Acta Univ. Sapientiae, Legal Studies, **12**, 2 (2023) 1–17

DOI: 10.47745/AUSLEG.2023.12.2.01

Geolocation Monitoring of an Employee from the Perspective of Article 8 of the ECHR[1]

Michał BARAŃSKI

PhD, Assistant Professor
University of Silesia in Katowice (Katowice, Poland)
e-mail: michal.baranski@us.edu.pl

Tomasz MIROSŁAWSKI

PhD candidate
Deák Ferenc Doctoral School of the Faculty of Law of the University of Miskolc (Miskolc, Hungary), Researcher at the Central European Academy of the University of Miskolc (Budapest, Hungary)
e-mail: tomasz.miroslawski@centraleuropeanacademy.hu

Abstract. Current technological and economic development has resulted in the increasing demand for and expansion of surveillance techniques that enable the precise monitoring of employees and objects in the workplace. One such technique is geolocation monitoring, which raises many questions and controversies regarding Article 8 of the European Convention on Human Rights. The employment relationship is characterized by the specific inequality of its parties and the conflict between their rights and interests. This conflict on the basis of the use of geolocation surveillance in the workplace takes the form of a conflict between the function and the right of the employer to organize the work process and monitor their expenses and the right of the employee to respect for their private life. In order to ensure adequate protection of the employee's privacy on the one hand and to determine the reasonable scope of acceptable interference with Article 8 of the ECHR in the case of the use of geolocation monitoring in the workplace on the other hand, it is necessary to strike a fair balance between relevant interests and rights of the employment relationship parties. This article aims to analyse the ECtHR's approach to the issue of GPS surveillance in and outside the workplace and to answer two questions: (1) whether the ECtHR's conclusions differ in the case of workplace geolocation from geolocation used in other circumstances and (2) whether the ECtHR's findings differ in the case of employee geolocation monitoring from other forms of workplace monitoring.

1 See the Convention for the Protection of Human Rights and Fundamental Freedoms of 4 November 1950, https://www.echr.coe.int/Pages/home.aspx?p=basictexts&c= (accessed: 15.11.2023); hereinafter referred to as ECHR.

Keywords: geolocation, surveillance, right to privacy, GPS, ECHR, employee monitoring

1. Initial Remarks

Under the European Convention on Human Rights, the normative basis for employees' right to privacy derives only from the general privacy framework (the issue of employees' right to privacy has not been regulated separately, which means that Article 8 of the ECHR will be fully applicable to them).[2] To this must be added that protecting privacy from an employment relations perspective is a relatively new aspect of international human rights protection.[3] The analysis of the European Court of Human Rights (ECtHR) judgments shows how the concept of 'private life' has evolved to also cover employment relationships.[4] The position taken was that 'in the course of their working lives the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world'.[5] Over time, as part of an employee's right to privacy in employment, the ECtHR has allowed an employee's right to develop a 'social identity'.[6]

One of the main issues considered by the ECtHR in the context of an employee's right to privacy is the legality of an employer's monitoring of an employee.[7] The

2 In accordance with Article 8, paragraph 1 of the ECHR, 'everyone has the right to respect for his private and family life, his home and his correspondence'. Furthermore, 'there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others' (Article 8, paragraph 2 of the ECHR).

3 See Hendrickx–van Bever 2013. 183.

4 See, for example, Judgments of the ECtHR: of 5 September 2017, *Bărbulescu v Romania*, Application No. 61496/08; of 12 June 2014, *Fernández Martínez v Spain*, Application No. 56030/07; of 7 February 2012, *Von Hannover v Germany (no. 2)*, Application No. 40660/08; of 28 November 2017, *Antović and Mirković v Montenegro*, Application No. 70838/13; of 25 September 2018, *Denisov v Ukraine*, Application No. 76639/11; of 25 September 2001, *P. G. and J. H. v the United Kingdom*, Application No. 44787/98; of 17 July 2003, *Perry v the United Kingdom*, Application No. 63737/00; of 17 October 2019, *Lopez Ribalda and Others v Spain*, Applications Nos. 1874/13 and 8567/13; Decision of the ECtHR of 5 October 2010, *Köpke v Germany*, Application No. 420/07.

5 Judgment of the ECtHR of 16 December 1992, *Niemietz v Germany*, Application No. 13710/88.

6 The concept of private life is not limited to the 'inner circle' in which an individual can lead their own personal life without outside interference, but it also includes the right to lead a 'private social life', i.e. the ability to establish and develop relationships with other people and the outside world, e.g. in the professional sphere. See *Bărbulescu v Romania*. See also: Barański 2021. 340–353; Otto 2016. 68–120.

7 See, for example, *Lopez Ribalda and Others v Spain* and the judgments mentioned therein. The case involved hidden video monitoring.

literature emphasizes that employee monitoring, understood as the observation of employees by the employer in any way, includes many different forms of employee surveillance.[8] According to the definition of monitoring set out in the code of practice on the protection of workers' personal data, drawn up by the International Labour Organization (ILO), monitoring 'includes, but is not limited to, the use of devices such as computers, video equipment, sound devices, telephones and other communication equipment, various methods of establishing identity and location, or any other method of surveillance'.[9] Therefore, geolocation monitoring is one of these forms of monitoring.[10]

The science of labour law has so far not focused on the issue of employee geolocation monitoring from a human rights perspective. From an international law context, the authors have so far only focused their attention on issues related to the processing of geolocation data in connection with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and by repealing Directive 95/46/EC (General Data Regulation).[11] Meanwhile, the ECtHR recently explicitly addressed the issue of geolocation monitoring in the workplace by deciding the case of *Florindo de Almeida Vasconcelos Gramaxo v Portugal* (Application No. 26968/16) on 13 December 2022.[12] The need to consider the theses derived from this judgment was the main contribution to the preparation of this article. The article answers the question of whether the ECtHR's conclusions differ in the case of workplace geolocation from geolocation used in other circumstances and whether the ECtHR's findings differ in the case of employee geolocation monitoring from other forms of workplace monitoring.

2. Differences between Workplace Geolocation and Any Other Geolocation

The ECtHR jurisprudential line on the protection of the right to respect for private and family life (Article 8 ECHR) in the context of geolocation surveillance is

8 Barański–Giermak 2017. 197.

9 See ILO 1997.

10 Geolocation data seems to fall within the conceptual scope of geoinformation, understood as 'information obtained through the interpretation of geospatial data'. See Jankowska–Pawełczyk 2014. 1. Also, see the literature quoted by the authors. In Polish legal literature, geoinformation is defined as 'information about the location, geometric properties and spatial relations of objects, which might be identified in relation to the Earth'; however, the concept of an object is used in its broad sense. Ibid.

11 OJ L 119, 4.5.2016. See also Stefański 2021. 14–17; Barański–Giermak 2017. 197–208.

12 Judgment of the ECtHR of 13 December 2022, *Florindo de Almeida Vasconcelos Gramaxo v Portugal*, Application No. 26968/16.

based on three cases. These cases are as follows: *Uzun v Germany*, in which the judgment was delivered on 2 September 2010; *Ben Faiza v France*, with the judgment from 8 February 2018; *Florindo de Almeida Vasconcelos Gramaxo v Portugal*, in which a judgment was issued on 13 December 2022.

Within the realm of *Uzun v Germany*, the applicant who was suspected of bomb attacks committed by an extremist terrorist organization, the so-called Anti-Imperialist Cell, alleged that the GPS observation he had been subjected to, and the use of the data obtained by this technique in the criminal proceedings against him, had violated his right to respect for his private life under Art. 8 and his right to a fair trial under Art. 6 of the ECHR.[13] A similar basis can be found in *Ben Faiza v France*, in which the applicant indicated that the installation of a geolocation device on his vehicle and the court order issued to the telephone operator to obtain information about his movements had constituted an interference with his right to respect for his private life.[14] However, the difference between the two cases is that the surveillance measures against Mr Faiza were taken because of his involvement in drug-trafficking offences.[15] The last of the cases to be addressed in this section of the paper significantly varies in its background from the previous two. *Florindo de Almeida Vasconcelos Gramaxo v Portugal* concerned the dismissal of the applicant on the basis of data collected from a geolocation system installed in a vehicle which his employer had made available to him in order to carry out his duties as a medical representative and also allowed him to use it for private purposes. The applicant alleged that the processing of the geolocation data obtained from the GPS system and his dismissal based on this data had infringed his right to respect for his private life. He also considered that the national proceedings against his dismissal had been unfair, and that the decision issued at the end had breached the principle of legal certainty.[16]

All of the above cases touch on essentially the same subject, namely the protection of the right to respect private life in the context of geolocation technology. Furthermore, it should be considered that the exact definition of geolocation proposed by D. Zannoni, who pointed out that GPS trackers are devices which enable to determine the precise location of the vehicles or objects on which they are installed, will apply to them.[17] Zannoni indicates that the basic function of GPS devices is to monitor the movements of objects. However, the geolocalization technique is often combined with further investigation activities, allowing the identification of the passengers on the vehicle or who use the object under monitoring, therefore linking the movements of vehicles or objects to the

13 *Uzun v Germany*, Application No. 35623/05, 2 September 2010, par. 3.
14 *Ben Faiza v France*, Application No. 31446/12, 8 February 2018, par. 3.
15 Id. par. 6.
16 *Florindo de Almeida Vasconcelos Gramaxo v Portugal*, Application No. 26968/16, 13 December 2022, par. 1.
17 Zannoni 2018. 297.

movement of persons.[18] Obviously, the term 'further investigation activities' used in the definition mentioned above, which derives from the conceptual framework of criminal procedure, cannot be directly applied to the geolocalization occurring in *Florindo de Almeida Vasconcelos Gramaxo v Portugal* because of its nature connected with the employment relationship. Although the phenomenon of linking the surveillance of movements of objects and vehicles with the surveillance of movements of specific persons was clearly visible in this case. This was confirmed by the Court itself, which indicated that the geolocation system used in the company car allowed tracking the vehicle's movement in real time, which in turn made it possible to trace the geographical location of the person or persons who were to use it at any given time or on a continuous basis.[19] In this context, it is also not insignificant that the GPS system used by the employer was initially not only used to monitor its property, i.e. the vehicle, but was also intended to monitor the applicant's working time and efficiency as an employee.[20] Only during the proceedings before the national courts did the Portuguese Court of Appeal questioned the possibility of using geolocation for the latter purpose and stated that GPS devices could not be used to monitor the efficiency of employees or their compliance with working hours.[21] This finding was endorsed by the ECtHR.[22]

However, despite the one definition of geolocation that can be applied to all of the above cases and the seemingly identical subject matter, the ECtHR did not adopt a uniform approach when examining them. The differences in the Court's conclusions are primarily due to the detailed circumstances and diverse backgrounds of the analysed cases. On the one hand, there are the cases *Uzun v Germany* and *Ben Faiza v France* related to the sphere of criminal proceedings, in which there was an intervention of public authorities into the privacy of the individual; on the other hand, there is the case of *Florindo de Almeida Vasconcelos Gramaxo v Portugal*, which arose from actions taken by two private parties (employer and employee) in the context of an employment relationship.

In order to comprehensively answer the first of the questions raised in the introduction, whether the ECtHR's conclusions differ in the case of workplace geolocation from geolocation used in other circumstances, the following part of the current section of the article will be devoted to an analysis of these conclusions developed on the basis of two categories of cases involving the issue of geolocalization so far decided by the Court.

18 Id. p. 297.
19 *Florindo de Almeida Vasconcelos Gramaxo v Portugal*, par. 95.
20 Id. par. 40.
21 Id. par. 118–119.
22 Id. par. 120.

The focal point of the judgments in *Uzun v Germany* and *Ben Faiza v France* is the analysis of Article 8 (2) of the Convention. This article introduces the possibility of public authorities to interfere with the right to respect for one's private life, conditioning this interference in accordance with the law and necessity in a democratic society.[23] ECtHR indicates that requirement of 'accordance with the law' means that the measures used by public authorities within interference should have some basis in domestic law.[24] The notion of 'law' is interpreted by the Court in Strasbourg in a broad manner, including both written and unwritten law (i.e. primary legislation, subsidiary rules, and interpretations given by the jurisprudence).[25] However, the ultimate characteristic that constitutes the notion of law adopted by the Court is its quality, requiring that it should be accessible to the persons concerned, who must, moreover, be able to foresee its consequences for them, and compatible with the rule of law.[26]

When discussing the requirement of foreseeability, the doctrine of criminal procedure, following the jurisprudence of ECtHR, argues that persons who may be potential targets of surveillance should not be enabled to foresee when the authorities are likely to interfere with their communications or track their movements so as not to be able to adapt their conduct accordingly. Nevertheless, the law must be sufficiently clear to permit citizens to recognize under what circumstances and under what conditions public authorities are entitled to infringe their privacy covertly.[27] Thus, the meaning of foreseeability *in concreto* has been rejected in this situation due to the fact that the success of relevant investigative methods, including GPS surveillance, requires an appropriate degree of unawareness on the part of the monitored person.[28] This understanding of foreseeability is specific for cases involving the use of geolocation in investigation techniques and significantly differs from the concept of foreseeability adopted for GPS tracking in the context of privacy at work, which will be addressed further below.

Another conclusion of the ECtHR, stemming from the analysis of the *Uzun v Germany* and *Ben Faiza v France* cases, is the division of surveillance methods into those that are more likely to violate a person's right to respect for their private life and those that have a lower probability of such violation. Geolocation-based techniques have been classified in the second category. The Court pointed out that GPS surveillance, by its very nature, should be distinguished from other methods

23 European Convention on Human Rights, Art. 8 (2).

24 *Uzun v Germany*, par. 60; *Ben Faiza v France*, par. 56.

25 Otto 2016. 80; Zannoni 2018. 300; *Kruslin v France*, Application No. 11801/85, 24 April 1990, par. 28–29; *The Sunday Times v United Kingdom*, Application No. 6538/74, 26 April 1979, par. 47; *Ben Faiza v France*, par. 56.

26 *Kruslin v France*, par. 27; *Uzun v Germany*, par. 60; Otto 2016. 80; Zannoni 2018. 299.

27 *Malone v The United Kingdom*, Application No. 8691/79, 2 August 1984, par. 67; *Kruslin v France*, par. 30.

28 Zannoni 2018. 297, 300.

of visual or acoustical surveillance because they disclose more information on a person's conduct, opinions, or feelings.[29]

The above conclusion directly translates into the Strasbourg Court's view that the strict standards set up and applied in the specific context of surveillance of telecommunications do not apply to cases regarding surveillance via GPS.[30] These standards indicate that, in order to prevent excessive abuses, national laws concerning the inception of telecommunications should define: the nature of the offences which may give rise to an interception order; categories of people liable to have their communications monitored; limits on the duration of such monitoring; the procedure to be followed for examining, using, and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which data obtained may or must be erased or the records destroyed.[31] With regards to GPS surveillance, in order to ensure an adequate level of protection against arbitrary interference, more general principles are sufficient, requiring domestic law to consider all the circumstances of the case such as: the nature, scope, and duration of the possible measures; the grounds required for ordering them; the authorities competent to permit, carry out, and supervise them; and the kind of remedy provided by national law.[32] Therefore, the 'simplified legality test' should be considered applicable to GPS surveillance,[33] and the scope of the margin of appreciation of Member States and the role of national legislation increases.[34] This is moreover evident on the ground of the national legislation invoked in the *Uzun v Germany* and *Ben Faiza v France* cases. Article 100c (1) no. 1 of the German Code of Criminal Procedure indicated that

> without the knowledge of the person concerned, a) photographs may be taken and visual recordings be made, b) other special technical means intended for the purpose of surveillance may be used to investigate the facts of the case or to detect the perpetrator's whereabouts if the investigation concerns a criminal offence of considerable gravity and if other means of investigating the facts of the case or of detecting the perpetrator's whereabouts had less prospect of success or were more difficult.[35]

29 *Uzun v Germany*, par. 52; *Ben Faiza v France*, par. 53.

30 *Uzun v Germany*, par. 66.

31 *Huvig v France*, Application No. 11105/84, 24 April 1990, par. 34; *Kruslin v France*, Application No. 11801/85, 24 April 1990, par. 35; *Weber and Saravia v Germany*, Application No. 54934/00, 29 June 2006, par. 95; *Uzun v Germany*, par. 65.

32 *Klass and Others v Germany*, Application No. 5029/71, 6 September 1978, par. 50; *Uzun v Germany*, par. 63.

33 Galetta–De Hert 2014. 61.

34 Zannoni 2018. 302; *Leander v Sweden*, Application No. 9248/81, 26 March 1987, par. 59; *Peck v The United Kingdom*, Application No. *44647/98, 28 April 2003, par. 77.*

35 Article 100c (1) No. 1 of the German Code of Criminal Procedure.

The ECtHR stated that under the wording of Art. 100c (1) no. 1 (b) in which the open clause 'other special technical means' was used, the usage of GPS surveillance was reasonably foreseeable.[36] Further, the Court ruled that the standards set by the aforementioned provision are sufficient and even quite strict, as the use of these monitoring methods is limited only against a person suspected of a criminal offence of considerable gravity and if other means of detecting the whereabouts of the accused had less prospect of success or were more difficult.

In contrast, the Court ruled the opposite in *Ben Faiza v France.* Considering Article 81 of the French Code of Criminal Procedure, which is highly general in its nature and stipulates that 'the investigating judge undertakes in accordance with the law any investigative step he deems useful for the discovery of the truth. He seeks out evidence of innocence as well as guilt',[37] ECtHR held that this provision neither meets the requirement of foreseeability nor constitutes the adequate and sufficient safeguards against abuse and thus cannot be the legal basis for the use of geolocation.[38]

Closing the analysis of the *Uzun v Germany* and *Ben Faiza v France* cases, it should be pointed out that the ECtHR, in these particular cases, attached great importance to the safeguards expressed in national laws, whose aim was to ensure that Article 8 of ECHR is not excessively infringed during the use of geolocation monitoring. This is linked to the requirements of paragraph 2 of Art. 8 of ECHR, to which interference by a public authority with the right to respect for private and family life must conform, in particular, to the requirement of 'necessity in a democratic society'. The notion of necessity in a democratic society means that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued.[39] Certainly, the fight against crime is an urgent social need, and the use of GPS in this context will be justified, but how should proportionality be considered? In accordance with the Court's view that geolocation is a less intrusive measure than, for example, visual surveillance, one has to agree with Zannoni's claim based on *a contrario* reasoning in relation to the *Uzun v Germany* judgement that when GPS is an investigative technique aimed at preventing crime, the proportionality requirement will in principle be met, unless monitoring is carried out over substantially long periods of time and/or when it will concern minor offences.[40]

36 *Uzun v Germany*, par. 68.

37 'The investigating judge undertakes in accordance with the law any investigative step he deems useful for the discovery of the truth. He seeks out evidence of innocence as well as guilt.' Article 81 of the French Code of Criminal Procedure, as translated in: https://sherloc.unodc.org/cld/uploads/res/document/fra/2006/code_of_criminal_procedure_en_html/France_Code_of_criminal_procedure_EN.pdf (accessed: 05.07.2023).

38 *Ben Faiza v France*, par. 59.

39 *Uzun v Germany*, par. 78; Id. par. 77.

40 Zannoni 2018. 308.

Turning to a brief analysis of the *Florindo de Almeida Vasconcelos Gramaxo v Portugal* case, limited to outlining the similarities and differences between the ECtHR's conclusions in the cases of geolocation at the workplace and usage of GPS surveillance as an investigation technique, it should first be pointed out that due to the character and factual circumstances of the case the Court indicated that in addition to the negative duties of the state, i.e. not interfering with the right to privacy, there are also positive obligations whose aim is to adopt appropriate measures to ensure respect for private life even in relations between individuals.[41] The choice of these measures is within the margin of appreciation of Member States,[42] which is to some extent related to the previously discussed cases.[43] However, in *Florindo de Almeida Vasconcelos Gramaxo v Portugal*, the Court ruled that, with regard to the surveillance of employees in the workplace, it is up to the states whether to adopt specific legislation or not, and the role of safeguarding the employee's right to respect for private life against excessive interference by the employer belongs to the national courts.[44] With this conclusion, the Court granted more discretion to the Member States in creating appropriate regulations concerning geolocation at the workplace than it did in the *Uzun v Germany* case, where, despite applying a simplified legality test regarding the usage of GPS during the investigation, ECtHR highlighted four issues that national law covering geolocation surveillance should address,[45] thus indicating that such a law should exist.

However, regardless of whether the role of shaping geo-surveillance guarantees is assigned to national courts or legislative acts, they must meet the requirements of accessibility and foreseeability.[46] On the ground of the second requisite, another difference emerged between the analysed geolocation use cases. In situations where GPS is used as an investigative technique, an understanding of foreseeability in an absolute sense (*in concreto*) is excluded.[47] When geolocation is used in the workplace to monitor an employee or the tool they are using (e.g. a vehicle), such strict foreseeability may not necessarily be imposed. In this situation, the requirement of foreseeability should be understood *in concreto*. This is because the Court attached great importance to the fact whether the person under the scope of the GPS surveillance was properly informed about it.[48]

While considering the proportionality of workplace geolocation, the ECtHR, unlike in previous cases, decided to shift from a rather schematic subsumption

41 *Florindo de Almeida Vasconcelos Gramaxo v Portugal*, par. 105.
42 Id. par. 107.
43 Zannoni 2018. 302.
44 *Florindo de Almeida Vasconcelos Gramaxo v Portugal*, par. 108.
45 *Uzun v Germany*, par. 63.
46 Otto 2016. 80.
47 Zannoni 2018. 300.
48 *Florindo de Almeida Vasconcelos Gramaxo v Portugal*, par. 116.

of Article 8(2) of the Convention and focused on an assessment of competing rights and interests made by the national courts. The assessment was conducted by examining, on the one hand, the employee's right to respect for his private life and, on the other hand, the right of his employer to control expenses arising from the use of company vehicles by employees.[49] In the course of proceedings before the national courts, greater force was attributed to the employer's right. However, the Portuguese Court of Appeal indicated that geolocation devices cannot be used to monitor the efficiency of employees or their compliance with working hours, as this would result in remote surveillance prohibited by Article 20 of the Portuguese Labour Code.[50] Thus, the court invalidated the data collected on the employee's work activity but, in contrast, found that the data on the number of kilometres travelled collected through the use of geolocation were lawful.[51] This position was confirmed by the ECtHR, which ruled that by taking into account only the geolocation data relating to the distances travelled, the Court of Appeal had limited the scope of the interference with the applicant's private life to what was strictly necessary to achieve the legitimate aim, namely, to monitor the company's expenditure.[52] That leads to the final conclusion that emerges from an analysis of cases decided by the ECtHR involving the issue of geolocation. Namely, in the situation where geolocation is used as a means of investigation (as in *Uzun v Germany* and *Ben Faiza v France*), its main focus is on a specific person and tracking their movement,[53] while in the context of an employment relationship (as in *Florindo de Almeida Vasconcelos Gramaxo v Portugal*), theoretically, the target of GPS monitoring can only be a work tool or other object entrusted by the employer to the employee. However, considering the above, the question is whether in *Florindo de Almeida Vasconcelos Gramaxo v Portugal* the actual limitation of GPS surveillance at the workplace to only the company vehicle the employee was using took place or not. The movement of a vehicle allows to read the movement of a driver, and the movement of a driver allows to draw conclusions about their life,[54] especially when this movement takes place in the time after work. In the present case, the employer was entitled to monitor his car used by the employee at work and after, 24 hours a day, seven days a week for three years.[55] During such a long period of intensive monitoring, the employer was able to acquire a lot of detailed data about the employee's private life. Therefore, the question raised above should be preliminarily answered in the negative.

49 Id. par. 115.
50 Id. par. 119.
51 Id. par. 119.
52 Id. par. 120.
53 *Uzun v Germany*, par. 49, 70.
54 Zannoni 2018. 311.
55 *Votum separatum in Florindo de Almeida Vasconcelos Gramaxo v Portugal*, par. 10.

3. Differences between Geolocation Monitoring and Other Forms of Monitoring in the Workplace

Since there are noticeable differences in the ECtHR's approach to the issue of workplace and non-employee geolocation, it is also important to consider whether the ECtHR's findings differ in the case of employee geolocation monitoring compared to other forms of workplace monitoring.

Similar to *Ben Faiza v France* and *Uzun v Germany*, in the *Florindo de Almeida Vasconcelos Gramaxo v Portugal* case the Court also distinguished between surveillance by geolocation and other methods applied in the workplace.[56] This last case is certainly distinguishable from the cases already examined by the Court concerning respect for private life in the context of employment relationships, since the information at issue was not images,[57] electronic messages,[58] or computer files[59] but geolocation data. Unfortunately, the Court did not indicate whether and, if so, which forms of workplace monitoring more or less violate Article 8 of the ECHR. Meanwhile, as already noted in the introduction, in deciding the *Florindo de Almeida Vasconcelos Gramaxo v Portugal* case, the ECtHR directly addressed geolocation monitoring in the workplace for the first time. Thus, it is now the sole reference point in this type of case. The ECtHR ruled only that the principles on employee video monitoring developed in other cases decided by the Court should apply *mutatis mutandis* to the *Florindo de Almeida Vasconcelos Gramaxo v Portugal* case.[60]

Referring to the already well-established line of case-law on video monitoring in the workplace, the ECtHR indicated that the national courts should have regard to the following factors when balancing the various interests at stake: (1) Has the employee been informed of the possibility of the employer taking surveillance measures and of the introduction of such measures?[61] (2) What was the extent of the surveillance carried out by the employer and the degree of intrusion into the employee's private life?[62] (3) Has the employer justified the use and extent of the surveillance on legitimate grounds?[63] (4) Was it possible to set

56 *Florindo de Almeida Vasconcelos Gramaxo v Portugal*, par. 93.
57 *Köpke v Germany*; *Antović and Mirković v Montenegro*; *Lopez Ribalda and Others v Spain*.
58 *Bărbulescu v Romania*.
59 Judgment of the ECtHR of 22 February 2022, *Libert v France*, Application No. 588/13.
60 *Florindo de Almeida Vasconcelos Gramaxo v Portugal*, par. 109.
61 While, in practice, this information may be communicated to employees in various ways, depending on the specific facts of each case, in principle, the warning must be clear about the nature of the surveillance and given before its implementation.
62 In this respect, particular consideration should be given to the degree of privacy of the place where the surveillance takes place, the spatial and temporal limits of the surveillance, and the number of people who have access to the surveillance results.
63 On this point, the more intrusive the surveillance, the more serious the justification required.

up a surveillance system based on less intrusive means and measures?[64] (5) What were the consequences of the surveillance for the employee who was subject to it?[65] (6) Has the employee been offered adequate safeguards, particularly where the employer's surveillance measures have been intrusive?[66]

The ECtHR generally concludes only with the guidance mentioned above, which may need to be revised when considering other factual situations related to geolocation monitoring in the workplace. In *Lopez Ribalda and Others v Spain*, the Court made it clear that, when analysing the proportionality of a form of employee surveillance, it is necessary to distinguish between the different places where the monitoring is installed (from the perspective of video monitoring, the expectation of respect for private life in the workplace should be very high in toilets or changing rooms, high in closed working areas such as offices, and lower in areas accessible to other employees or the general public).[67] Although in the case of any form of employee monitoring, any interference by the employer after working hours is in general excluded, from the perspective of the scope, place, and purpose of geolocation, controlling the location of an employee's company vehicle, parked in a place strictly designated by the employer (e.g. in front of the employee's house), should be considered legal in the light of Article 8 of the ECHR, when the employee may use such a vehicle after working hours only between the workplace and home. The purpose of such geolocation is only to protect the employer's property. In our opinion, since the employee cannot use the vehicle for any other purpose or route, there is no risk of excessive interference with the employee's right to privacy (even if the geolocalization is active 24/7).

As in the *Lopez Ribalda and Others v Spain* case, the justification in the *Florindo de Almeida Vasconcelos Gramaxo v Portugal* case also lacked extensive considerations on the impact of the unequal relationship between the employee and the employer (employee subordination) on maintaining a balance between their interests (in this case, given the use of geolocation monitoring in the workplace).[68]

Another important issue is the potential admissibility at the ECHR level of the employer's use of hidden geolocation monitoring in the workplace. In the oft-cited case of *Lopez Ribalda and Others v Spain*, the ECtHR pointed out that the requirement of transparency and the consequent right to information is

64 In this respect, it must be assessed based on the particular circumstances of each case whether the legitimate aim pursued by the employer could be achieved by less intrusive means.

65 In particular, it is important to check how the employer used the results of the surveillance measure and whether they served to achieve the stated aim of the measure.

66 These safeguards can be implemented, among other means, by informing the employees concerned or staff representatives about the introduction and extent of the surveillance, declaring the adoption of such a measure to an independent body or allowing them to complain. See also *Lopez Ribalda and Others v Spain*, par. 116.

67 *Lopez Ribalda and Others v Spain*, par. 125.

68 See also Barański 2020. 26–32.

fundamental, primarily through the prism of employment relationships in which the employer has significant powers over its subordinate employees; however, the provision of information to the monitored person and its extent constitute only one of the criteria to be taken into account in a given case when assessing the proportionality of the use of this form of employee control (in the absence of such information, the other criteria identified by the Court should be taken into account all the more).[69] Since the Court in the case of *Florindo de Almeida Vasconcelos Gramaxo v Portugal* signalled the legitimacy of using the jurisprudence on video surveillance, it would mean that it also allows, after meeting all strict assumptions and by way of exception, the legal use of hidden geolocation monitoring in the workplace. Undoubtedly, 'hidden monitoring threatens the information autonomy of the employee because, in such circumstances, the employee is deprived of the possibility to decide on the scope of information disclosed about himself'.[70] However, it cannot be overlooked that the issue of the admissibility of using monitoring in the workplace also includes issues related to the employer's needs to 'maintain broadly understood safety at work and protect property'.[71] In such circumstances, geolocation after working hours should be excluded each time. It also seems that the use of hidden geolocation monitoring, legally admissible under certain conditions, will not be conducive to proper cooperation and conflict-free relations between the employer and employees and between employees.[72]

In very specific factual circumstances of a given case, geolocation monitoring in the workplace may interfere much more with the employee's right to privacy than other forms of monitoring. The literature already raises the issue of implanting employees with subcutaneous chips, whose task may be, among others, geolocation.[73] Apart from the obvious controversies resulting from this, going far beyond the issues related to Art. 8 of the ECHR because of direct interference with human tissue, an implanted subcutaneous chip could, for example, protect the lives of miners by determining their location in real time, without the risk of losing the tracking device. In such a situation, compared to other forms of monitoring, geolocation monitoring in the workplace interferes much more with the right to privacy. Moreover, with such an assumption, through the prism of these other forms of monitoring, the ECtHR's potential conclusion would have to be even far different from the one expressed by the Tribunal in the previously analysed cases of *Ben Faiza v France* and *Uzun v Germany*, where geolocation technology was described as less interfering with the right to privacy compared

69 *Lopez Ribalda and Others v Spain*, par. 131.
70 Kuba 2019. 32.
71 Muszalski 2019. Art. 222, par. 1.
72 Barański 2016. 26–32.
73 Surdykowska 2023.

to other technologies. These issues are undoubtedly becoming a considerable challenge in the world of work and sooner or later will probably become the subject of adjudication before ECtHR.

When answering the question of whether there are differences between geolocation monitoring and other forms of monitoring in the workplace that would force a paradigm shift, as a rule, a negative answer should be given. ECtHR takes full advantage of the existing jurisprudence regarding video surveillance, which is sufficient in most cases. This also applies to restrictive geolocation monitoring after working hours to protect the employer's property or hidden geolocation monitoring. Therefore, the general legality criteria are common to all forms of monitoring. At the same time, it is possible to imagine situations where the determination of the legality of geolocation monitoring through the prism of Art. 8 of the ECHR will be specific enough to break the described general criteria and force a new approach to the issue (geolocation monitoring using microchips to protect life or health).

4. Conclusions

The existing line of ECtHR jurisprudence concerning the issue of geolocation as a surveillance measure includes three cases: *Uzun v Germany*, *Ben Faiza v France, and Florindo de Almeida Vasconcelos Gramaxo v Portugal.* However, the latter case constitutes a specific departure from the previous two rulings covering the non-employment sphere. Namely, in the *Uzun v Germany* and *Ben Faiza v France* cases, the Court classified geolocation-based techniques into the second category of surveillance methods that are less likely to violate a person's right to respect for their private life; therefore, in accordance with the view of the Strasbourg Court, the strict standards set up and applied in the specific context of surveillance of telecommunications will not be applicable to cases regarding surveillance via GPS. In turn, when ruling on geolocation monitoring in an employment context, the Court did not distinguish which forms of workplace surveillance infringe Art. 8 of the ECHR to a greater or lesser extent. Moreover, it indicated that the principles of employee video monitoring developed in other cases decided by the Court should apply *mutatis mutandis* to the *Florindo de Almeida Vasconcelos Gramaxo v Portugal* case.

However, the Court's specific equating of the criteria for the legality of geolocation monitoring with the legality criteria of other forms of employee monitoring evident in the *Florindo de Almeida Vasconcelos Gramaxo v Portugal* case does not mean that it shall apply to all factual circumstances involving geolocation monitoring in the workplace. Progressive technological development, including the advancement of devices that enable the monitoring of employees, may lead to a situation in

which geolocation surveillance in the workplace can interfere much more with the employee's right to privacy than other forms of monitoring. An example of this situation is the subcutaneous chips that can be implanted into employees and which allow to check their current localization.[74] The expansion and use of this type of technology, which is linked in the literature to the concept of digital Taylorism,[75] and the potential disputes that will arise on this ground may force the Court to set new criteria of legality and lead to the development of a separate line of jurisprudence covering the issue of geolocalization in the workplace.

Moreover, the need to treat the European Convention on Human Rights as a 'living instrument', whose provisions should be interpreted in accordance with present-day conditions,[76] was partially highlighted by the ECtHR itself. In *Kopke v Germany*, it ruled that 'the competing interests concerned might well be given a different weight in the future, having regard to the extent to which intrusions into private life were made possible by new, more sophisticated technologies'.[77]

In order to ensure the effective protection of employee's privacy and a fair balance of the employer's interests in the context of geolocation surveillance, the Court should consistently follow its previously adopted integrated approach[78] to the interpretation of the Convention's provisions, according to which there is no rigid separation of social and economic rights from the rights enshrined in the Convention.[79] An integrated approach enables the ECtHR to analyse Art. 8 of the ECHR in the light of the rules set out in the European Social Charter, which are of great relevance in relation to the employment sphere (e.g. the right to work, the right to dignity at work, or the right to just conditions of work).[80] This, in turn, provides the Court with a complete picture of the conflict between the employer's interests and the rights of the employee, the consideration of which is crucial for determining the reasonable scope of acceptable interference with the right to privacy in situations involving the use of geolocation surveillance methods in the workplace.

References

BARAŃSKI, M. 2020. Ukryty monitoring w zakładzie pracy w kontekście wyroku Europejskiego Trybunału Praw Człowieka z dnia 17 października 2019 r. (López Ribalda i inni v Hiszpania, skargi nr 1874/13 i 8567/13). *Monitor Prawa Pracy* 2020/3: 26–32.

74 Surdykowska 2023. 6.
75 See also: Otto 2022. 52; Brown–Lauder–Ashton 2010.
76 *Tyler v the United Kingdom*, Application No. 5856/72, 25 April 1978, par. 31.
77 *Köpke v Germany*, par. A(2).
78 Scheinin 2001. 32.
79 Mantouvalou 2005. 573; *Airey v Ireland*, Application No. 6289/73, 9 October 1979, par. 26.
80 Otto 2016. 88.

2021. Artificial Intelligence in the Workplace through the Prism of Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms. In: Martín, L. M.–Załucki, M. (eds), *Artificial Intelligence and Human Rights*. Madrid. 340–353.

BARAŃSKI, M.–GIERMAK, M. 2017. Protection of Employees' Geolocation Data in EU Law. In: Jankowska, M.–Pawełczyk, M.–Augustyn, S.–Kulawiak, M. (eds), *Earth Observation & Navigation. Law and Technology*. Warsaw. 199–210.

BROWN, P.–LAUDER, H.–ASHTON, D. 2010. Digital Taylorism. In: Brown, P.–Lauder, H.–Ashton, D. (eds), *The Global Auction: The Broken Promises of Education, Jobs, and Incomes*. Oxford.

GALETTA, A.–DE HERT, P. 2014. Complementing the Surveillance Law Principles of the ECtHR with Its Environmental Law Principles: An Integrated Technology Approach to a Human Rights Framework for Surveillance. *Utrecht Law Review* 10(1): 55–75. https://doi.org/10.18352/ulr.257.

HENDRICKX, F.–VAN BEVER, A. 2013. Article 8 ECHR: Judicial Patterns of Employment Privacy Protection. In: Dorssemont, F.–Lörcher, K.–Schömann, I. (eds), *The European Convention on Human Rights and the Employment Relation*. Oxford. https://api.semanticscholar.org/CorpusID:157298534 (accessed: 15.11.2023).

ILO. 1997. *Protection of Workers' Personal Data. An ILO Code of Practice*. Geneva. https://www.ilo.org/sites/default/files/wcmsp5/groups/public/%40ed_protect/%40protrav/%40safework/documents/normativeinstrument/wcms_107797.pdf (accessed: 09.11.2023).

JANKOWSKA, M.–PAWEŁCZYK, M. 2014. The Notion of Geospatial Information – Several Preliminary Remarks, Spatial Information and Public Information. In: Jankowska, M.–Pawełczyk, M. (eds), *Geoinformation Law and Practice*. Warsaw.

KUBA, M. 2019. Monitoring poczty elektronicznej pracownika – refleksje na tle nowych regulacji prawnych. *Praca i Zabezpieczenie Społeczne* 2019/11: 29–35.

MANTOUVALOU, V. 2005. Work and Private Life: Sidabras and Dziautas v Lithuania. *European Law Review* 2005: https://api.semanticscholar.org/CorpusID:144696139 (accessed: 15.11.2023).

MILLER, A. 2018. More Companies Are Using Technology to Monitor Employees, Sparking Privacy Concerns. ABCNews 10.03.2018. https://abcnews.go.com/US/companies-technology-monitor-employees-sparking-privacy-concerns/story?id=53388270 (accessed: 09.07.2023).

MUSZALSKI, W. (ed.). 2019. *Kodeks pracy. Komentarz*. Warsaw.

OTTO, M. 2016. *Right to Privacy in Employment – A Comparative Analysis*. Oxford–Portland (Oregon).

2022. A Step towards Digital Self- & Co-determination in the Context of Algorithmic Management System. *Italian Labour Law e-Journal* 15(1): 51–64. https://doi.org/10.6092/issn.1561-8048/15220.

SCHEININ, M. 2001. Economic and Social Rights as Legal Rights. In: Eide, A.–Krause, C.–Rosa, A. (eds), *Economic, Social and Cultural Rights*. 2nd edition. Dordrecht.

STEFAŃSKI, K. 2021. Employee Geolocation versus the GDPR. *Praca i Zabezpieczenie Społeczne* 2021/4: 14–17.

SURDYKOWSKA, B. 2023. O lęku przed nadciągającym chipowaniem pracowników – uwagi na tle powstającego ustawodawstwa w USA. *Z Problematyki Prawa Pracy i Polityki Socjalnej* 2023/21: 1–15.

ZANNONI, D. 2018. GPS Surveillance for the Perspective of the European Convention on Human Rights. *European Criminal Law Review* 8: 294–312. https://doi.org/10.5771/2193-5505-2018-2-294.