**Bialystok Legal Studies**
**Białostockie Studia Prawnicze**
**2024 vol. 29 no. 2**

sciendo

DOI: 10.15290/bsp.2024.29.02.09

Received: 12.10.2023
Accepted: 17.02.2024

**Iwona Sierocka**
University of Bialystok, Poland
i.sierocka@uwb.edu.pl
ORCID ID: https://orcid.org/0000–0003-1659–1717

# Control of Remote Workers by Means of Artificial Intelligence

**Abstract:** Remote work, by its very nature, is characterised by the performance of the duties of the employment relationship, in whole or in part, at a place chosen by the employee, at a time agreed upon with the employer. Despite the fact that the employee performs his/her work outside the employer's place of business, he/she remains under the employer's control. The issues under consideration here are the scope of this control and the manner in which it is carried out. In my deliberations, I focus on control performed with the use of algorithmic technologies, in particular artificial intelligence, for which a Regulation of the European Parliament and of the Council Laying Down Harmonised Provisions on Artificial Intelligence (Artificial Intelligence Act) was adopted on 23 June 2023.
**Keywords:** algorithmic management, artificial intelligence, remote work

## Introduction

By its very nature, an employment-based job is characterised by the employee's subordination to the employer, which means that the employer is entitled to give instructions to the employee, who is obliged to perform work under the direction of the employer and at a place and time designated by them. The essential expression of the employee's subordination to the employer is his/her dependence regarding the object of performance, whereby the employer indicates the tasks to be performed, specifies the manner in which they are to be performed, as well as the methods and means by which they are to be performed (Judgment of the Supreme Court 2015). A characteristic feature of contractually subordinated work is the possibility of specifying the employee's duties on a daily basis and, in particular, of determining the activities falling within the scope of the agreed type of work and the manner

in which they are to be performed (Order of the Supreme Court 2020). The employee's subordination does not mean constant supervision by a superior over the activities performed; it is sufficient to determine the tasks and the time of their performance and, upon completion, to check the quality and punctuality of the work performed. A remote employee who performs his/her work, in whole or in part, at a place of his/her own choosing, each time agreed with the employer, has more freedom to organise his/her work and to shape his/her work schedule and working hours. However, he/she remains under the employer's control, which can be carried out in the traditional way by inspecting the employee directly at the place where he/she performs remote work. Nowadays, in the era of digital transformation, control carried out with the use of artificial intelligence is becoming increasingly important. The subject of the subsequent discussion will be issues concerning the inspection of employees working remotely. This atypical form of employment for workers was first introduced into Polish legislation by the Act on Specific Solutions Related to Preventing, Counteracting, and Combating COVID-19, Other Infectious Diseases, and Emergency Situations Caused by Them of 2 March 2020. As remote work proved to be a beneficial form of employment for both employees and employers, it was permanently incorporated into the Labour Code by the Act on Amending the Labour Code of 1 December 2022 and Certain Other Acts. The discussion below will focus on the scope of control over an employee performing remote work, as well as the principles and methods of its implementation, with particular emphasis placed on algorithmic technologies, which significantly facilitate the monitoring of employees working remotely but at the same time carry certain risks for employees.

## 1. Guidelines for conducting inspections

According to the wording of Article 67(28) § 1 of the Labour Code, the subject of the employer's control may be the following three areas: 1) performance of remote work, 2) occupational health and safety, and 3) compliance with security and information protection requirements, including procedures protecting personal data. The scope of the inspection is decided by the employer; its subject may be all or some of the spheres indicated by the legislation.

When carrying out the inspection, an employer should comply with the rules set out in any agreement concluded with trade unions, the regulations on remote work and, in the absence of the company's own employment regulations, in the remote work order or agreement concluded with the specific employee. The employer's right to control extends to all employees carrying out remote work, regardless of whether the remote work was entrusted at the start of the employment relationship or during it. The place where the work is performed is also irrelevant; it only influences the manner in which the inspection is carried out. In the case of work carried out

at the employee's place of residence, the inspection activities undertaken by the employer must not violate the privacy of the employee or other persons nor impede the use of the home premises in a manner consistent with their purpose (Article 67(28) § 2 of the Labour Code). The caveats provided for in Article 67(28) § 2 of the Labour Code indicate that the employer's inspection should be limited to the place where the employee actually performs his/her professional duties. Furthermore, it is necessary to carry it out in a way that is least onerous for the household members. In view of the principle of proportionality that applies to the employer, an inspection carried out with the use of modern technology is most convenient. The restrictions indicated do not bind the employer when inspecting remote work carried out away from the employee's place of residence. In such a case, the employer, exercising his/her managerial powers, has the possibility of carrying out the inspection under the rules applicable to all employees.

According to Article 67(28) § 1 of the Labour Code, the inspection is carried out in consultation with the employee at the workplace and during working hours. This provision is mandatory, which means that it cannot be violated even with the consent of the employee (Sobczyk, 2023, para. 2). The exact date of the inspection is agreed upon with the employee, which means that the employer cannot arbitrarily set the date. Bearing in mind that remote work is generally carried out at the employee's place of residence, the requirement to agree on the date on which the inspection is to be carried out is intended to prevent an unexpected surprise visit which could cause disruption to the family life of the employee and his/her household members. The employee, on the other hand, may not deprive the employer of the possibility of carrying out the inspection by persistently not agreeing to it. Such behaviour, violating the employer's basic right, could give rise to the application of certain disciplinary measures provided for in the labour-law provisions (Kuba, 2014, para. 3(6); Wujczyk, 2012, para. 23).

If the inspection reveals deficiencies in compliance with rules and regulations on occupational health and safety of which the employee has been informed, or with procedures on the protection of information, including procedures on the protection of personal data, the employer may either set a deadline for rectifying the deficiencies or withdraw consent for remote work (Article 67(28) § 3 of the Labour Code). Consent for remote work may be withdrawn as soon as the deficiencies are discovered, even if it was possible to remedy them within a certain period of time, or at a later date if the deficiencies are not remedied within the agreed period of time. Withdrawal of consent implies that the employee has to start work at a place and time set by the employer; in this case, no two-day notice period is stipulated. As a result, the employee may be obliged to start work immediately at the place designated by the employer. An employee who refuses to stop working remotely or who takes up traditional work in violation of the deadline set by the employer risks certain negative consequences under labour law, ranging from a disciplinary penalty to termination

of the employment relationship in exceptional situations, even under a disciplinary procedure.

The actions set out in Article 67(28) § 3 of the Labour Code, i.e. setting a time limit for the rectification of the identified deficiencies or revoking the consent for remote work, apply to employees who originally performed their employment duties in a traditional manner (at the employer's place of business) as well as those who switched to remote work during their employment. In the case of an employee who has been working remotely from the very beginning, a breach of the employee's duties entitles the employer to take action that may be taken in relation to employees in general: the employer may apply a disciplinary penalty or terminate the employment relationship. However, the employer cannot decide on a cessation of remote working on his/her own. A transition to the traditional way of performing work can take place by agreement between the parties or by way of a change notice (Article 42 of the Labour Code). Deficiencies identified in the course of inspections also entitle the employer to apply disciplinary measures covering all employees, i.e. imposing a disciplinary penalty or even terminating the employment relationship in specific situations.

## 2. The right to remuneration for the time of inspection

Against the background of the provisions on remote work, the question arises of whether the employee retains the right to remuneration for the time of inspection. According to Gładoch, 'the time of inspection should be treated as a time of not performing work, for which the employee is not entitled to remuneration, unless the employer adopts a different solution favourable to the employee' (Gładoch, 2023, p. 106). It is worth noting here that, in accordance with Article 128 § 1 of the Labour Code, working time is not only the time during which the employee actually performs the duties arising from the employment relationship, but also periods of non-performance of work during which he/she remains at the employer's disposal at the workplace or at any other place designated as the place of work. Being at the employer's disposal means the state of being physically present in the workplace or another place which the employer intends to designate for the performance of work. It is also important that the employee has a real opportunity to perform work and fulfil the employer's instructions, as well as that he/she demonstrates readiness in this respect, i.e. that he/she is willing to start work immediately. If, due to an inspection carried out directly at the place of work, the employee working remotely is unable to fulfil his/her duties, he/she remains at the disposal of the employer. As a result, the period of inspection should be classified as working time, for which the employee is entitled to appropriate remuneration (Sierocka, 2023, p. 65); this applies in particular to short-term inspections. According to Mądrala, in the case of longer visits caused

by deficiencies on the part of the employee, the right to remuneration may be disputed (Mądrala, 2023, pp. 113–114).

## 3. Methods of conducting oversight

The oversight of remote employees can be carried out through conventional means, namely through visits to the work site. In this manner, the employer primarily monitors workplace safety and hygiene. Performing work at a place chosen by the employee does not exclude the employer's responsibility for the state of health and safety at work (Article 207 of the Labour Code). The employer's obligations related to the protection of employees' life and health are reduced to a certain extent by waiving requirements which are impossible to implement in relation to remote work (Dzienisiuk, Skoczyński, & Zieliński et al., 2017). The necessity of ensuring safe and hygienic working conditions for remote workers entitles the employer to control the employee with regard to compliance with the health and safety rules and regulations in force at the given workplace.

Remote work performed by a designated employee may also be subjected to traditional forms of monitoring, the purpose of which is to determine whether the tasks entrusted to the remote worker are performed in a timely, reliable manner in accordance with the employer's rules and expectations. In the course of the inspection, the employer assesses the quality and efficiency of the remote work. The actions taken by the employer serve the purpose of considering whether the employee performs the employment contract diligently and scrupulously. Through direct oversight at the location of work, the employer may also observe the employee's adherence to requirements regarding safety and information protection, including procedures for safeguarding personal data. With regard to the latter, the essence of the inspection is to obtain information as to whether the employee who performs remote work complies in particular with the rules provided for in the Personal Data Protection Act of 10 May 2018 and in 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 95 Directive/46/EC (General Data Protection Regulation). The employer's actions also serve to protect company confidentiality.

In the era of the Fourth Industrial Revolution (Schwab 2018, p. 26 ff.; Stelina, 2023, p. 123), which is characterised by the unification of the real world of machines with the virtual world of the internet, information technology, and people (Wodnicka, 2021, pp. 50–51), the monitoring of work execution and adherence to principles regarding safety and information protection, including personal data, is increasingly conducted through automated monitoring and decision-making systems. Among ac-

tivities categorised as algorithmic management (Nowik, 2020, p. 269 ff.), artificial intelligence (AI) holds a fundamental significance.

Artificial intelligence is framed conceptually in various ways. For instance, John McCarthy coined the term as being 'the science and engineering of making intelligent machines' (McCarthy, 2007, p. 2). Elaine Rich characterises it as 'research aimed at creating computers with abilities where humans are currently superior' (Rich, 1984, p. 1). Some argue that artificial intelligence is the 'study of mental abilities through computational models' (Charniak & McDermott, 1985, p. 6). Defining artificial intelligence necessitates acknowledging that it goes beyond being a computer program with a decisive computational speed advantage over humans (Betlej, 2019, pp. 192–205). AI is characterised by (1) learning, understood as the ability to acquire relevant information and the principles of using it; (2) reasoning, the ability to apply acquired rules to achieve approximate or precise conclusions; and (3) iteration, the ability to modify processes based on newly acquired information (Gasparski, 2019, p. 255). As a result, AI activity is comparable to the functioning of the human brain (Kalisz, 2020, p. 159).

Artificial intelligence enables employers to monitor employees' productivity and efficiency. Through applied algorithms, employers have the ability to determine whether work is being carried out in a timely manner, in line with directives, and whether employees are effectively utilising their working hours (Nowik, 2020, p. 270). Therefore, the employee may be required to log in to the company's IT system at the start of work (which makes it possible to measure working time), to check his/her email at specified intervals (Mitrus, 2009, p. 167), and to provide periodic reports on the activities undertaken. Artificial intelligence swiftly analyses and processes various types of data and information provided by the employee (Eager et al., 2020, p. 15; Więckowska, 2022, p. 244 ff.). Based on the outcomes, the employer gauges the quality and quantity of the employee's work and their commitment to fulfilling professional duties, which is significant, for instance, in the context of their compensation. Modern technologies enable employers to conduct an objective, precise, and unbiased assessment of an employee's work, skills, and contribution, devoid of human emotions and prejudices (Otto, 2022, p. 147). Additionally, artificial intelligence also facilitates the evaluation of employees' creativity, their capabilities, and their aptitude for creative thinking and planning (Bąba, 2020, p. 17).

Artificial intelligence also poses distinct risks. For instance, it can steer employers towards making decisions that infringe upon employees' rights, which is often attributed to the malfunctioning of the AI system. Instances may arise where applied algorithms rely on erroneous or inadequate data, resulting in, for example, unequal treatment of workers. A noteworthy case is that of Amazon, which developed an artificial intelligence algorithm for recruitment purposes, aiming to identify the best candidates for employment. However, the use of inappropriate methods led to discrimination against women (Pfeifer-Chomiczewska, 2022, p. 63). Similar risks may

manifest for remote workers, with software errors or the application of algorithms based on improper parameters potentially leading to an inaccurate and unreliable assessment of their work. Employers should provide employees with the opportunity to challenge opinions and conclusions generated by AI; this should apply not only when the assessment of a remote worker is flawed but also when such an assessment is fundamentally correct. However, such practices remain in contradiction with social principles. Artificial intelligence lacks empathy and emotions; given this, evaluations of an employee's achievements, work outcomes, or behaviour based on algorithms may require adjustments due to the particular circumstances of each employee. Hence the final judgement should always rest with humans. A review within the employer's competence or as designated by them holds particular significance if AI reports serve as the basis for terminating an employment contract or applying any disciplinary measures to a remote worker. Additionally, it is crucial for employees to trust the actions taken by artificial intelligence. To foster this trust, employees should be informed about the parameters subject to analysis and the algorithms used by their employer.

The use of modern technologies also brings the risk of personal data and confidential corporate information being exposed or lost. This threat can be instigated by the malicious activities of malware, often developed with the integration of artificial intelligence; such programs exhibit the capability of dynamically altering their code, making them undetectable to antivirus programs or users until the moment of a deliberate attack (Adamczyk et al., 2019, p. 2003 ff.; Kalisz, 2020, p. 164). In light of the risk of fundamental rights violations acknowledged and protected by European Union law, particularly the privacy and dignity of employees, non-discrimination, and workers' rights, the Artificial Intelligence Act was enacted by the European Parliament and Council on 23 June 2023. This regulation establishes harmonised provisions concerning artificial intelligence and amends certain legislative acts of the Union. Negotiations with Member States are currently underway (Bujalski, 2023). According to the document, three categories of artificial intelligence are envisaged: unacceptable risk, high risk, and low or minimal risk. It is concluded that artificial intelligence systems used in the areas of employment, workforce management, and access to self-employment, in particular for the recruitment and selection of candidates, promotion and termination decisions, the assignment of tasks, monitoring, or evaluation of persons in contractual employment relationships, should be classified as high risk, as these systems may significantly affect the future job prospects and livelihoods of these persons (recital 36).

According to the adopted document, high-risk artificial intelligence systems must comply with certain standards that relate to data and its management, documentation and logging of events, provision of information to users, human oversight, reliability, accuracy, and security. In particular, such systems are required to provide a certain degree of transparency; users should be able to interpret the results

of the system and use them accordingly (recital 47). It is further stipulated that high-risk artificial intelligence systems should be designed and developed in such a way that individuals may supervise their operation (recital 48). The regulation adopted by the European Parliament is the first AI document in the world, therefore it is impossible to assess how effective its provisions will prove to be in practice.

## 4. Monitoring of business email

An instrument used to control an employee performing remote work is the monitoring of company email, which may be conducted through the utilisation of artificial intelligence. Thanks to cutting-edge technologies, the employer can monitor both the quantity and the content of messages incoming to and outgoing from the employee. In accordance with Article 22(3) § 1 of the Labour Code, the employer is entitled to utilise monitoring of official email provided it is necessary to ensure work organisation, enabling the full utilisation of working time and the proper use of tools provided to the employee. The condition of necessity is fulfilled when the employer demonstrates that both objectives indicated in the provision can only be realised through the monitoring of business email (Kuba, 2019, p. 31; Łapiński, 2020, pp. 52–53). Monitoring of business email does not entitle the employer to violate the secrecy of correspondence and other personal rights of the employee. Thus the legislation recognises the primacy of the rights guaranteed by the Polish Constitution (Article 49) over the employer's interest. Consequently, even if the employer prohibits the use of business email for private purposes, he/she does not have the right to read the private correspondence of an employee who has not complied with this prohibition.

The employee should be informed of the monitoring of his/her email two weeks before it is initiated, in a manner customary for the employer concerned. It is possible to send a suitable letter to each employee, to place a relevant notice on the noticeboard, and/or to provide information in the form of an email. In the case of newly hired employees, information on the implementation of email monitoring should be provided in writing before the employee is allowed to work. In the notice, the employer must indicate the purpose of the monitoring and the manner in which it is to be carried out, as well as its scope. With regard to the latter, it is necessary to specify the level of detail of the monitoring; the employer should clarify whether the object of the monitoring will be only basic information on the senders and addressees of messages, the dates of sending and receiving the correspondence and its topics, and/or whether the content of individual messages will also be reviewed. As there are no reservations in the Labour Code as to the tools the employer may use for this purpose, various organisational and technical solutions, including those using artificial intelligence, are admissible. Information related to the monitoring of business email is laid down in collective agreements, work regulations, or in a notice

if the employer is not covered by a collective agreement or is not obliged to lay down work regulations. The employer is obligated to visibly and legibly label the monitored email boxes.

The provisions of the Polish Labour Code are in line with the guidelines of the European Court of Human Rights. In accordance with the views of legal academics and commentators, as well as an established line of judicial decisions of the Court, it is emphasised that national authorities should ensure that the introduction of measures by an employer to monitor correspondence and other communications, regardless of the extent and duration of such measures, is accompanied by adequate and sufficient safeguards against abuse. To this end, it is necessary to notify an employee of the monitoring of his/her correspondence and other communications. This kind of notification should be clear about the nature of the monitoring and should be done in advance, with the employee being warned about the extent of the employer's monitoring and the degree of interference with privacy; moreover, the employer should provide legitimate reasons justifying the monitoring of the messages and access to their actual content (Judgment of the European Court of Human Rights 2017).

## Conclusion

The performance, in whole or in part, of work at a location chosen by the employee does not deprive the employer of managerial powers. In particular, the employer is provided with the right to inspect work performed remotely. Among the methods of controlling the employee, control carried out with the use of modern technologies, especially artificial intelligence, is a particularly convenient instrument. By reducing the time needed for data processing and analysis, algorithmic management makes it possible for the employer to make quick and, in most situations, accurate decisions. Inspections with the use of modern technology are, as a rule, also convenient for the employee; unlike a traditional inspection, which involves observing the work directly at the place where it is carried out, an algorithmic inspection interferes little with the employee's family life, or not at all, and, moreover, provides greater choice as to where to fulfil the obligations arising from the employment relationship. The employer may, for example, accept the performance of work abroad. However, the potential threats associated with the implementation of artificial intelligence must not be overlooked. Erroneous algorithms can lead to an improper assessment of an employee's performance and a violation of their rights. Furthermore, there is a danger of leaks of sensitive data and confidential corporate information. Modern technologies employed for monitoring remote employees are susceptible to attacks by malicious software, causing the loss of corporate data.

**REFERENCES**

Act on Amending the Labour Code of 1 December 2022 and Certain Other Acts (Journal of Laws of 2023, item 240).

Act on Specific Solutions Related to Preventing, Counteracting, and Combating COVID-19, Other Infectious Diseases, and Emergency Situations Caused by Them of 2 March 2020 (consolidated text, Journal of Laws of 2023, item 1327).

Adamczyk, M., Betlej, A., Gondek, J., & Ohotina, A. (2019). Technology and sustainable development: Towards the future? *Entrepreneurship and Sustainable Issues*, *6*(4). 2003.

Bąba, M. (2020). Algorytmy – nowy wymiar nadzoru i kontroli nad świadczącym pracę. *Praca i Zabezpieczenie Społeczne*, *3*. p. 17.

Betlej, A. (2019). *Społeczeństwo sieciowe – potencjały zmian i ambiwalentne efekty*. Wydawnictwo KUL.

Bujalski, R. (2023). *Akt o sztucznej inteligencji*. LEX/el.

Charniak, E. & McDermott, D. (1985). *Introduction to artificial intelligence*. Addison Wesley Publishing Company, p. 6.

Dzienisiuk, D., Skoczyński, J., & Zieliński, T. (2017). Komentarz do art. 67(17). In L. Florek (Ed.), *Kodeks pracy. Komentarz*, Lex.

Eager, J., Whittle, M., Smit. J., Cacciaguerra, G., & Lale-Demoz, E. (2020). *Opportunities of artificial intelligence*. European Parliament, Policy Department for Economic, Scientific and Quality of Life Policies. https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652713/IPOL_STU(2020)652713_EN.pdf

Gasparski, W. W. (2019). AI przedsiębiorczość: sztuczna inteligencja jako wyzwanie dla prakseologii i etyki biznesu. *Prakseologia*, *161*. p. 255

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 (O. J. EU L 2016, No. 119).

Gładoch, M. (2023). *Praca zdalna. Kontrola trzeźwości. Nowelizacja Kodeksu pracy, komentarz. Linia orzecznicza,* C.H.Beck, p. 106.

Judgment of the European Court of Human Rights of 5 September 2017 on the case of *Bărbulescu v. Romania*, application no. 61496/08. https://etpcz.ms.gov.pl/detailsetpc/monitoring$0020prawo$0020do$0020prywatno$015bci/990000000000001_I_ETPC_061496_2008_Wy_2017–09-05_001

Judgment of the Supreme Court of 24 June 2015,on the case of II PK 189/14, Lex no. 1764808

Kalisz, M. (2020). Sztuczna inteligencja – osiągnięcia, zagrożenia, perspektywy. *Transformacje*, *1*(2). pp. 159, 164.

Kuba, M. (2014). *Prawne formy kontroli pracownika w miejscu pracy*. Lex, para 3(6)

Kuba, M. (2019). Monitoring poczty elektronicznej pracownika – refleksje na tle nowych regulacji prawnych. *Praca i Zabezpieczenie Społeczne*, *11*. p. 31

Łapiński, K. (2020). Wybrane aspekty dotyczące stosowania monitoringu w miejscu pracy. *Radca Prawny. Zeszyty Naukowe*, *1*(22). pp. 52–53.

Mądrala M. (2023), Praca zdalna. Komentarz do nowelizacji Kodeksu pracy. Wzory, Wolters Kluwer, pp. 113–114.

McCarthy, J. (2007). *What is artificial intelligence?* Stanford University. https://www-formal.stanford.edu/jmc/whatisai.pdf

Mitrus, L. (2009). Podporządkowanie pracownika zatrudnionego w formie telepracy. In Z. Góral (Ed.), *Z zagadnień współczesnego prawa pracy. Księga jubileuszowa Profesora Henryka*, Wolters Kluwer, p. 162.

Nowik, P. (2020). Specyfika pracy na globalnych platformach internetowych w świetle zarządzania algorytmicznego. *Studia Prawnicze KUL*, *8*(81). pp. 269–270

Order of the Supreme Court of 6 May 2020, on the case of I PK 60/19, Lex no. 320792

Otto, M. (2022). Dyskryminacja algorytmiczna w zatrudnieniu. Zarys problem. *Studia z Zakresu Prawa Pracy i Polityki Społecznej*, *2*(29), p. 147.

Personal Data Protection Act of 10 May 2018 (Dz. U. 2019, item 1781).

Pfeifer-Chomiczewska, K. (2022). Artificial intelligence and contractual liability under Polish law: Selected issues. *Studia Prawno-Ekonomaczne*, *124*, p. 163.

Rich, E. (1984). *Artificial intelligence*. McGraw-Hill, p. 1.

Schwab, K. (2018). *Czwarta rewolucja przemysłowa*. Wydawnictwo Studia EMKA, pp. 26.

Sierocka, I. (2023). Komentarz do art. 67(28) In D. Książek, M. Kurzynoga, I. Sierocka, K. Bartosiak, & Ł. Łaguna (Eds.), *Praca zdalna. Praktyczny komentarz z przykładami*, Infor, p. 65.

Sobczyk, A. (2023). Komentarz do art 67(28) In A. Sobczyk (Ed.), *Kodeks pracy. Komentarz,* Legalis, para. 2.

Stelina, J. (2022). Czwarta rewolucja przemysłowa a prawo pracy. In K. Rączka, B. Godlewska-Bujok, E. Maniewska, W. Ostaszewski, M. Raczkowski, & A. Ziętek-Capiga (Eds.), *Między ideowością a pragmatyzmem. Księga jubileuszowa dedykowana Profesor Małgorzacie Gersdorf*. Wolters Kluwer. p. 123.

Więckowska, M. (2022). Artificial inteligence, machine learning, deep learning, etyka I rodo – jak to wszystko połączyć? In B. Fischer, A. Pązik, & M. Świerczyński (Eds.), *Prawo sztucznej inteligencji i nowych technologii* (p. 244). Wolters Kluwer.

Wodnicka, M. (2021). Wpływ czwartej rewolucji przemysłowej na innowacyjność usług. *Optimum: Economic Studies*, *3*(105). pp. 50–51.

Wujczyk, M. (2012). *Prawo pracownika do ochrony prywatności*. Lex, para 23.