Acta Iuris Stetinensis

2020, No. 3 (Vol. 31), 79–94
ISSN: 2083-4373 e-ISSN: 2545-3181
DOI: 10.18276/ais.2020.31-05

Krystian Ryś
MA
University of Opole, Poland
Faculty of Law and Administration
e-mail: krys@uni.opole.pl
ORCID ID: 0000-0002-9635-0720

Internet of Things and biometric data versus employee privacy in the Polish case

Abstract

The Internet of Things is a modern technology that affects every area of human life, including employment relationships. IoT enables the processing of specific personal data categories, including biometric data, and entails the risk of employers interfering with employee privacy. Due to the use of intelligent solutions, the issue of employee privacy, which is, in principle, a personal right subject to protection, becomes significant. The relationship between an employee and an employer includes two subjects of legal protection, the meeting of which may lead to internal contradiction. There is the employee's dignity and privacy, on the one hand, and protection of reasonable interests of an employer, on the other. A definition of the concept of the Internet of Things and its applications was introduced. Moreover, the author proposed setting a specific legal framework for this and discussed the issue of biometric data. It was also shown how far IoT solutions, which make it possible to analyse and describe the personality of an individual, may interfere with the information autonomy of a person. As a consequence, the employer's interference with employee privacy cannot be unrestricted, because it should be limited by purpose and lawfulness. This is the purpose of the current legislation.

Keywords: Internet of Things, biometric data, employee privacy

Introduction

The purpose of this study is to outline the subject matter of utilisation of IoT technology in employment relations and its consequences related to the employees' situation in the process of work performance. An analysis of various areas of IoT applications and the resulting possibilities allows for the assumption that IoT permits far-reaching interference in the employees' private sphere, and thus it may affect (or even violate) their fundamental rights. Of course, in this case, there is a visible clash between the rights and interests of both parties to the employment relationship. Taking into account the fact that IoT allows for autonomous collection and processing of specific types of personal data, namely biometric data, it appears necessary to include IoT in a specific legal framework.

During the performance of their work, employees generate vast amounts of data around them. This data can be received by smart devices. In this way, the employer can obtain extremely sensitive information allowing for the identification of employees, assessment of their suitability for work and to gain knowledge about their internal reactions, e.g. stress levels and behavioural data. The reason why this issue is vital is that the real-time transfer of this data takes place entirely beyond the employees' conscious control. The possibilities of interfering with the employees' information autonomy offered by IoT may give rise to concerns from the perspective of both legal protection and ethical assessment.

The main research objective is to determine whether the current law sufficiently regulates the use of IoT in employment relations, and in particular, whether it provides a sufficient level of employee privacy protection. On that account, the aspects of desirability, adequacy and legality of data processing remain extremely important.

This is important, because it is assumed that IoT will lead to a perceptibly greater revolution than the Internet or mobile communications.[1] Due to the use of intelligent solutions, the issue of employee privacy, which is, in principle, a personal right subject to protection, becomes significant. The right is held by every natural person, and therefore an employee as well. The relationship between an employee and an employer includes two subjects of legal protection, the meeting of which may lead to an internal contradiction. There is an employee's dignity and privacy, on the one hand, and the protection of the reasonable material and non-material interests of

1 Kwiatkowska, E.M., *Rozwój Internetu rzeczy – szanse i zagrożenia*, "Internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2014, No. 8, p. 60.

an employer, on the other.[2] This subject is important, because IoT-based solutions are increasingly becoming an integral part of a job and can change the situation of employees.

The concept of the Internet of Things

The concept refers to the transfer of information between objects or between objects and people.[3] The Internet serves as a communication platform used for the transmission of data with the use of a computer network. It makes it possible to collect, process and exchange data by objects without human interference, which is referred to as M2M.[4] The concept of IoT appeared when the number of devices connected to the web exceeded the number of people on Earth.[5] The term was first used by K. Ashton in the title of a presentation for Procter & Gamble in 1999.[6]

Kevin Ashton[7] observed that the problem of computerisation and data exchange on the web lies in the total dependence on the human factor, as materials and information have been collected and created by people. Human participation in the process of entering data onto the web involves certain drawbacks. The main problem is that there is limited time available to an individual. Moreover, his or her work bears the risk of negligence and inattentiveness in the process of its creation. This proves that people are neither the best elements of the system nor optimum subjects of the mechanism of processing data with the use of the web. Technological development should therefore be oriented towards a broader use of the possibilities offered by computers. It is necessary to equip them with the ability to independently receive stimuli from the outer world and thus gather and process external information. To

2 Knade, A., *Czy pracodawca ma prawo inwigilować pracownika? Prawo do prywatności pracownika a interesy pracodawcy*, in: Chrzczonowicz, P. et al. (eds.), *Społeczeństwo inwigilowane w państwie prawa*. Toruń 2003, p. 59.

3 It should be clarified that the Internet is only a transfer point, but its substance and aim is to collect as much as data as possible.

4 Machine to Machine.

5 Such a position was taken by Cisco Internet Business Solutions Group (Cisco IBSG) – in 2000, the world population was ca. 6 billion people, and only 500 million devices were connected to the web. The number of smart devices exceeded the world population for the first time at the turn of 2008 and 2009. In 2010, we faced a dynamic growth in the number of smartphones and tablets, as a result of which the number of devices included in the network increased to 12.5 billion. – in: Kwiatkowska, E.M., op. cit., p. 61.

6 Maj, I., *Internet rzeczy i zagrożenia z nim związane*, "Bezpieczeństwo. Teoria i Praktyka" 2015, No. 3, p. 51.

7 Ashton, K., *That "Internet of things" Thing*, 22.06.2009, RFID Journal, http://www.itrco.jp/libraries/RFIDjournal-That%20Internet%20of%20Things%20Thing.pdf (accessed 17.09.2020).

put it in simple terms, K. Ashton argued that modern data transfer should be based on making it possible for computers to "see, hear and smell the world". This could be possible with the use of various kinds of sensors and identification systems.[8]

IoT is a term directly related to the technological revolution in IT and telecommunications,[9] which affects both business organisations and the public sector, as well as the private lives of community members. The pace at which this phenomenon is developing is illustrated by the dynamics of searching the phrase "*Internet of Things*" in web browsers, which has shown huge growth of interest in recent years.[10]

It is difficult to develop a single, detailed definition of the concept of IoT. It may describe a situation in which the number of smart products grows and points out new possibilities provided by connected devices.[11] Others depict it as sensors and actuators placed in machines and other physical objects for the purposes of data collection, remote activity monitoring, decision-making and, most of all, applying optimisation processes in all areas of manufacture, including infrastructure and healthcare.[12] According to the author, IoT is more than just devices and sensors; it is a kind of autonomous data exchange environment.

To put it in simple terms, IoT may therefore be defined as an ecosystem within which objects equipped with appropriate sensors may communicate with computers. One should note that such an interaction may occur both with and without human participation.[13]

Literature indicates that IoT is based on three fundamental pillars referring to the features of smart objects. *Smart* objects may identify themselves, ensure communication and cooperate. In other words, the concept of the Internet of Things

8 Kwiatkowska, E.M., op. cit., p. 61.

9 Changes in the area of data technology and transmission that are related to the development of the Internet of Things are often referred to as the fourth industrial revolution. See Rot, A. and Blaicke, A.B., *Zagrożenia wynikające z implementacji koncepcji Internetu rzeczy w wybranych obszarach zastosowań*, "Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2017, No. 341. p. 317.

10 Senkus, P. et al., *Internet of Things: przeszłość – teraźniejszość – przyszłość*, "Zeszyty Naukowe Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach. Seria: Administracja i Zarządzanie" 2014, No. 103, pp. 164-165.

11 Heppelmann, J. and Porter, M., *How smart, connected products are transforming competition*, "Harvard Business Review" 2014, pp. 64-88, as cited in: Wielki, J., *Internet Rzeczy i jego wpływ na modele biznesowe współczesnych organizacji gospodarczych*, "Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2016, No. 281, p. 209.

12 Dobbs, R. et al., *No ordinary disruption*, New York 2015, p. 38, as cited in: ibidem, p. 209.

13 Malucha, M., *Internet rzeczy – kontekst technologiczny i obszary zastosowań*, "Studia i Prace WNEiZ US" 2018, No. 54, p. 55.

covers objects working with the use of various sensors and mechanisms based on the following assumptions: everything can introduce itself; everything can communicate; and everything can influence each other.[14]

IoT represents a global infrastructure of an information society, the purpose of which is to combine material and virtual things. The difference between these categories comes down to the environment in which they exist and operate. However, both material and virtual things can be identified and included in the web.[15]

Looking at it from the point of view of employment, one can conclude that the organisation of a working environment based on the application of IoT is beneficial in various respects, which include improvement of productivity, acceleration of the innovative cycle in the organisation, expansion of the product and service range, as well as reduction of costs and increase of profitability.[16] It seems that IoT will completely change the interactions between employers and employees, as the employer is given the opportunity to better control and verify a person's suitability for a particular job. In the author's opinion, no other technology has such an impact on the situation of workers, especially with regard to their sensitive data and information autonomy.

The interest of business organisations and enterprises in IoT technology is determined by social and economic market changes. One can undoubtedly assume that the environment in which companies operate is currently subject to rapid changes, as the requirements of customers and employees are growing, with market competition being more and more fierce. It is therefore necessary to undertake steps to increase the effectiveness. At the same time, the management needs fast and continuous access to reliable and comprehensive information concerning the internal situation regarding company operations. IoT can be perceived as a specific technological revolution in this respect.[17]

IoT application areas

IoT may have numerous applications and impacts on employment relations. In the context of the discussed issues, it is important for IoT to make it possible to improve generally defined work performance processes, which should translate into a significant increase of production effectiveness, cost optimisation and employee

14 Krysiński, M., *Internet rzeczy – innowacyjne narzędzie dla firm*, "Ekonomiczne Problemy Usług" 2016, No. 122, p. 280.

15 Kwiatkowska, E.M., op. cit., p. 62.

16 Wielki, J., op. cit., p. 210.

17 Krysiński, M., op. cit., p. 281.

efficiency. IoT allows for an optimal organisation of the work environment, taking into account the data collected in the course of work, the predisposition of employees and their reactions. IoT enables unlimited analysis of the work process, both in relation to the equipment used and the employees themselves.

The scope of IoT makes it possible to analyse it in terms of employment relationships and the situation of people performing work. Its development is favoured by the popularisation of the *System on a Chip* (SOC). This solution consists in the placement of a processor, RAM, radio communication systems and analogue systems in a single integrated circuit. As a consequence, a virtually complete actuator of a small size and high functionality is obtained.[18] Such technological development makes it possible to equip employees with devices having sensors gathering and processing specific data, of which biometric data is the most significant. The question of the scope and purpose of gathering such data remains open. A further step will involve microchipping employees by placing special devices under their skin.

IoT technology may be applied in every dimension of the working environment. The components of IoT technology may serve different purposes and, most of all, be of different sizes. Solutions available on the market include simple interactive devices, such as microprocessors (beacons) and sensors, as well as complex devices performing complicated functions: industrial robots, autonomous transport devices, smart measuring devices or mobile devices. Integrated circuits are often assembled with the use of hi-tech electronics including, for example, flexible PCBs (printed circuit boards).[19] As a result of the progress in this area, IoT solutions may be getting closer to the employee. They can be found not only in production and office devices, as well as buildings, but also in clothes, watches and ID cards.

Legal aspects of using the Internet of Things

The social and economic significance of IoT makes it necessary to specify the legal framework for this phenomenon in the future. In my opinion, it will be very difficult to regulate all aspects of this technology, mainly due to the abundance of applications and areas of use, which will probably continuously evolve and progress. However, using IoT is linked to the issue of the security of collecting data, its processing and the protection of privacy.

18 *Raport Grupy Roboczej ds. Internetu rzeczy przy Ministrze Cyfryzacji, IoT w polskiej gospodarce,* Ministerstwo Cyfryzacji 2019, https://www.gov.pl/attachment/82ad18f8-2ac1-4433-a1ea-f887b5-22e46b, p. 10 (accessed 04.04.2020).

19 Ibidem, pp. 9 and 12.

The above issue is crucial both for employees and employers. One can assume without any major reservations that the use of smart devices involves the risk of data theft and enables deep intrusion into privacy. Given the fact that we currently face hacker attacks on computers, tablets and smartphones connected to a network, such activities will obviously be possible with respect to all devices based on the IoT concept. Due to the wide range of the potential application of this technology, the problem of protection against such attacks and ensuring data security is particularly important. This requires special attention from the legislator, as the Internet of Things makes it possible to use biometric data, including behavioural data. Appropriate legal norms should provide some kind of support for entities using IoT to take relevant steps. Legal regulations should be adjusted to the new reality before IoT becomes widespread in everyday life. In the author's opinion, it is currently possible to predict certain directions of progress in the use of IoT in labour relations, which should be borne in mind by the legislator. However, it should be noted that, due to the pace at which modern technologies develop, the legislator may fall behind when enacting relevant regulations. The range of legal provisions is also debatable, since the creation of domestic law can hardly be regarded as sufficient in the face of such a global phenomenon, because IoT devices are solutions that appear everywhere and affect the work situation regardless of the location.

Potential actions are necessary, as the functioning of IoT is inextricably related to data management. A system that consists of objects permanently connected to the web and constantly exchanging information leads to a critical amount of generated data and the number of processes used for its processing. It is said that IoT involves the creation of more than 2.5 trillion bytes per day, most of which have come into existence in recent years. It is not data collection itself that poses the greatest challenge, but its processing and analysis. In other words, Big Data will require the use of technology enabling the effective processing of unstructured data.[20]

The widespread use of the Internet of Things requires trust in the new technologies and a guarantee to individuals that the information generated on the web will not be used inappropriately. There are no doubts as to the fact that the respect for privacy and data protection are fundamental human rights in the European Union.

As mentioned above, the ability to connect physical objects and establish communication between them is the essence of the Internet of Things. This technology makes it possible for devices to act or react autonomously. It is the exclusion of the human factor from active data processing that makes it so unique. There is currently no law that would regulate IoT in general. Nevertheless, there are vertical regulations that appear in the world concerning the selected areas in which it

20 Kwiatkowska, E.M., op. cit., p. 69.

occurs, e.g. the USA.[21] However, it seems that a comprehensive regulation covering at least cybersecurity, personal data, liability for damages and intellectual property would be advisable. Ethical issues and delimitation of boundaries within which IoT devices could be installed could be important. An example would be a ban on the use of subcutaneous chips as they involve interference with human physical integrity and lack of control of whether the chips also operate outside working hours.

IoT technology, due to its global character and generally unlimited range, as well as the exclusion of the human factor from the process of data analysis and collection, makes it necessary to look at biometric data processing in a different way. Its scope is expanding as a result of technological progress. After all, IoT devices allow all types of data to be collected and processed autonomously and independently of human will. From the point of view of the issue, the sensitive data of the employees – retina, shape of the auricle or motor and reactions – is important. IoT and the connection of all kinds of devices which transmit any data onto the web is opening new fields for computational social research. Big Data[22] can make it possible to discover interesting relationships and acquire knowledge about employees concerning highly intimate matters.[23]

It is also noteworthy that physical objects included in the ecosystem of IoT enable acquisition of knowledge in a way that is virtually impossible to be controlled by the entity providing such information, especially behavioural data, as well as unlimited profiling of individuals. The scope of potential interference with an employee's private life is too far reaching, whereas the collected data may be transferred anytime, anywhere.[24] This process may be difficult to control; therefore, it requires special attention from legislators. In labour relations, IoT requires special attention, because its essence presupposes the inequality of the parties to the relationship, and as a consequence, some enhanced protection is required by employees.

21 The American California Consumer Privacy Act of 2018 (1798.100 – 1798.199, *Title 1.81.5 added by Stats. 2018, Ch. 55, Sec. 3.* Civil Code), the so-called California IoT Act, is an example of such legislation.

22 The term means large, variable and diverse datasets that are of high value.

23 Jemielniak, D., *Socjologia internetu*, Warszawa 2019, p. 45.

24 Due to the extensive possibilities of identifying individuals and collecting data that is not related to work.

Biometric data

The concept of biometric data is defined in Regulation (EC) 2016/679 of the European Parliament and of the Council[25] (hereinafter GDPR). Pursuant to Article 4(14) of the GDPR, personal data are resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual, which allows or confirms the unique identification of that person, such as facial images or fingerprint data.

The development of IoT leads to the progress of biometric methods that enable the use of the unique physical, physiological or behavioural characteristics of an individual for the purposes of identification and identity verification. They include fingerprints, palm, ear or face geometry, the iris, the fundus, the palm or the blood vessel arrangement of the palm or finger, voice, deportment or even the way one hits the keyboard.[26]

The EU legislator decided to include biometric data in the category of special personal data (Article 9(1) of the GDPR). It does not matter whether new, e.g. health-related, information is generated as a result of its processing. The point is that technologies involving iris or fundus scanning may make health problems to surface.[27]

Biometric data makes it possible to identify a person or explicitly confirm their identity. It is particularly valuable due to its uniqueness. As a consequence, its collection and processing are specific, as it involves greater interference with the information independence of an individual, which is related to the physical or physiological structure or physical characteristics of an individual.[28] What is more, it cannot exist independently, as it depends on various carriers – saliva, blood, fundus image or fingerprints.[29]

However, it should be pointed out that according to the definition of biometric data introduced by the EU legislator, it includes only data that enables the

25 Regulation 2016/679 of the European Parliament and of the Council (EU) 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, OJ L 119, 4.5.2016, pp. 1–88.

26 Pyka, A., *Przetwarzanie danych biometrycznych. Aspekty prawne*, "Studia Prawa Publicznego" 2018, No. 3, p. 133.

27 Ibidem, p. 138.

28 Ibidem, p. 138.

29 Bąba, M., *Próba wyznaczenia zakresu pojęcia danych biometrycznych*, "Prawo Mediów Elektronicznych" 2016, No. 2, p. 26.

identification and verification of a given person. Not every biometric method allows one to achieve such a goal with the use of specific carriers.

In the context of the discussed issues, it can be noted that the aspect of collecting and processing special categories of data started to appear in the rulings together with the spread of modern technologies. A view was expressed that digitally processed information on characteristic points of employees' fingerprints is their personal data. It should be mentioned that the collection and gathering, i.e. processing, of employees' data, such as fingerprints or the iris pattern, is generally allowed, but it must be done in compliance with the provisions of the Polish data protection act.[30] The above view should obviously be extended with the provisions of the GDPR and the Polish labour code[31] (hereinafter "LC"). These pieces of legislation now complement the protection of personal data in labour relations.

The Internet of Things versus employee privacy

The processing of data is the essence of IoT. In labour relations, it is important that this process is registered by relevant algorithms, which work continuously and, to some extent, arrange the collected data strings by making sense out of them, which, as a consequence, leads to the creation of information about an employee. It enables the development of knowledge that makes it possible to identify and describe one's personality, as the Internet of Things offers limitless possibilities for analysis.[32] That is why it is possible to study the behaviour and characteristics of individuals, including sensitive data, thoroughly, based on automatic algorithms.

According to M. Bąba, IoT involves elimination of separateness of individuals and unlimited access to them through the observation of spontaneously revealed personal states. Privacy may be examined from different angles, as it is an area in which individuals attach specific value to a certain range of information about themselves. That is why they tend to protect and share it. This kind of data and information remains private irrespective of its disclosure. This is an explicit expression of the information autonomy of an individual.[33]

30 Judgement of the Voivodeship Administrative Court in Warszawa of 27 November 2008, II SA/Wa 903/08, LEX No. 521934.

31 Act of 26 June 1974 – Labour Code, Dz.U. (Journal of Laws) of 1974 No. 24 item 141, as amended.

32 Bąba, M., *Refleksje wokół prywatności i autonomii informacyjnej w świecie Internetu (wszech) rzeczy*, "Zeszyty Naukowe Wydziału Informatycznych Technik Zarządzania Wyższej Szkoły Informatyki Stosowanej i Zarządzania pod Auspicjami Polskiej Akademii Nauk. Współczesne Problemy Zarządzania" 2018, No. 2, p. 34.

33 Ibidem, p. 34.

In this context, there is no reason for depriving employees of their privacy and the possibility to freely dispose of it. People spontaneously manifest their behaviours and personal states in the process of work. The conclusion that the work performance process may merge with an employee's private life is therefore legitimate. The process of biometric data processing is related to the possibility of far-reaching encroachment into an employee's private sphere. As a consequence, we are facing interference with the information autonomy of an individual. Such a problem may also appear in the relationship between an employer and an employee. For obvious reasons, in this case, the economic and organisational advantage of an employer can be observed. In this context, the principle of data processing legalism is particularly important. This is expressed in Article 5(1) of the GDPR, which sets out that it must be processed lawfully.

The EU legislator assumed that biometric data processing involves the necessity of the controller proving that there are any of the legal bases for data processing mentioned in Article 9(2) of the GDPR. In principle, it is not allowed to process personal data that can be defined as sensitive data, including data revealing racial or ethnic origin, political opinion, religion or beliefs or trade union membership, as well as genetic, biometric data for the purposes of identifying a natural person or data concerning the health or sexual orientation of an individual.

Legal bases for the processing of biometric data are particularly important. Circumstances precluding the general ban on using this kind of data are set out in Article 9(2). The express consent of the data subject is one of the conditions for the lawfulness of data processing. It is hard to imagine that consent for the processing of biometric data in a relationship between an employee and an employer could be given upon the initiative of the former. Such a position is justified by the nature of the relationship between parties to an employment relationship and the specific dependence of an employee on an employer. In the employment relationship, the subordination of the employees to the employer is a basic characteristic, so the possibility of expressing one's will completely freely may be doubtful. In such a situation, the employee's consent will, in a sense, be based on an organisational and economic compulsion. Such a rule is also provided for in the LC. Without discussing the nature of such consent, one can conclude that the currently applicable Article 22^{1b} of the LC regulates this matter. The said provision expressly refers to Article 9(1) of the GDPR; therefore, it also applies to biometric data processing by an employer. This is related to both the employee and the employer. However, pursuant to Article 22^{1b}(1) of the LC, its lawfulness depends on consent, though the legislator does not specify that it should be expressed. It is nevertheless important that such data must be provided on the initiative of the person being an employer or a candidate for employment. Moreover, as provided by Article 22^{1b}(2), biometric

data processing is also permissible in a situation where it has to be provided due to the control of access to particularly important information, the disclosure of which may cause damage to the employer, or access to rooms that require special protection.

The opinion of the District Court in Giżycko stating that "pursuant to the new wording of Article 22^{1b} of the LC, so-called special category data may be processed on the basis of an employee's consent only if it is provided upon the initiative of an employee. As a consequence, the legislator precludes the application of consent if an employee is not the initiator of the provision of information on his sobriety" seems reasonable.[34] The above-mentioned opinion should be interpreted as referring not only to an employee's sobriety, but to all kinds of data, in particular biometric (including behavioural) data under Article 22^{1b} of the LB. It seems that such a position reflects the main assumptions made concerning personal data protection in the Polish legal system.

Given the above, the question arises as to whether the currently applicable GDPR and LC regulations are sufficient and relevant for the current extent of technological progress in the field of biometric data. It is hard to provide an explicit answer, as the issue involves the interests of both, employees and employers. Moreover, as provided by Article 22^{1b}(2), biometric data processing is permissible if it has to be provided due to the control of access to particularly important information, the disclosure of which may cause damage to the employer, or access to rooms that require special protection. These circumstances rightly make the use of such data lawful. Nevertheless, as far as the employer's interests are concerned, it does not cover issues related to the streamlining of production processes or increasing effectiveness. Article 9(2)(b) of the GDPR precludes a general ban on using biometric data if it is not necessary for the fulfilment of duties and the exercise of special rights by a data controller or a data subject in the area of labour law, social security and social protection, provided that it is allowed under EU law or the law of a member state or a collective agreement under the law of a member state providing for the appropriate protection of the fundamental rights and interests of a data subject.

In the context of the cited provision of the GDPR, the specific flexibility of the bases for the lawfulness of biometric data processing is noteworthy. Its use may be permitted under EU law and the domestic law of a member state or even under a collective agreement made under the law of a member state.

According to legal academics, "legal provisions under which a collective agreement may be established must provide for appropriate protection of the fundamental rights and interests of the data subject. However, the question of whether such

34 Judgement of the District Court in Giżycko of 10 September 2019, IV P 49/19, LEX No. 2747635.

a solution, despite providing greater flexibility, will not lower the level of protection of the personal data subject (employees in particular) raises concerns. However, there are generally no doubts as to the fact that the processing of sensitive data must be allowed if it is necessary for the purposes of employment or social security".[35]

The discussed regulation authorises the creation of grounds for such activities under relevant provisions, including secondary legislation passed by virtue of a delegation of legislative powers or under collective agreements. Biometric data processing in employment relationships cannot be associated exclusively with actions having negative consequences for employees. There should be no obstacles for the parties to reach a collective agreement to agree upon the given manner and scope of using sensitive data, in particular social and economic relationships, provided that the dominant party (the employer) is responsible for the proper protection of and respect for employees' fundamental rights. This is important due to the fact that IoT is much more than just a tendency in recent years. It has the potential to revolutionise numerous areas of life, including employee relationships.

The regulation on the issue of biometric data protection at the EU level is undoubtedly a positive thing. The introduction of Article 22^{1b} of the LC, which could be extended in line with the provisions of Article 9(2)(b) of the GDPR, is also noteworthy. IoT is a constantly developing technology that finds new applications in more and more areas. As a consequence, it may be necessary to introduce legal changes corresponding to emerging needs. According to the author, it will be necessary to regulate the use of IoT comprehensively in the long term. It should be added that distinguishing between a data controller and a data processor already poses a problem.[36] IoT undoubtedly increases the possibilities for employers to collect and process employees' personal data. Therefore, the legislator should introduce into labour law solutions aimed at a certain limit on the actions taken by the employer. Nevertheless, this is difficult, because this field is – in a certain sense – very hectic and rapidly changing.

One should also remember that IoT involves totally automated data processing, including profiling. The consequences may be twofold. On the one hand, they may offer more individual solutions for employees, but on the other hand, they can lead to unfair discrimination. Some restrictions are necessary even though the establishment of grounds for biometric data protection under collective agreements is authorised. The purpose and appropriateness of the manner in which biometric

35 Kuba, M., *Komentarz do art. 9*, in: Bielak-Jomaa, E. and Lubasz, D. (eds.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, LEX 2018.

36 This issue has been discussed by Deloitte in: *Internet Rzeczy, ochrona prywatności a bezpieczeństwo danych,* https://www2.deloitte.com/pl/pl/pages/doradztwo-prawne/articles/Internet-Rzeczy-ochrona-prywatnosci-a-bezpieczenstwo-danych.html (accessed 07.07.2020).

data is collected and processed should therefore be taken into account. For example, the use of biometric data for the purpose of controlling employees' working time is disproportionate to the intended purpose of its processing.[37]

The opinion of the Judgement of the Court of Appeal in Gdańsk is correct in that an employer's interference with an employee's private sphere through the use of IoT solutions at the workplace may not be unlimited. An employer should observe the general provisions of the labour law, including Article 11^1 of the LC, which stipulates that they are obliged to respect the dignity and personal rights of an employee. Thus, the cited provision should set limits for any interference with an employee's privacy. As established in judicial decisions, respect for an employee's dignity and privacy as their personal rights is one of the fundamental duties of an employer.[38]

Conclusions

Modern technologies, including IoT, have great influence on every aspect of people's daily life. They undoubtedly affect the relationship between an employer and an employee, in particular the conditions of the work performed. Due to their specific nature, IoT solutions may be applied in virtually every industry, and they will probably become widespread in the near future. Although there are numerous advantages of their application, there are also certain risks related to information autonomy. That is why IoT will require an international legal framework. The specificity of IoT is based on the broad possibility of generating information, including employee data, the collection and processing of which is a key element of computerised reality. As a result, IoT makes it necessary to examine the issue of using sensitive data in greater detail.

The application of IoT in the working environment may involve biometric data, including behavioural data processing, which makes it possible to unambiguously identify an employee. Naturally, the use of modern technologies at a workplace does not have to involve only surveillance. Ubiquitous sensors, cameras, remote video surveillance of an employee at the workplace – all these factors may cause a person employed at a modern company to feel trapped. Currently applicable regulations set out grounds on which such data may be lawfully used by an employer quite precisely. The processing of personal and biometric data itself has been regulated by virtue of the provisions of the GDPR, which deserves credit. The authorisation

37 Judgement of the Supreme Administrative Court of 1 December 2009, I OSK 249/09, "Orzecznictwo Naczelnego Sądu Administracyjnego i wojewódzkich sądów administracyjnych" 2011/2/39.

38 Judgement of the Court of Appeal in Gdańsk of 12 June 2013, III APa 16/13, LEX No. 1339302.

of the establishment of legal bases for such activities under collective agreements is certainly an interesting solution.

There are no doubts as to the fact that an employer is able to use IoT technological solutions that make it possible to collect precise information on employees. Moreover, it seems that such solutions will be continuously developed. The risk of violating information autonomy, as well as far-reaching interference with employee privacy, should also be taken into account. It has long been pointed out in rulings that express consent for collecting and processing employees' data given at the request of an employer violates their rights and freedom of will.[39] Due to such risks, the processing of data collected with the use of IoT devices should be subject to specific restrictions regarding the purpose, adequacy and lawfulness. This is all the more important as IoT solutions enabling extensive interference with the information autonomy of an employee will become widespread in the era of Industry 4.0.

References

Ashton, K., *That "Internet of things" Thing*, 22.06.2009, RFID Journal, http://www.itrco.jp/libraries/RFIDjournal-That%20Internet%20of%20Things%20Thing.pdf.

Bąba, M., *Próba wyznaczenia zakresu pojęcia danych biometrycznych*, "Prawo Mediów Elektronicznych" 2016, No. 2.

Bąba, M., *Refleksje wokół prywatności i autonomii informacyjnej w świecie Internetu (wszech)rzeczy*, "Zeszyty Naukowe Wydziału Informatycznych Technik Zarządzania Wyższej Szkoły Informatyki Stosowanej i Zarządzania pod Auspicjami Polskiej Akademii Nauk. Współczesne problemy zarządzania" 2018, No. 2.

Bielak-Jomaa, E. and Lubasz, D. (ed.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, LEX 2018.

Chrzczonowicz, P. et al. (ed.), *Społeczeństwo inwigilowane w państwie prawa*, Toruń 2003.

Internet Rzeczy, ochrona prywatności a bezpieczeństwo danych, Deloitte, https://www2.deloitte.com/pl/pl/pages/doradztwo-prawne/articles/Internet-Rzeczy-ochrona-prywatnosci-a-bezpieczenstwo-danych.html.

Jemielniak, D., *Socjologia internetu*, Warszawa 2019.

Knade, A., *Czy pracodawca ma prawo inwigilować pracownika? Prawo do prywatności pracownika a interesy pracodawcy*, in Chrzczonowicz, P. et al. (eds.), *Społeczeństwo inwigilowane w państwie prawa*, Toruń 2003.

Krysiński, M., *Internet rzeczy – innowacyjne narzędzie dla firm*, "Ekonomiczne Problemy Usług" 2016, No. 122.

Kuba, M., *Komentarz do art. 9*, in: Bielak-Jomaa, E. and Lubasz, D. (eds.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, LEX 2018.

39 Judgement of the Court of Appeal of 17 October 2018, II PK 178/18, LEX No. 2562148.

Kwiatkowska, E.M., *Rozwój Internetu rzeczy – szanse i zagrożenia*, "Internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2014, No. 8.

Maj, I., *Internet rzeczy i zagrożenia z nim związane*, "Bezpieczeństwo. Teoria i praktyka" 2015, No. 3.

Malucha, M., *Internet rzeczy – kontekst technologiczny i obszary zastosowań*, "Studia i Prace WNEiZ US" 2018, No. 54.

Pyka, A., *Przetwarzanie danych biometrycznych. Aspekty prawne*, "Studia Prawa Publicznego" 2018, No. 3.

Raport Grupy Roboczej ds. Internetu rzeczy przy Ministrze Cyfryzacji, IoT w polskiej gospodarce, Ministerstwo Cyfryzacji, 2019, https://www.gov.pl/attachment/82ad18f8-2ac1-4433-a1ea-f887b522e46b.

Rot, A. and Blaicke, A.B., *Zagrożenia wynikające z implementacji koncepcji Internetu rzeczy w wybranych obszarach zastosowań*, "Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2017, No. 341.

Rot, A. and Blaicke B., *Bezpieczeństwo Internetu rzeczy. Wybrane zagrożenia i sposoby zabezpieczeń na przykładzie systemów produkcyjnych*, "Zeszyty Naukowe Politechniki Częstochowskiej. Zarządzanie" 2017, No. 26.

Senkus, P. et al., *Internet of Things: przeszłość – teraźniejszość – przyszłość*, "Zeszyty Naukowe Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach. Seria: Administracja i Zarządzanie" 2014, No. 103.

Wielki, J., *Internet Rzeczy i jego wpływ na modele biznesowe współczesnych organizacji gospodarczych*, "Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2016, No. 281.

CITATION

Ryś, K., *Internet of Things and biometric data versus employee privacy in the Polish case*, "Acta Iuris Stetinensis" 2020, No. 3 (Vol. 31), 79–94, DOI: 10.18276/ais.2020.31-05.