t. LXII, nr 4/2021 DOI 10.33226/0032-6186.2021.4.2

Dr hab. Krzysztof Stefański, prof. UŁ
Uniwersytet Łódzki
ORCID:0000-0001-6313-7387
e-mail: kstefanski@wpia.uni.lodz.pl

Employee geolocation versus the GDPR

Geolokalizacja pracowników a regulacje RODO

Abstract
Geolocalisation is an extremely helpful tool used by many businesses. Moreover, there are industries where it is difficult to imagine doing business without the use of geolocation. However, the use of this technology may raise concerns regarding potential infringements of employees' right to privacy. The GDPR and sector-specific regulations in the EU Member States are frequently perceived as restricting business operations. Employers who geolocate employees, however, should also see the benefits of such regulations. They do impose certain restrictions, but by regulating the use of the GPS technology they also provide opportunity to protect the interests of the enterprise while protecting the privacy of employees. The appropriate application of these regulations, therefore, may be beneficial for both parties to the employment relationship.

Keywords
geolocation, GPS, GDPR, personal data protection, right to privacy

JEL: K31

Streszczenie
Geolokalizacja jest niezwykle pomocnym narzędziem stosowanym w praktyce wielu przedsiębiorstw. Co więcej, istnieją branże, w których trudno wyobrazić sobie prowadzenie działalności bez stosowania geolokalizacji. Jednakże zastosowanie tej technologii może budzić wątpliwości związane z potencjalnym naruszeniem prawa do prywatności pracowników. Regulacje odnoszące się do ochrony danych osobowych, zwłaszcza RODO, wprowadzają pewne standardy ochrony w tym względzie, jednak są one postrzegane przez pracodawców jako ograniczające prowadzenie działalności gospodarczej. Zdaniem autora warto postulować zmianę takiego podejścia, bowiem unormowania takie dają szerokie możliwości zabezpieczenia interesów przedsiębiorstwa, przy zachowaniu ochrony prywatności pracowników.

Słowa kluczowe
geolokalizacja, GPS, RODO, ochrona danych osobowych, prawo do prywatności

Geolocation in business practice

Geolocation is a process of detecting the location of a given object on Earth. It helps to detect the location of people or objects, e.g. mobile telephones, tablets, or other mobile devices, by means of GPS or other similar systems, such as the European Gallileo, Russian GLONASS, or Chinese Compass. These systems make it possible to determine in real time the location of an object with an accuracy of approximately 1–3 metres. In the nearest future this accuracy will reach approximately 10 cm.[1] Apart from satellite location, other systems exist which are based on different technological solutions. One of the most advanced methods is radio frequency identification (RFID) which is used, e.g. in the mining industry. Location systems boast multiple uses — both in the delivery of public duties — by police and other services, search and rescue, and air traffic control — and in the private sector — mainly in road freight transport, as well as in public transport and commerce.

Some industries are legally required to monitor freight transports. Many countries have enacted laws and regulations on the duty of monitoring the transports of certain goods. One example may be the Hungarian system EKAER which regulates any and all shipments on the Hungarian territory[2], German rules of registration of coffee transports from other states, or the Polish system SENT which regulates transports of fuels, crude oil, and alcohol[3]. In terms of the European law, as of 20 May 2019, the monitoring duty applies to tobacco products which must be registered in the Track & Trace system[4] (on foot of the Directive 2014/40/EU[5]). The foregoing systems are designed to seal the tax system and eliminate illicit trading in certain goods.

By and large the monitoring systems for transports and location control are operated for commercial purposes. Employers use geolocation systems for various purposes, e.g. to protect employer's property, oversee the use of resources, control employees' working time, or ensure employee safety at work. Modern control systems enable a more effective use of resources and costs optimisation, which helps businesses to develop their market position. This is of particular importance for highly competitive industries, where any solutions helping to save time and resources may be the success factors in gaining competitive advantage.

The purposes identified above are certainly legitimate and the use of geolocation systems in some industries is surely more than reasonable. The demand for their applications upsurges with the increase of their data acquisition capacity and accuracy, as well as the downfall of the prices for such systems. It goes without saying that the number of businesses utilising such solutions will be on the increase. It is, therefore, expedient to ask questions about the legitimacy of the use of such systems in the light of employee right to privacy and the personal data protection regulations.

Right to privacy

The right to privacy is a human right guaranteed by a series of international and European legal acts, as well as by individual national legislations. One example is Article 12 of the Universal Declaration of Human Rights which provides that: "No one shall be subjected to arbitrary interference with his privacy (…). Everyone has the right to the protection of the law against such interference". Likewise, this right is enshrined in Article 17 of the International Covenant on Civil and Political Rights which stipulates that: "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence…", Article 8 of the European Convention on Human Rights 1950 which also regulates the right to privacy, "Everyone has the right to respect for his private and family life, his home and his correspondence.", which also lays down more specific regulations.

The right to privacy and personal data protection is also set forth in the Charter of Fundamental Rights of the European Union. In terms of its Article 7, everyone has the right to respect for his or her private and family life, home and communications. Article 8 of this Charter stipulates that everyone has the right to the protection of personal data concerning him or her, and develops this principle in its further regulations.

The right to privacy is the subject matter of a many of judicial decisions of the European Court of Human Rights. These judicial decisions help to specify and adequately construe the international law in this respect, and examples of the most significant judicial decisions include Sunday Times Case[6], Malone Case[7], Kruslin Case[8], and many other. The judgments relating to the privacy of an employee (e.g. Niemietz[9] and Halford[10] Cases), in which the Tribunal recognized that professional life is a key forum for exercising the right to private life, are also of significant importance. that professional life represents a crucial forum for the fulfillment of the right to private life (Otto, 2016, p. 74).

The right to privacy is enshrined in the constitutions of many countries. In some of them this right explicitly arises out of the constitutional law. This is exemplified by Article 18.1 of the Spanish constitution, Article 2(6) of the Swedish constitution, or Article 102 of the Norwegian constitution. In other cases the right to privacy is not explicitly expressed in the constitution, but ensues from other fundamental rights, e.g. the right to protection of private or family life, etc. — e.g. in Article 26 of the Portuguese constitution, or Article 96 of the Latvian constitution. In other countries this right is construed in terms of other constitutional norms. The German constitution makes no direct reference to the right to privacy, however, in terms of the German constitutional law it represents a part of more general rights, e.g. to human dignity (Article 1(1) of the Constitution), personal freedom (Article 2(1)), and is directly linked to the right to confidentiality of correspondence and integrity of the place of residence (Cornell, 2021). Articles 1(1) and 2(1), as the Federal German Constitutional Court has interpreted them, lay the foundation for a general freedom of action, the right to free self-determination, and the right to a private sphere. The Polish Constitution holds two article of relevance for the right to privacy, Articles 47 and 49. According to Article 47 "everyone has the right to legal protection of his private and family life, of his honour and good reputation and to make decisions about his personal life." Article 49 stipulates the right to privacy and freedom of communications. Both articles take their starting point in Article 30, human dignity.

The Polish legal doctrine notes that "privacy is to be protected, because every person has the right to exclusive control of the sphere of life that does not concern the others and in which freedom from the curiosity of the others is a specific conditio sine qua non of the free development of an individual (Safian, 2006, p. 211).

GPS versus employee data protection

The use of geolocation to monitor employees may give rise to far-reaching issues with personal data processing, such as the scope and transparency of data acquisition, or the purposes of data processing. In the European Union the fundamental regulation in this respect is the GDPR, as well as the sector-specific regulations adopted in the legislations of the Member States. Data processing, in the context of employment, is regulated by Article 88 of the GDPR. This regulation enables the Member States to issue the afore-mentioned sector-specific regulations in this respect. Also, it is noted that these regulations must encompass appropriate and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place.

It needs to be noted that the scope of data acquisition is relative to the needs of the entity which acquires the same. Geolocation devices, with their original and simplest settings, only collect and transmit information about a GPS receiver's location on the surface of the Earth (geographic longitude, latitude, and height), the direction of its movement, and the time of registration of the given location. In other words, location data are the information collected by an application or service provider about where the user's mobile device is located at a given time. However, contemporary systems offer much greater capabilities. They may collect data about

the speed of travel, driving style, compliance with the traffic code, parking places, stopovers, etc. Additionally, continuous data acquisition may help find out employee behaviour models, their preferred routes, places of rest, meal break destinations, etc. Therefore, it is important to restrict the scope of employee data acquisition. The key issue is that employers should acquire the data that correspond with the purposes of data processing (principle of data minimisation). Hence employer is required to clearly specify the purpose of data acquisition. Some reasonable purposes of monitoring are, for instance:

- ❒ to protect confidential information representing business secret,
- ❒ to protect employer's property,
- ❒ to prevent actions to the prejudice of the work place,
- ❒ to oversee appropriate work performance, including working time compliance.

Monitoring systems may be applied as a preventive measure, or in response to any irregularities found.

Data acquisition must comply with the principle of proportionality. This means that the measures taken must be proportionate to the purpose of monitoring. Processing cannot be considered necessary or proportionate, if the interest served by the processing is only of little importance, while the impact on privacy is high. It also means that an employer must perform only those processing operations which can achieve the intended purpose while having the least impact on privacy.

In this context the Privacy Impact Assessment is essential. A privacy impact assessment (PIA) is an essential tool for performing and documenting such a proportionality test. A PIA is explicitly required under the GDPR if a type of processing is likely to pose a high risk to the privacy of natural persons (such as employees), in particular when new technologies are used. A high risk must be assumed and a PIA must be performed in particular if the processing involves more information, involves more sensitive information, or occurs systematically over a longer time-period, and may cause decisions about a person which have a significant effect on their life (such as legal decisions).

The GDPR also requires employers to implement privacy by design and by default. Privacy by design means that whenever new systems, applications or technologies are developed, the impact on privacy should be considered from the very beginning. Privacy by default means that the default settings of systems, applications or technologies should minimise the amount and the sensitivity of personal data processed automatically. Therefore, privacy by design and by default help ensure that personal data is only processed if this is necessary and proportionate.[11]

Another issue is the monitoring of company vehicles also used for employee's private purposes. In such situations, while collecting vehicle data, employer may also obtain data of employee's private life. Employer is not entitled to acquire such data, unless we are dealing with an extraordinary situation, e.g. the taking of vehicle. One possible solution is to install a system working in two modes — travel on business and in private. In keeping with the "privacy by default" principle introduced by the GDPR, the private travel mode should be a default setting on the GPS.

The third fundamental principle of employee data processing, in addition to the principles of minimisation and proportionality, is the principle of transparency (see more e.g. Gawronski, 2019). This means that employees must be informed that they are subject to geolocation. In particular, employees should be made aware:

- ❒ that a GPS monitoring device is installed on the company vehicles,
- ❒ what data are collected by the said device (e.g. travel speed, current position, distance travelled, length of stopovers, places visited, etc.),
- ❒ what is the purpose of data acquisition (e.g. to increase labour safety, optimise logistic operations, etc.).

Importantly, such information must be passed across to employees prior to the start-up of the system. New employees must be advised of the presence of the system on being admitted to work. The Article 29 Working Party has brought to attention that the information communicated to employees must be clear and intelligible. Additionally, it is recommended that the process of formulating and assessing the inner guidelines and policies, e.g. in respect of monitoring at the work place, should involve staff representatives.[12] Also, the vehicles equipped with GPS devices are required to be appropriately labelled, e.g. by means of special geolocation notice stickers. It needs to be emphasised that even though employer does label the geolocated vehicles, this does not discharge him from the duty to supply employee, as the data subject, with any and all information required under the GDPR and communicate with him in relation to his personal data processing (Article 12 RODO), or from the information duty laid down in Article 13 of the GDPR.

It is recognised that for the purposes of ordinary geolocation of employees it is sufficient to simply advise them of this fact. However, at times employee's consent is required to process his data. This will apply when geolocation is used after the working hours or during rest breaks, e.g. during employee's private travels. Such consent should be clear and explicit, best expressed in writing or by electronic means. The declaration of consent for personal data processing should specify, e.g. the purpose of his data processing, the controller who is going to process them, and the rights of the consenting data subject. Doubts may arise about the voluntary nature of employee's consent for his personal data processing, the more so that the EU legislator definitely notes that such consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller (preamble to the GDPR 43). This is confirmed by the position of the Article 29 Working Party which emphasises that employees are essentially not "free" to give such consent for their data processing.[13]

Summary

For many businesses the use of contemporary control devices, such as GPS, is an important part of their

operations, business strategies, and building competitive advantage. Such monitoring systems ale legally allowable and no need exists to change that. However, the use of such systems for the purpose of controlling employees may pose a threat to their privacy. Hence, it is necessary to precisely abide by the rules within the existing laws and regulations. The provisions of the GDPR enforce the application of the rules of personal data protection regulated therein, under the threat of criminal and civil liability (see more: Barański & Giermak, 2017, p. 208). However, it is worthwhile for entrepreneurs to see not only the risk of liability, but also the benefits related to compliance with data protection rules.

The GDPR and sector-specific regulations in the EU Member States are frequently perceived as restricting business operations. Employers who geolocate employees, however, should also see the benefits of such regulations. They do impose certain restrictions, but by regulating the use of the GPS technology they also provide opportunity to protect the interests of the enterprise while protecting the privacy of employees. The appropriate application of these regulations, therefore, may be beneficial for both parties to the employment relationship.

Notes/Przypisy

1 As per the forecast of the European Space Agency for Galileo system.

2 For more — see https://ekaer.nav.gov.hu

3 For more — see https://puesc.gov.pl/en/web/puesc/e-przewoz

4 For more — see https://ec.europa.eu/health/tobacco/tracking_tracing_system_en

5 Directive 2014/40/EU of the European Parliament and of the Council of 3 April 2014 on the approximation of the laws, regulations and administrative provisions of the Member States concerning the manufacture, presentation and sale of tobacco and related products and repealing Directive 2001/37/EC (OJ, L 127/1, 29.04.2014).

6 Judgement of the European Court of Human Rights of 26.04.1979, 6538/74 Sunday Times v United Kingdom, publications of the European Court of Human Rights, Serie A: Judgements and decision, Vol. 82, s. 32.

7 Judgement of the European Court of Human Rights of 2.07.1984, 8691/79 Malone v United Kingdom, Serie A, Vol. 30, p. 30.

8 Judgement of the European Court of Human Rights of 24.04.1990, 11801/85 Kruslin v France, Serie A, Vol. 176, p. 24.

9 Judgement of the European Court of Human Rights of 16.12.1992, 13710/88 Niemietz v Germany seria A, Vol. 251-B.

10 Judgement of the European Court of Human Rights of 25.06.1997, 20605/92 Halford v. United Kingdom, Reports 1997–III.

11 Privacy and monitoring at work under the GDPR. https://legalict.com/factsheets/privacy-monitoring-work-gdpr/

12 Article 29 Data Protection Working Party "Opinion 2/2017 on data processing at work 8.06.2017, WP 249". http://ec.europa.eu/newsroom/document.cfm?doc_id=45631

13 Article 29 Data Protection Working Party Opinion 2/2017 on data processing at work 8.06.2017, WP 249. http://ec.europa.eu/newsroom/document.cfm?doc_id=45631

References/Bibliografia

Barański, M. & Giermak, M. (2017). Protection of employees' geolocation data in EU law. In: *Earth observation & navigation: law and technology*. Warsaw.

Cornell, A. J. (2021). *Right to Privacy. Max Planck Encyclopedia of Comparative Constitutional Law*. https://oxcon.ouplaw.com/view/10.1093/law:mpeccol/law-mpeccol-e156

Gawronski, M. (ed.). (2019). *Guide to GDPR*. Alphen aan den Rijn.

Otto, M. (2016). *The right to privacy in employment: a comparative analysis*. Oxford, Portland, Oregon.

Safjan, M. (2006). Prawo do ochrony życia prywatnego. W: *Szkoła Praw Człowieka*. Warszawa: Helsińska Fundacja Praw Człowieka.

Dr hab. Krzysztof Stefański, prof. UŁ, Associated professor at the Labour Law Department at the Faculty of Law and Administration of the University of Lodz. Team Coordinator of AI Work Team — The research team for conducting studies on the consequences of the development of artificial intelligence and other modern technologies for the labour market, labour law and social insurance. Director of the Postgraduate Studies on Personal Data Protection at the University of Lodz. Author and co-author of numerous publications in the field of labour law, including 4 books and many scientific articles. Co-author of a commentary to the Labour Law Code, ed. by K.W. Baran, (commentary to the Working Time chapter) and a commentary to the "Anti-crisis Shield" (ed. by K.W. Baran). His scientific interests concentrate on issue of working time, termination of the contract of employment, employment in public administration and the consequences of development of artificial intelligence and other modern technologies for the labour law.

Dr hab. Krzysztof Stefański, prof. UŁ, doktor habilitowany nauk prawnych, profesor Uniwersytetu Łódzkiego, pracuje w Katedrze Prawa Pracy na Wydziale Prawa i Administracji UŁ. Koordynator AI Work Team — Zespołu badawczego ds. prowadzenia badań nad skutkami rozwoju sztucznej inteligencji i innych nowoczesnych technologii dla rynku pracy oraz prawa pracy i ubezpieczeń społecznych. Kierownik Podyplomowych Studiów Ochrony Danych Osobowych UŁ. Autor i współautor licznych publikacji z zakresu prawa pracy i prawa urzędniczego, m.in. 4 monografii, części komentarza do Kodeksu pracy (red. K.W. Baran, wyd. III, IV i V) oraz części komentarza do „tarczy antykryzysowej" (red. K. W. Baran), a także kilkudziesięciu artykułów w czasopismach naukowych. Jego zainteresowania naukowe obejmują kwestie czasu pracy, ustania stosunku pracy i prawa zatrudnienia w administracji publicznej, a także wpływu rozwoju sztucznej inteligencji i innych nowoczesnych technologii na prawo pracy.