behaviour of a person, or if the information determines or influences the treatment or evaluation of a person[16]. It is also information about a particular employee that is the result of modifying, observing, inferring about him, including if these operations are carried out in information systems, using technological tools and artificial intelligence solutions. The information must only relate to a specific person, so it must be information about that person[17].

The use of modern technology makes it possible to base personal data processing operations on automated decision-making, including in the form of profiling[18]. Profiling is the collection of information about an individual (or a group of individuals) and the assessment of their characteristics or behavioural patterns in order to place them in a specific category or group, in particular to analyse and/or predict about, for example, their ability to perform a task, interests, or possible behaviour[19].

4. Risks of using new technologies in the context of employee data protection

The development of new technologies is not only an opportunity to optimise employees' working time and reduce employers' operating costs, but also risks in the context of data protection regulations. This is particularly relevant in the context of using artificial intelligence sys-

[16] Article 29 Data Protection Working Party: *Paper on Data Protection Issues Related to RFID Technology*, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_pl.pdf (Accessed: 12.02.2024).

[17] Article 29 Data Protection Working Party: *Opinion 4/2007 on the Concept of Personal Data,* WP 136, 20 June 2007, p. 26.

[18] Profiling, under Article 4(4) of the GDPR, means any form of automated processing of personal data that involves the use of personal data to evaluate certain personal factors of an individual, in particular to analyse or predict aspects relating to that individual's performance, economic situation, health, personal preferences, interests, reliability, behavior, location or movement.

[19] Article 29 Data Protection Working Party: *Guidelines on Automated Decision-Making in Individual Cases and Profiling for the Purposes of Regulation 2016/679,* https://www.uodo.gov.pl/data/filemanager_pl/908.pdf (Accessed: 12.02.2024).

tems, such as ChatGPT, which are based on large language models. This is because they learn from huge amounts of data that are publicly available on the Internet and include personal data.

Technologies that process personal data may change the conditions of the work environment, which may manifest itself in the creation of certain risks for employees and data subjects. Among them, the following are pointed out: profiling of employees and others; risk of discrimination; invasion of privacy; lack of transparency in the processing of personal data by Chatbot, lack of knowledge of employees regarding data processing both at the stage of "training" and use of artificial intelligence models on which they are based.

Technologies based on complex mathematical algorithms that collect information about an employee from various sources (the employer's IT systems, intranet resources, the Internet, the employer's social media, or the employee's private social profiles), then collate and analyse it based on opaque algorithms and employees' lack of knowledge of what sources and what data about them are collected and processed, can lead to employee profiling. Consequently, a person can be permanently associated with a specific category and assigned specific preferences, which can lead to discrimination against the employee. Even more questionable is profiling based on systems that make decisions on their own (the so-called automated decision-making). This is because in systems based on algorithms, learning systems and artificial intelligence, the decision is not subject to any human control. According to Article 22(3) of the GDPR, the data subject (employee) has at least the right to obtain human intervention from the controller (employer). Human intervention is a key element of data protection under the GDPR, and any review of decisions made by artificial intelligence must be carried out by a person with the authority and ability to change the decision[20].

The increase in the amount of data generated in the work environment, coupled with new techniques for analysing and collating data, can create the risk of further non-compliant processing. An exam-

[20] Article 29 Data Protection Working Party: *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679*, adopted on 3 October 2017, as last revised and adopted on 6 February 2018, https://www.uodo.gov.pl/data/filemanager_pl/908.pdf (Accessed: 12.02.2024).

ple of this is the use of systems that are legally installed to protect the employer's property, and are used to monitor the availability and performance of employees or to continuously track employee movements and behaviour[21]. New forms of data processing, such as those indicating the use of online services or location data from a smart device, are much less visible to employees than other more traditional forms, such as overt video surveillance. As a result, employees are often unaware of the use of these technologies, and employers may unlawfully process the data without notifying the employees[22]. Artificial intelligence and monitoring technologies, such as wearable devices, combined with the Internet and large data sets can lead to the loss of employee control over their own data, to ethical issues, and pressure on employee productivity.

The rapid adoption of new information technologies in the workplace in the form of infrastructure, applications and smart devices allows for new types of systematic and potentially invasive data processing. Algorithms not only aggregate data, but also take it to the "next", more complex level, which can lead to employee profiling[23], and this, in turn, can lead to discrimination against employees, especially in labour relations. This is because it relates directly to the assessment of employee performance, health, personal preferences, behaviour, location, reliability. Meanwhile, the operation of the algorithm is not fully objectified, as the result depends on the assumptions made and the data provided. If the former are flawed (discriminatory) and the latter inaccurate, there may be a violation of the principle of equal treatment and even discrimination against employees[24].

In addition, it is possible to use personal data beyond its original purpose of collection to explore or apply new employer purposes and opportunities. Data analytics includes methods and patterns of use that neither the data collector nor the data subject considered or could even

[21] Article 29 Data Protection Working Party: *Opinion 2/2017 on Data Processing at Work*, https://iod.uj.edu.pl/documents/138774264/138805617/Opinia_na_temat_przetwarzania_danych_w_miejscu_pracy.pdf/88fef283-2478-4a1a-9e15-28f0c53ef944 (Accessed: 12.02.2024).

[22] Ibidem.

[23] M. T. Bodie, M. A. Cherry, M. L. McCormick, J. Tang: *The Law and Policy of People Analytics*. "Colorado Law Review" 2017, vol. 88, no. 4, pp. 999–1000.

[24] Ł. Pisarczyk: *Stosunek pracy…*, p. 157; D. Dzienisiuk: *Dyskryminacja w cyfrowym świecie pracy*. In: *Prawo pracy i prawo socjalne*..., pp. 72–74.

have imagined at the time of data collection. It should be added that in the context of personnel analytics, the risk may relate to the accuracy of personal data, as employers may use algorithms that will make assessments of employees resulting from the combination of data sets, including personal data, and their processing[25].

Employers who implement new technologies that characterise, evaluate, specify, place employees on a scale of suitability, punish, define standards which, if not met, lead to dismissal, must be aware of the risks associated with the possibility of dehumanisation, evaluating employees solely by machine, reinforcing social inequality, as well as violating the dignity of the employee[26].

5. Personal data processing rules and standards vs. advanced technologies in the workplace

In the era of the growing role of modern technology and artificial intelligence in the workplace, it is important to ensure compliance with data protection regulations. The processing of personal data by technology and artificial intelligence must comply with the principles relating to the processing of personal data indicated in Article 5 of the GDPR: legality, transparency, minimisation of information collected, data retention and security of processing. The principles set forth in this provision are general standards expressing the basic ideas and values of personal data protection policy[27].

In any situation of data processing within the framework of modern technologies and artificial intelligence systems, it is necessary to determine the legal basis for the processing. The basis for the processing of data should be determined for both the training stage and the use of these systems. Meanwhile, their processing by operators of artifi-

[25] EDPS: *Opinion on Online Manipulation and Personal Data*, Opinion 3/2018, https://www.edps.europa.eu/sites/default/files/publication/18-03-19_online_manipulation_en.pdf (Accessed: 12.02.2024).

[26] M. Bąba: *Logika algorytmów w świecie pracy ery technologicznej – nowe możliwości i nowe ograniczenia*. "Praca i Zabezpieczenie Społeczne" 2022, no. 8, p. 10; Policy Strategy Working Group 2: *Digital Economy*, Report – adopted October 2020, https://globalprivacyassembly.org/wp-content/uploads/2020/10/GPA-PSWG2_Digital_Economy_Working_Group_Report_public.pdf (Accessed: 12.02.2024).

[27] A. Nerka: *Komentarz do art. 5 RODO*. In: *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*. Ed. M. Sakowska-Baryła. C. H. Beck 2018, p. 142.

cial intelligence technologies (in systems implemented by the employer) is often carried out without indicating the basis and with the lack of correctness of personal data processed and provided by mathematical algorithms. The employer should take care of the correctness of the data with regard to the information created or inferred by the artificial intelligence system (e.g., classification of emails as spam). Artificial intelligence systems that would enable employees using them to make informed decisions should meet transparency requirements, as employees should be aware that they are interacting with artificial intelligence.

Employers collecting personal data (including employee data) are required to specify the purpose for which the data are collected and the retention period. After its expiration, the information should either be deleted or anonymised. This principle is aimed at reducing the collection and storage of personal data and shortening the processing period. In the case of technological solutions, such as ChatGPT, whose algorithms "learn" from the data provided by their users, it will not be possible to implement this principle. The same applies to the principle of data minimisation, according to which personal data should be limited to what is necessary to achieve the purpose of processing.

The GDPR introduces the requirement to maintain an adequate level of protection of personal data and minimise potential threats to the confidentiality, integrity and availability of this information. As a result of this principle, data processors are required to implement appropriate security measures, such as data encryption, limiting access to authorised users (employees) only, regular security reviews and risk management. If advanced technologies and artificial intelligence are used, it can be difficult and sometimes impossible to carry out these responsibilities, especially for an employer who is implementing solutions that expand the level of scalability of information systems and software in an environment of ever-increasing numbers of users or increasing volumes of processed data. The possibility of an unauthorised third-party access to confidential information is also increasing. Consequently, the lack of adequate security may result in the use of artificial intelligence models to extract personal data or, for example, to circumvent privacy safeguards by means of appropriately prepared prompts by artificial intelligence solutions (ChatGPT)[28].

[28] On March 31, 2023, the Italian data protection authority blocked ChatGPT for raising privacy concerns, stressing that there was no legal basis to justify the "massive

The implementation of mechanisms based on modern technologies that affect an employee's right to privacy and the protection of his personal data requires an analysis of potential risks to the rights and freedoms of employees and other persons whose data will be processed[29]. In addition, in accordance with Article 35(1) of the GDPR, if a particular type of processing – in particular using new technologies – by its nature, scope, context and purposes is likely to result in a high risk of infringement of the rights or freedoms of individuals, the controller (employer) shall assess the effects of the planned processing operations on the protection of personal data before starting the processing. In the communication of the President of the Office for Personal Data Protection of June 17, 2019 on the list of types of personal data processing operations requiring an assessment of the effects of processing on the protection of personal data[30], it is indicated that an impact assessment is required for operations involving, among other things, large-scale systematic monitoring of publicly accessible places using elements of recognition of features or characteristics of objects that will be in the monitored space. The examples of such operations are systems for monitoring the working time of employees and the flow of information in the tools they use (e-mail, Internet); collection and use of data by applications installed in mobile devices, including those integrated into a uniform, helmet or otherwise connected to the person acquiring the data; vehicle monitoring systems that establish connections with the environment, including other vehicles, i.e. machine–to–machine communication systems in which the car informs the environment of its behaviour (movement) and, in the event of an emerging danger, receives warning messages from this environment (road infrastructure, other cars).

collection and storage of personal data to 'train' the algorithms underlying the platform." After Open AI made the appropriate changes, in April 2023. the supervisory authority allowed the tool to be offered again in Italy. Among the measures taken by Open AI were detailed descriptions of the artificial intelligence "training and development" process included in privacy policies and other documentation, including what categories of personal data, and for what purposes, are processed.

[29] Case C-131/12, Google Spain vs. Agencia Española de Protección de Datos (AEPD), Judgement of 13 May 2014, ECLI:EU:C:2014:317.

[30] M.P. poz. 666.

The employer's obligation to conduct a risk assessment is in line with one of the fundamental principles under Article 25 of the GDPR – privacy by design and privacy by default, in light of which, taking into account the state of technical knowledge, the cost of implementation and the nature, scope, context and purposes of the processing and the risk of violation of the rights or freedoms of individuals with different probability of occurrence and severity of the risk resulting from the processing, the controller (employer) – both in determining the means of processing and at the time of the processing itself – shall implement appropriate technical and organisational measures designed to effectively implement the principles of data protection and that, by default, only those personal data are processed that are necessary to achieve each specific purpose of the processing. This principle is characterised by the obligation to take proactive measures – it anticipates and prevents the loss of privacy and personal data before they occur. Data protection incorporated into technology should not be treated as an add-on, but as an essential and integral part of the system, without the effect of reducing its functionality[31].

6. Concluding remarks

Modern technologies that process personal data will certainly change the conditions of the work environment, which will manifest itself in the occurrence of risks caused by the complexity of new technologies and work processes. There will be challenges in involving employees in the implementation of digitisation in the workplace. It seems that a tailored system of education and training for employees, as well as the introduction of guidelines and standards to ensure responsible and compliant use of technology in the workplace, will be fundamental to the proper, non-infringing use of technological tools and artificial intelligence solutions. With the increasing power of algorithms, there is a risk of these systems being used to manipulate or exploit personal data, hence the need for clear rules for the ethical use of artificial intelligence.

[31] A. Magiera, J. Wyczik: *Akt o AI w kontekście ochrony danych*. "ABI Expert" 2023, no. 1, p. 15.

Considering the risks and threats to the protection of personal data and privacy of employees and others, employers should include in the organisation's management model the approach of proper design of technical systems, organisation and procedures for the use of advanced technologies. Indeed, the employer may implement and apply solutions for the supervision and control of the employee's work, in order to properly carry out the employee's tasks and duties, but at the same time is obliged to assess the balance between the employer's legitimate interest in protecting its business and the legitimate expectations of protecting the privacy of data subjects, i.e., employees.

It should be noted that technology, especially artificial intelligence, is not a typical work tool that an employee uses to do his job. Rather, it is a solution that forces the employees to cooperate with each other. An employee using such technology not only improves his competence and skills, but also develops the capabilities of this tool, improving it for the tasks he performs.

However, in order for the use of technology and artificial intelligence as a labour tool to serve these purposes, there should be closer cooperation between the employer and employees in research and innovation in the development of digital technologies for the needs of the specific employer. After all, the creation, implementation and use of modern technologies in labour relations should be ethical, safe and convenient, and based on respect for workers' rights.

Bibliography

Arendt, Ł., Kwiatkowski, E.: *Kontrowersje wokół wpływu nowoczesnych technologii nazatrudnienie i bezrobocie*. "Ekonomista" 2023, no. 2, p. 199.

Article 29 Data Protection Working Party: *Guidelines 3/2019 on the Processing of Personal Data by Video Devices Version 2.0*, adopted on January 29, 2020, https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en.

Article 29 Data Protection Working Party: *Guidelines on Automated Decision-Making in Individual Cases and Profiling for the Purposes of Regulation 2016/679*, https://www.uodo.gov.pl/data/filemanager_pl/908.pdf.

Article 29 Data Protection Working Party: *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679*, adopted on 3 October 2017, as last revised and adopted on 6 february 2018, https://www.uodo.gov.pl/data/filemanager_pl/908.pdf.

Article 29 Data Protection Working Party: *Opinion 2/2017 on Data Processing at Work*, adopted on 8 June 2017, https://ec.europa.eu/newsroom/article29/items/610169.

Article 29 Data Protection Working Party: *Opinion 4/2007 on the Concept of Personal Data*, WP 136, 20 June 2007, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf.

Article 29 Data Protection Working Party: *Paper on Data Protection Issues Related to RFID Technology*, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_pl.pdf.

Barański, M., Giermak, M.: *Przetwarzanie danych osobowych w kontekście zatrudnienia pracowniczego (uwagi de lege ferenda)*. "Państwo i Prawo" 2017, no. 9, pp. 90–91.

Bąba, M.: *Logika algorytmów w świecie pracy ery technologicznej – nowe możliwości i nowe ograniczenia*. "PiZS" 2022, no. 8, p. 10.

Bender, N.: *Prywatność pracowników vs. nowoczesne technologie*. "Monitor Prawa Pracy" 2020, no. 4, p. 24.

Bodie, M. T., Cherry, M. A., McCormick, M. L., Tang, J.: *The Law and Policy of People Analytics*. "Colorado Law Review" 2017, vol. 88, no. 4, pp. 999–1000.

CJEU, Judgement of 9 November 2010, Joined cases C-92/09 and C-93/09, Volker und Markus Schecke GbR and Hartmut Eifert vs. Land Hessen, ECLI:EU:C:2010:662.

CJEU, Judgement of 13 May 2014, Case C-131/12, Google Spain vs. Agencia Española de Protección de Datos (AEPD), ECLI:EU:C:2014:317.

CJEU, Judgement of 20 December 2017, Case C-434/16, Peter Nowak vs. Data Protection Commissioner, ECLI:EU:C:2017:994.

Dörre-Kolasa, D.: *Monitoring w miejscu pracy a prawo do prywatności*. "PiZS" 2004, no. 9, pp. 10–12.

Dzienisiuk, D.: *Dyskryminacja w cyfrowym świecie pracy*. In: *Prawo pracy i prawo socjalne: teraźniejszość i przyszłość: księga jubileuszowa dedykowana Profesorowi Herbertowi Szurgaczowi*. Eds. R. Babińska-Górecka, A. Przybyłowicz, K. Stopka, A. Tomanek. Wrocław 2021, pp. 69–76.

EDPS: *Opinion on online manipulation and personal data,* Opinion 3/2018, https://www.edps.europa.eu/sites/default/files/publication/18-03-19_online_manipulation_en.pdf.

Fajgielski, P.: *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych-osobowych. Komentarz*. Warszawa 2022.

Lubasz, D.: *Komentarz do art. 4 RODO*. In: *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*. Eds. E. Bielak-Jomaa, D. Lubasz. Wolters Kluwer 2018, p. 171.

Madej-Kaleta, M.: *Nowoczesne technologie w gospodarce a ochrona pracowników w prawie pracy*. In: *Prawo pracy. Między gospodarką a ochrona pracy. Księga Ju-*

bileuszowa Profesora Ludwika Florka. Eds. M. Latos-Miłkowska, Ł. Pisarczyk. Warszawa 2016, pp. 252–262.
Magiera, A., Wyczik, J.: *Akt o AI w kontekście ochrony danych*. "ABI Expert" 2023, no. 1, p. 15.
Nerka, A.: *Komentarz do art. 5 RODO*. In: *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*. Ed. M. Sakowska-Baryła. C. H. Beck, 2018, p. 142.
Nowe technologie w HR. Raport, https://mycompanypolska.pl/artykul/nowe-technologie-whrraport/10919.
Nowik, P.: *Definicja sztucznej inteligencji w nauce prawa pracy*. "PiZS" 2023, no. 9, p. 7.
Pisarczyk, Ł.: *Stosunek pracy wobec zmian technologicznych*. In: *Prawo pracy i prawo socjalne: teraźniejszość i przyszłość: księga jubileuszowa dedykowana Profesorowi Herbertowi Szurgaczowi*. Eds. R. Babińska-Górecka, A. Przybyłowicz, K. Stopka, A. Tomanek. Wrocław 2021, pp. 149–152.
Piwowarska, K.: *Czy nowe technologie zrewolucjonizują rynek pracy?* "Studia Prawnicze. Rozprawy i Materiały" 2018, no. 2.
Policy Strategy Working Group 2: *Digital Economy*, Report, adopted October 2020, https://globalprivacyassembly.org/wp-content/uploads/2020/10/GPA-PSWG2_Digital_Economy_Working_Group_Report_public.pdf.
Vrbka, J., Nica, E., Podhorská, I.: *Equilibrium* 2019, vol. 14, no. 4, p. 739.

Wykorzystanie nowoczesnych technologii w zatrudnieniu a ochrona danych osobowych – wybrane zagadnienia

Streszczenie

Nowoczesne technologie i sztuczna inteligencja są coraz częściej wykorzystywane w stosunkach pracy. Rozwiązania technologiczne wspierają pracodawców w zarządzaniu organizacją, obniżają koszty nadzoru nad przebiegiem pracy oraz umożliwiają łatwiejszą i szybszą kontrolę pracy personelu. Wykorzystanie technologii, zwłaszcza bez wystarczającego nadzoru ze strony człowieka, rodzi jednak ryzyko w obszarze prawa pracowników do prywatności i ochrony danych. Może to nie tylko grozić naruszeniem przepisów o ochronie danych osobowych, ale również prowadzić do naruszenia prywatności pracowników, dyskryminacji, a nawet odczłowieczenia warunków pracy. Artykuł ma na celu wskazanie potencjalnych zagrożeń dla ochrony danych osobowych pracowników w związku z wykorzystaniem zaawansowanych technologicznie rozwiązań i sztucznej inteligencji w stosunkach pracy oraz obowiązków pracodawcy w zakresie przetwarzania danych, zgodnie z zasadami określonymi w RODO.

Słowa kluczowe: nowe technologie, sztuczna inteligencja, dane osobowe, przetwarzanie danych osobowych pracowników, zasady przetwarzania danych osobowych, nowoczesne technologie w zatrudnieniu