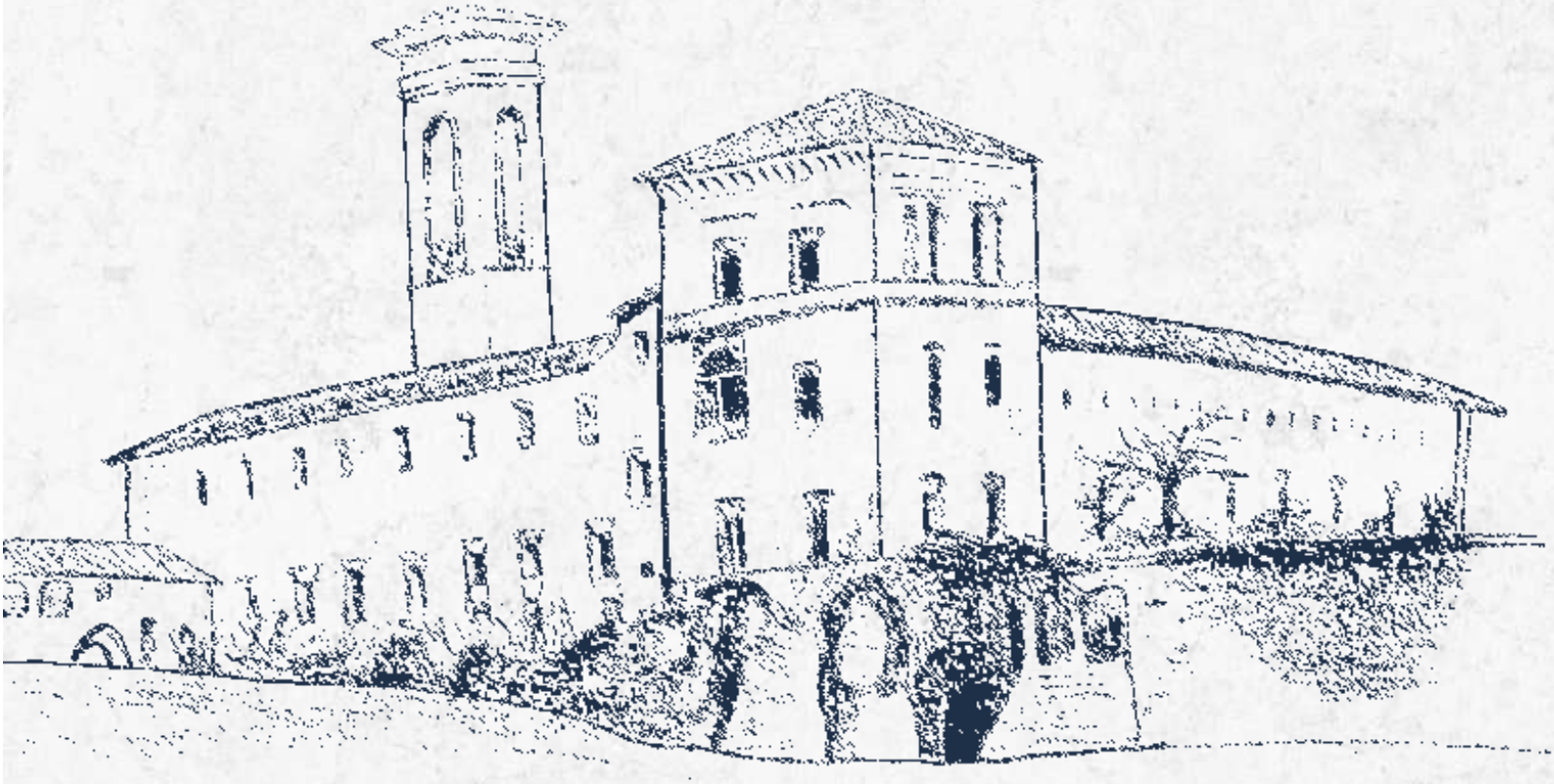
OPEN ACCESS
ISSN 2280-4056

E-Journal of International and Comparative

LABOUR STUDIES

Volume 12 No. 03/2023



ADAPT UNIVERSITY PRESS
www.adapt.it

E-Journal of International and Comparative **LABOUR STUDIES**

ADAPT *International School of Higher Education in Labour and Industrial Relations*

E-Journal of International and Comparative

LABOUR STUDIES

Volume 12 No. 03/2023

ADAPT UNIVERSITY PRESS
www.adapt.it

Online Publication of the ADAPT Series
Registration No. 1609, 11 November 2001, Court of Modena
www.adaptbulletin.eu

Covert Surveillance at the Workplace and the ECtHR Approach: Possible Risks of Breaching GDPR Rules

Aljoša Polajžar [*]

Abstract: This paper addresses the issue of (im)permissibility and consequences of covert surveillance at the workplace – from ECtHR case law and GDPR perspective. In the first part the relevant ECtHR case law is examined. It follows that covert surveillance at the workplace is (under certain conditions) compliant with Article 8 ECHR – although the developments in ECtHR reasoning from case *Köpke* (2010) to case *Lopez Ribalda* (2019) show a more stringent ECtHR approach towards covert surveillance. Moreover, ECtHR itself highlighted in *Lopez Ribalda* (where there was no violation of Article 8 ECHR) that workers had (and should have resorted to) other available administrative, civil and criminal procedures (besides the employment dispute) to protect their right to personal data.

Keywords: *Labour law; ECHR; GDPR; Worker's right to personal data protection; covert surveillance.*

1. Introduction

The development of information and communication technology (ICT) has brought numerous new possibilities for employers to control workers at the workplace.[1] As has already been extensively discussed in literature the surveillance of a worker constitutes an interference with the worker's

[*] Researcher at University of Maribor, Faculty of Law (Slovenia). Email address: aljosa.polajzar@um.si.

[1] See: Bhave, Devasheesh, Laurel, Reeshad 2020; Edwards, Martin, Henderson, 2018; Katsabian, 2019.

right to personal data protection.[2] Therefore, the main problem (especially for employers) is where to draw the line between lawful and unlawful monitoring (surveillance).

In the European regional legal framework (Council of Europe and the EU) the most important standards for assessing the limits of permissible monitoring stem, inter alia, from the European Court of Human Rights (hereinafter: ECtHR) case law and from the provisions of the General Data Protection Regulation[3] (hereinafter: GDPR). Both ECtHR case law relating to worker's personal data (privacy) protection[4] and the provisions of GDPR setting important safeguards for workers personal data protection[5] were extensively discussed in literature.

However, gaps in legal science and case law (both ECtHR and Court of Justice of the European Union (hereinafter: CJEU)) remain. A very important issue (up to now neglected in legal science) is the interplay between the standards (and outcomes) set in ECtHR case law and requirements of personal data protection under GDPR. This is particularly evident in case of covert monitoring (where the worker has not been informed of the monitoring in advance) at the workplace.

On the one hand (as it will be shown in the analysis within this paper), ECtHR has already decided that the exercise of covert monitoring of a worker at the workplace does not, in certain circumstances, constitute a violation of Article 8 (right to private life) of European Convention on Human Rights[6] (hereinafter: ECHR).[7] On the other hand, it is problematic in practice whether such results of ECtHR judgments (no violation of Article 8 ECHR) can guarantee the employers that they will not face legal consequences for breaches of GDPR due to covert monitoring. The provisions of GDPR apply directly and uniformly throughout the EU, thus it is any case essential that any (covert) surveillance complies also

[2] See, *inter alia*: Atkinson, 2018; Eichenhofer, 2016; Eklund, 2019.

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119.

[4] See: Bagdanskis, Sartatavičius, 2012; Calomme, 2017; D'Aponte, 2021; Klein, 2018; Kaiser, 2018; Lockwood, 2018; Stanev, 2019; Turanjanin, 2020.

[5] See: Brkan, 2017; Dimitrova, 2020; Halefom, 2022; Keane, 2019; Munteanu, Povey, 2022; Ogriseg, 2017; Sychenko, Chernyaeva, 2019.

[6] European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), 1950, as amended by Protocols Nos. 11, 14, 15 and supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13 and 16.

[7] See Dimitrova, 2020; Turanjanin, 2020.

with the provisions of GDPR (and not only with Article 8 ECHR). Nonetheless, in this respect it is especially problematic (for employers in practice) that so far, no judicial decisions about worker's personal data protection (in the context of covert surveillance and GDPR) have been adopted by CJEU.

Consequently, the thesis of the paper is that even if the covert surveillance at the workplace (conducted by the employer) does not under certain criteria (developed by ECtHR) violate Article 8 ECHR – this does not guarantee the employer that its exercise of the very same covert surveillance will not be found in violation with GDPR, and thus subject to legal consequences (e.g. administrative fines) under GDPR. Rather than ECtHR's case law standards (which interpret the ECHR), the key to ensuring legal certainty (for employers) in the exercise of covert surveillance in the workplace is the compliance of such surveillance with GDPR.

The main expected outcomes of this paper are, firstly, to critically evaluate the content and legal importance of the existent ECtHR case law on covert monitoring at the workplace. And secondly, to emphasise the importance of refocusing worker's personal data protection (above the national level) merely from the framework of the interpretation of Article 8 by ECtHR towards the EU law framework with CJEU as the main actor for interpretation of the relevant provisions of GDPR. Thus, cases concerning worker's personal data protection are to be more often referred to CJEU as question for preliminary ruling (instead of only individual complaints before ECtHR being launched).

The paper's scope will be limited to the analysis of selected legal sources connected to worker's personal data protection.[8] Within the legal

[8] At the outset, it is worth explaining that Article 8 ECHR (Right to respect for private and family life) covers various aspects of the protection of the personality rights and privacy of the worker. From the right to protection of worker's private sphere, spatial privacy, to communication privacy and the right to protection of personal data. In the case law under review (the context of covert workplace surveillance) ECtHR addresses the issue under the notion of "worker's privacy protection" (including both communication privacy, and personal data protection in the same term). Covert surveillance (for example video-surveillance) also involves the processing of the worker's personal data. In the context of this article, we will limit the research scope to ECtHR case law and GDPR provisions related to worker's personal data protection (and not other aspects of privacy (e.g., communication privacy) under EU law). Therefore, from the terminological point of view we will primarily focus on the right to personal data protection, except for cases where "worker's privacy protection" concept (covering also worker right to protection of personal data) is used within ECtHR case law.

framework of the Council of Europe relevant ECtHR case law will be analysed. Within the EU legal framework only the relevant GDPR provisions will be analysed – due to currently non-existent CJEU judgments regarding worker's personal data protection (in the context of GDPR).

Methodologically, the paper will be based on the normative-dogmatic method and the methods of analysis and synthesis. The selected judgments of ECtHR relating to the protection of the worker's personal data (workplace surveillance) will be analysed in detail. The possible limitations or inconsistencies of ECtHR approach – which may cause uncertainties regarding applicable legal standards and legal consequences of covert monitoring for employers – will be highlighted. Furthermore, case law and the issues at stake will be set in the context of the provisions of GDPR, which impose a number of obligations on employers as data controllers in relation to the processing of personal data[9], as well as legal consequences in the event of breaches.

First part of the paper will thus present the relevant excerpts of ECtHR case law on the (im)permissibility of covert surveillance at the workplace. Second part will present selected relevant provisions of GDPR in this respect – including employer's obligations, and legal consequences for infringing provisions of GDPR. Third part will be devoted to a critical discussion and analysis of the presented legal aspects relating to the exercise of covert surveillance at the workplace in light of the presented ECtHR case law, GDPR provisions, and the above set aims of the paper.

2. ECtHR case law on covert surveillance at the workplace

At the outset, the ECHR contains a list of fundamental human rights that are subject to dynamic and evolving interpretation by ECtHR in light of evolving social conditions and ideas.[10] By deciding specific cases, ECtHR has an indirect influence on the consolidation of human rights standards between Contracting States, especially in light of their diverse legal systems.[11] Furthermore, *Sychenko* & *Chernyaeva* note that ECtHR judgments have a significant impact on the level of protection of the worker's personal data.[12]

[9] See: Voigt, von dem Bussche, 2017.
[10] Schabas, 2015, pp. 1, 48.
[11] Stone Sweet, Keller, 2008, p. 3.
[12] Sychenko, Chernyaeva, 2019, p. 172.

ECtHR has dealt with some important cases concerning the interpretation of Article 8 ECHR (Right to respect for private and family life) in cases of employer's (covert) surveillance of workers at the workplace. We will analyse the relevant case law according to the type of covert monitoring. Therefore, the relevant case law can be divided into two main groups. The first group includes cases where the usage of electronic work equipment (computer, telephone, internet usage etc.) has been covertly monitored. The second group includes cases where the employer has carried out covert video surveillance in the workplace.

2.1. Covert monitoring of electronic work equipment usage (computer, telephone, internet usage)

In the first three judgments presented in this section (*Halford*, *Copland* and *Barbulescu*), ECtHR ruled that the covert exercise of surveillance constituted a violation of the worker's right to private life under Article 8 ECHR. Nonetheless, in the *Libert* case, ECtHR ruled that the covert surveillance did not constitute a violation of Article 8 ECHR.

2.1.1. *Halford v United Kingdom*

In *Halford v UK* the complainant alleged that the interception of telephone conversations (made on a work telephone) constituted a violation of Article 8 ECHR. The employer had not imposed any internal rules or restrictions on the use of work telephones, or otherwise alerted the worker to the fact that her communications might be subject to surveillance. This is also why the worker had a reasonable expectation of privacy in her use of the telephone. ECtHR expressly rejected the respondent State's argument that the worker did not enjoy a "*reasonable expectation of privacy*" on the work phones and that the employer (as the owner of work equipment) was, therefore, entitled to monitor worker's calls even without worker's knowledge or consent (covert surveillance). Even in these cases, the worker is protected by Article 8 of the ECHR, as ownership of work-related resources/equipment is irrelevant.[13]

[13] ECtHR, *Halford v the United Kingdom*, Case No. 20605/92, ECLI:CE:ECHR:1997:0625JUD002060592, paras. 16, 43-45.

2.1.2. *Copland v United Kingdom*

In *Copland v UK* the employer (public sector) exercised control over the worker's work telephone, email, and internet use. The monitoring had no legal basis in internal rules or legislation. The monitoring was carried out for the purpose of checking whether the worker was using work equipment excessively for private purposes. For this purpose, the employer collected data on telephone calls and websites visited (date, time of visit, etc.). The monitoring of telephone use was carried out for 18 months and of internet use for 2 months. In its reasoning, ECtHR confirmed that as in *Halford,* it was decisive that the worker had not received any warning that her use of work resources would be subject to surveillance (there were no internal rules at the employer), and therefore enjoyed a reasonable expectation of privacy. However, it is worth noting that, as a guide for the future, ECtHR has stated that it does not exclude the possibility that control over a worker's use of the telephone, email or internet may be permissible under certain conditions (proportionality and legitimate aim).[14]

2.1.3. *Barbulescu v Romania*

The case represents the first time ECtHR has dealt with the monitoring by technical means (by a private sector employer) of the content of the worker's electronic communications. On the first instance ECtHR ruled (by 6 votes to 1) that there had been no violation of Article 8 ECHR (Eklund, 2019).
The Grand Chamber of ECtHR then reversed the above decision and ruled (by 11 votes to 6) that there had been a violation of the worker's right to private life under Article 8 ECHR. In the proceedings before ECtHR, the complainant alleged that his employer's dismissal was based on a violation of his right to private life. As the national courts failed to declare such dismissal unlawful, and thus protect his rights, Romania is liable for breach of Article 8 ECHR for failure to fulfil its obligations.[15]
The worker was employed by a private company and used a "Yahoo Messenger" work account for his work. The employer had internal rules governing the use of company equipment. Article 50 of those rules

[14] ECtHR, *Copland v the United Kingdom*, Case No. 62617/00, ECLI:CE:ECHR:2007:0403JUD006261700, paras. 7, 10-11, 15, 41, 46.
[15] ECtHR, *Barbulescu v Romania* (Grand Chamber), Case No. 61496/08, ECLI:CE:ECHR:2017:0905JUD006149608, para. 3.

provided that any disturbance of the peace and discipline at the workplace was strictly prohibited, in particular the use of computers, printers and telephones for private purposes. The same rules did not contain any other provisions stipulating that the worker's use of ICT resources could be monitored. To this end, the employer prepared a circular reminding workers that it (as employer) had a duty to supervise their work and to take punitive action against infringers, and would therefore supervise and punish any potential infringers. The worker has signed two documents acknowledging that he is aware of both the internal rules and the latter circular. This was followed by the monitoring of the worker's communication via the company computer. The employer recorded the content of the worker's communications, accumulating a total of 45 pages of content over the eight days of monitoring (5 of the processed messages were also sent from the worker's private Yahoo account). Some of the messages were of an intimate nature, exchanged with the worker's fiancee and brother. After the worker was informed of the evidence gathered, his dismissal followed (in August 2007), which the worker unsuccessfully challenged before the national labour courts.[16]

ECtHR stressed the particular importance of the fact that the case concerns an interference with privacy in the context of an employment relationship, since the latter is a specific form of contractual relationship based on the legal subordination of the worker. Therefore, the State is obliged to protect the worker against the possibility of abuse of the employer's control of communications by means of appropriate safeguards.[17]

Within judgment's reasoning ECtHR has created abstract criteria or factors that national courts must take into account when assessing the limits of the permissibility of surveillance of a worker. It is important to consider:

- the existence of a notice to the worker that the monitoring is being carried out. To comply with Article 8 ECHR, such notice must be clear and given in advance;
- the extent of the surveillance and the degree of interference with the worker's privacy. In this respect, a distinction should be made between monitoring the flow of communication (traffic data) and monitoring the actual content of the communication. It is also important whether there is continuous monitoring of all

[16] Ibidem, paras 11-17, 21, 23.
[17] Ibidem, paras. 117, 120.

communications or only intermittent monitoring of individual messages;
- the existence of legitimate interests for conducting the monitoring. In particular, the reasons for monitoring the content of the communication must be justified;
- the existence of other monitoring options that meet the employer's objectives without controlling the content of the communications (existence of less intrusive measures);
- the consequences of the monitoring for the worker (what the employer will do with the information obtained from the monitoring);
- the existence of adequate safeguards to protect worker's privacy, in particular the prohibition on the employer from knowing the content of the communication unless the worker has been informed in advance of this possibility.[18]

By applying the above mentioned criteria to the case at hand the ECtHR concluded that the employer attempted to justify the surveillance by arguing that the surveillance was necessary to protect against liability for possible unlawful acts of workers on the Internet, to prevent the leakage of business secrets and to ensure the security of the information system. However, in ECtHR's view, all these reasons were of a hypothetical or theoretical nature, as there was no evidence that the complainant had endangered the undertaking in any of these ways. It is therefore doubtful whether these grounds justify strict control over the content of the communications. Less invasive measures might be sufficient, which would be for the national courts to decide. Furthermore, in ECtHR's view, the advance notification did not meet the required standards, since the internal rules and the circular did not make it clear that the employer would be able to inspect the content of worker's communication.[19] For all the above reasons, the ECtHR held that the strict surveillance (flow and content) of the worker's communications via Yahoo messenger was impermissible and that Romania was liable for violating Article 8 ECHR by failing to ensure that the worker's right to privacy was adequately protected.[20]

Lastly, and very importantly, the judgment touch upon the conceptual issue according to which Contracting States have a wide margin of discretion to protect worker's right to a private life. In ECtHR's view,

[18] Ibidem, para. 121.
[19] Ibidem, paras. 133-137.
[20] Ibidem, paras. 140-141.

these measures do not necessarily have to be solely in the context of labour law, but can also be in the context of civil, criminal law etc. It is therefore necessary to make a comprehensive assessment of whether a particular State had an adequate legislative framework to protect the right to (communicative) privacy of the worker vis-à-vis the employer.[21] And precisely this aspect was the main argument of the dissenting judges in their dissenting opinion, in which they took a closer look at the protection of worker's privacy (personal data) in the Romanian legal system. They argued that labour courts, which adjudicate on the unlawfulness of dismissals, were not the only option available to the worker. Firstly, from a criminal law perspective, the worker could have brought proceedings for the criminal offence of breach of secrecy of communications. Secondly, the legislative framework on the protection of personal data allowed the worker to report the matter to the supervisory authority and also to initiate a claim for damages for breaches of the legislation on the protection of personal data. Thirdly, the general rules of civil law also allowed for a claim for damages for the harm caused by unlawful conduct. The judges, therefore, considered that the worker should have also availed himself of these other legal possibilities, rather than focusing solely on challenging the lawfulness of the dismissal in the context of an employment dispute. The present judgment should, consequently, not be understood as a request to Contracting States that labour courts assume a protective role for cases where there are also more specialised remedies available to workers – for example, proceedings for breaches of data protection provisions under GDPR, etc.[22]

2.1.4. *Libert v France*

In *Libert v France* the worker claimed that there had been a violation of Article 8 ECHR due to the opening of his files stored on his work computer (without his knowledge and prior notification). The ECtHR ruled by 6 votes to 1 that there had been no violation of Article 8 ECHR. The worker was employed by the French National Railway Company (a State-owned company). On the day of his return to work, the worker was informed that his computer had been seized by the employer. At a meeting in the following days, the employer informed him that a large

[21] Ibidem, paras. 113, 116.
[22] ECtHR, *Barbulescu v Romania* (Grand Chamber), joint dissenting opinion of Judges Raimondi, Dedov, Kjølbro, Mits, Mourou-Vikström and Eicke, Case No. 61496/08, ECLI:CE:ECHR:2017:0905JUD006149608, paras. 9, 12, 17, 26.

amount of pornographic material (pictures and films) were found on the hard drive of the company computer in a folder (entitled '*fun*'). The employee was neither present at the surveillance carried out nor informed of it.[23]
The employer had internal rules regarding the use of the company's IT system, which allowed the use of company equipment for work purposes only. The rules provided that occasional and reasonable use of e-mail and internet for private purposes was permissible. In doing so, the rules stipulated that private information (files and folders on the computer) must be clearly marked as 'private'.[24]
ECtHR concluded that the interference was legally foreseeable and in conformity with the law. According to ECtHR, the general statutory provisions of French law, in the light of national case-law, allowed the employer, under certain conditions, to open files stored on the disk of the worker's work computer. Secondly, the interference pursued a legitimate aim since the employer has a legitimate interest in the use of the company equipment for work purposes because of the need to ensure the smooth running of the work process. To this end, they may put in place control mechanisms to check that workers are diligently and conscientiously fulfilling their obligations under the employment relationship.[25] And lastly, the worker had failed to properly mark (in accordance with the employer's internal rules) the folder or files on the hard drive as "*private*". ECtHR thus held that there had been no violation of Article 8 ECHR.[26]

2.2. Covert video surveillance in the workplace

The admissibility of covert video surveillance in the workplace has been dealt with in cases *Köpke v Germany* and *Lopez Ribalda and Others v Spain*. Moreover, and very importantly, in both cases ECtHR ruled that the covert surveillance did not constitute a violation of Article 8 ECHR.

2.2.1. *Köpke v Germany*

In *Köpke v Germany,* the worker alleged that covert video surveillance carried out by a detective agency on behalf of his employer violated his

[23] ECtHR, *Libert v France*, Case No. 588/13, ECLI:CE:ECHR:2018:0222JUD000058813, paras. 7, 9, 12.
[24] Ibidem, para. 19.
[25] Ibidem, paras. 38-41, 44, 46.
[26] Ibidem, paras. 51-53.

right to private life under Article 8 ECHR. ECtHR dismissed the claim as inadmissible (manifestly unfounded, see Article 35 ECHR). The worker was employed in a German department store (private sector). The employer had commissioned a detective agency to carry out video surveillance in part of the store because of suspicions of theft of products. After carrying out the covert surveillance and processing the data, the agency produced a report which led to the worker's dismissal due to shoplifting.[27]

ECtHR considered whether the German courts had struck the right balance between the worker's right to privacy (Article 8 ECHR) and the employer's interest in protecting private property (Article 1 to Protocol 1 ECHR). Importantly, the reason for the covert video surveillance was to verify the veracity of a reasonable suspicion that the worker had committed a criminal offence. It is the requirement of reasonable suspicion that is an important safeguard for the worker. This is precisely why it is important to enable the employer to gather evidence that will enable him to prove the criminal conduct of the worker and thus effectively protect his rights. ECtHR goes on to note that there were no other equally effective, less invasive measures available to the employer to protect its assets. Supervision by a supervisor, co-workers or transparent video surveillance are not sufficiently effective measures to detect this type of theft.[28]

Interestingly, ECtHR has explicitly stated that it allows for the possibility that the conflicting interests of the worker and the employer may be given a different weight in the future (in the light of the intrusion into worker's private life by new advanced technologies).[29]

2.2.2. *Lopez Ribalda and Others v Spain*

The mentioned ECtHR openness to a different approach can be seen in the more recent case of *Lopez Ribalda and Others v Spain*, which is factually essentially the same to the *Köpke* case. Not only did ECtHR not declare the complaint manifestly unfounded and dismiss it (as in *Köpke* according to Article 35 ECHR), but it even upheld the workers' claim at first instance (Chamber), ruling (by 6 votes to 1) that there had been a

[27] ECtHR, *Köpke v Germany*, Case No. 420/07, ECLI:CE:ECHR:2010:1005DEC000042007 (the judgment is not divided into paragraphs).
[28] Ibidem.
[29] Ibidem.

violation of Article 8 ECHR as a result of the covert video surveillance. Nonetheless, the Grand Chamber reversed this decision and ruled by 14 votes to 3 that there had been no violation of worker's right to private life under Article 8 ECHR.[30]

The workers were employed as salesclerks in a department store (private sector). The employer had launched an internal investigation and, as part of it, a covert video surveillance, due to the unexplained disappearance of goods (total value of approximately 80.000 EUR). After ten days of surveillance, the employer realised that the goods were being stolen by its workers and terminated the employment contracts of fourteen workers.[31]

ECtHR applied the criteria developed in *Barbulescu v Romania (*see above) in order to find a fair balance between the interests of the workers (protection of personal data, privacy) and the employer (protection of property).[32]

In the judgment ECtHR recognised the international validity and importance of the right to be informed about the exercise of (video)surveillance. The latter is particularly relevant in the context of employment relationships, as the employer is in a position of dominance vis-à-vis workers and potential abuses of dominance must be prevented. However, ECtHR points out that the requirement to give notice of the implementation of video surveillance is only one of the criteria to be taken into account when assessing the proportionality of a measure in a given case. In the absence of such notification, the assessment of the safeguards arising from the other criteria will be all the more important. This means that the absence of this prior notification can only be justified if there is an "overriding reason" to protect a public or private interest.[33]

As regards the other criteria, in the light of the disappearance of goods in recent months, there was a legitimate interest to protect employer's property. The surveillance was also appropriately limited in space and time (it lasted 10 days and until the thieves were discovered). Very importantly, ECtHR emphasised that the shop workers *enjoyed a low expectation of privacy. The* latter is very high in enclosed spaces (e.g. offices), but significantly lower in spaces (e.g. the shop) accessible to other workers, the public, etc.

[30] ECtHR, *Lopez Ribalda and Others v Spain* (Grand Chamber), Case Nos. 1874/13 and 8567/13, ECLI:CE:ECHR:2019:1017JUD000187413.
[31] Ibidem, paras. 10-16.
[32] Ibidem, paras. 116, 118, 122.
[33] Ibidem, para. 133.

Therefore, the interference with the right to privacy did not reach a high level of seriousness.[34]

Finally, and very importantly, ECtHR points out that the complainants had a number of other safeguards available to them under the domestic legal order, which they did not avail themselves of. They could have brought a claim for damages for breach of the law governing the protection of personal data and could have lodged a complaint with the competent supervisory authority, which could have imposed a fine on the employer. In this respect, ECtHR confirms the view (first expressed in *Barbulescu* case) that the protection of a worker's privacy can also be achieved through civil, administrative and criminal law rules – and not just through labour law. Accordingly, there has been no violation of Article 8 ECHR.[35]

The judges in the dissenting opinion focused on the question of the necessity of the monitoring. According to the dissenting opinion the employer has not yet exhausted all the possibilities for protecting its rights. He has not reported the thefts or the offences to the police, which, as the competent authority, would have carried out an investigation. The employer thus stepped into the shoes of the law enforcement authorities and carried out their tasks on its own using covert methods. Nor does the need to investigate a violation (crime) on the basis of the existence of a reasonable suspicion justify this type of covert private surveillance (investigation). The judges considered that the existence of "reasonable suspicion" as a condition for the imposition of surveillance is an important but not a sufficient safeguard. For example, a requirement for confirmation of the existence of reasonable suspicion by a third party could be an important additional procedural safeguard. In light of the increasing role and capacity of technology in today's society, individuals cannot afford to take justice into their own hands (with the help of technology). This must be prevented by a predictable legal framework with appropriate safeguards.[36]

[34] Ibidem, paras. 124-126.
[35] Ibidem, paras. 135-136.
[36] ECtHR, *Lopez Ribalda and Others v Spain* (Grand Chamber), joint dissenting opinion of Judges Gaetano, Grozev, and Yudkivska, Case Nos. 1874/13 and 8567/13, ECLI:CE:ECHR:2019:1017JUD000187413, paras. 9, 11, 15.

3. The EU (GDPR) legal framework and worker's personal data protection

At the outset, within the EU law legal framework CJEU plays a very important role, as it is the only court with the power to interpret EU law. Through its interpretation of EU law, CJEU ensures that secondary law (e.g. GDPR) is compatible with primary EU law (e.g. EU Charter of Fundamental Rights[37] etc.). Therefore, CJEU also plays an important role in the protection of human rights.[38] In this context the preliminary ruling reference procedure under Article 267 of the Treaty on the Functioning of the European Union[39] (hereinafter: TFEU) is of particular importance.[40] In contrast to the system of protection under the ECHR, an individual has no right of individual appeal to CJEU after exhausting all national remedies.[41]

3.1. Safeguards for worker's personal data protection under GDPR

At the outset, as Article 1 of GDPR makes clear, its purpose is to protect the fundamental rights and freedoms of individuals and, in particular, their right to the protection of personal data. Also, recital 4 confirms that GDPR respects all fundamental rights recognised by the EU Charter of Fundamental Rights, in particular respect for private and family life and communications, the protection of personal data and the freedom of economic initiative.

3.1.1. Fundamental principles of data processing

Article 5, paragraph 1, point a, of GDPR sets out the fundamental principles relating to the processing of personal data. First, personal data must be processed lawfully, fairly and transparently. The requirement of lawfulness of processing is specified in Article 6 GDPR, according to which processing is lawful only where the conditions in the enumerated cases set out in that Article are met. The transparency of processing is specified, inter alia, in Article 12 GDPR, which imposes an obligation on the controller (employer) to provide individuals (workers) with all

[37] Charter of Fundamental Rights of the European Union, OJ C 326.
[38] Trstenjak, Brkan, 2012, pp. 121-122, 128.
[39] Treaty on the Functioning of the European Union, OJ C 326, 26. 10. 2012.
[40] Lenaerts, Maselis, Gutman, 2014, p. 48.
[41] Letnar Černič, 2015, p. 81.

information relating to the processing in a concise, transparent, plain, easily accessible, and comprehensible form. Article 14 GDPR requires, inter alia, the provision of information on the purposes of and the legal basis for the processing of the personal data. As confirmed by the Article 29 Data Protection Working Party (2017a) all the above applies also in the context of workplace surveillance, as workers must be informed in advance of the existence of surveillance and other relevant information in this respect.[42]

3.1.2. Data processing impact analysis (DPIA)

As outlined by the Article 29 Data Protection Working Party guidelines (2017b) the so-called data processing impact analysis is a preventive process aimed at describing actions, assessing the necessity and proportionality of processing. It helps to manage the risks to the protection of human rights (of workers) arising from the processing of personal data. It is also helpful for employers as it demonstrates due diligence prior to the implementation of control systems through the DPIA. It is important that employers carry out a DPIA before they start to carry out any monitoring or processing. The implementation of a DPIA can also help to increase the confidence of the persons (e.g., workers) whose data is being processed. Failure to carry out or incorrectly carrying out a DPIA (and the resulting unlawful processing of personal data) may lead to payment of heavy administrative fines. In this context it is important to point out that according to Article 29 Data Protection Working Party guidelines (2017b) the DPIA will likely to be required (mandatory) before introducing surveillance systems at the workplace.[43]

3.1.3. Administrative fines for GDPR infringements

An important feature of GDPR are the extremely high administrative fines, which in themselves have a deterrent effect on potential infringers.

[42] Article 29 Data Protection Working Party, Working document on the surveillance of electronic communications in the workplace, No. 5401/01/EN/Final WP 55, 2002, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp55_en.pdf (accessed March 13, 2023), p. 8.

[43] Article 29 Data Protection working party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, No. 17/EN, WP 248, 2017b, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 (accessed March 13, 2023), pp. 4, 9-12, 14, 19.

Under Article 83, paragraph 1 GDPR, the general principle applies that administrative fines must be dissuasive, proportionate, and effective in each individual case. Under Article 83, paragraph 5 GDPR, fines (up to 20,000,000 EUR or, in the case of an undertaking, up to 4% of the total worldwide annual turnover) are imposed for infringements of the basic principles of processing (see Article 5 GDPR), lawfulness of processing (see Article 6 GDPR), provisions on consent (see Article 7 GDPR), and most importantly for infringing, inter alia, the right to prior notification and information (which is not fulfilled in covert monitoring) in accordance with the transparency principle under Articles 12 to 14 GDPR. Moreover, failure to carry out a mandatory DPIA or to consult the supervisory authority, as well as carrying out a DPIA in an incorrect manner, may also result in fines for companies or employers of up to 10,000,000 EUR or up to 4% of the total worldwide annual turnover.[44] GDPR thus introduces heavy fines for virtually any breach of its provisions. As stated by *Grentzenberg* & *Kirchner* (2019) these new rules have a strong deterrent effect, forcing companies to implement GDPR properly. Given these high financial risks (potential fines), it is essential that companies are able to confirm their compliance with GDPR rules with appropriate documentation (including when carrying out surveillance of workers).[45]

3.2. GDPR and covert monitoring at the workplace

CJEU has not yet ruled on whether it would be permissible (under GDPR) to carry out covert surveillance (data processing without prior notification) under specifically justified circumstances. In this context, it is worth pointing out that a particularly relevant interpretation would be that of Article 14, paragraph 5, point b GDPR, which is a potential legal basis for a possibility to derogate from the obligation to priorly inform the employee about the processing of his or her personal data. According to the said legal provision paragraphs 1 to 4 (Article 14 GDPR) shall not apply "*in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing.*" Nonetheless, without CJEU case law on the matter (of covert surveillance at the workplace) it remains uncertain in which possible cases this exception could apply. This is even more so, given the development

[44] See ibidem, p. 4.
[45] Grentzenberg, Kirchner, 2019, p. 146.

of the content of the guidelines by the GDPR supervisory authorities, which will be presented below.

The transparency principle (prior notification and giving all the necessary information regarding the data processing – surveillance) is emphasised in all relevant documents of the Article 29 Working party and the European Data protection Board related, inter alia, to processing of personal data (surveillance) at the workplace.[46]

Moreover, a very interesting development – similar to the apparent progression of ECtHR case law towards more emphasis on worker's personal data (privacy) protection in the more recent *Lopez Ribalda* case (2019) versus the *Köpke* case (2010) – can also be seen in the development of the opinions of the Article 29 Working Party and the European Data Protection Board. If the Article 29 Working Party opinion (from year 2002), still allowed the possibility of carrying out covert surveillance in the workplace under certain justified grounds[47] – the newer Article 29 Working party guidelines (form year 2017) no longer mention the possibility of derogating from the principle of transparency by carrying out covert surveillance. Instead, in that section of the latter newer guidelines it is written: *"with new technologies, the need for transparency becomes more evident since they enable the collection and further processing of possibly huge amounts of personal data in a covert way*."[48] Similarly, the most recent European Data Protection Board (from year 2020) guidelines on processing of personal data through video devices (covering also the employment context) do not mention at any point any exception or possibility to carry out covert surveillance in the workplace (the topic of covert surveillance is not expressly addressed – only the rules on transparency of processing are emphasised).[49]

---

[46] See Article 29 Data Protection Working Party, 2002, op. cit., p. 14; A Article 29 Data Protection Working Party, Opinion 2/2017 on data processing at work, No. 17/EN WP 249, 2017a, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169 (accessed March 13, 2023), p. 8; European Data Protection Board, Guidelines 3/2019 on processing of personal data through video devices, Version 2.0, Adopted on 29 January 2020, 2020, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en (accessed March 13, 2023), p. 26.

[47] Article 29 Data Protection Working Party, 2002, op. cit., p. 14 (point 3.1.3. "Transparency").

[48] Article 29 Data Protection Working Party, 2017a, op. cit., p. 8 (point 3.1.2. "Transparency").

[49] See European Data Protection Board, *op. cit.*, pp. 26–27.

4. Analysis and discussion

In relation to presented ECtHR case law on covert monitoring at the workplace and relevant GDPR provisions the following observations may be made.

First, as can be seen from the *Köpke* and *Lopez Ribalda* cases, the exercise of covert surveillance can be in compliance with Article 8 ECHR. Indeed, ECtHR also explicitly stresses the importance of transparency (prior notification) in the criteria it has developed. However, ECtHR points out that the requirement to give notice of the implementation of video surveillance is only one of the criteria to be taken into account when assessing the proportionality of a measure in a given case. In the absence of such notification, the assessment of the safeguards arising from the other criteria will be all the more important. This means that the absence of this prior notification can only be justified if there is an "overriding reason" to protect a public or private interest.[50] Important abstract criteria for assessing such cases were already developed in *Barbulescu* case,[51] and later confirmed in *Lopez Ribalda*.[52]

Second, in its assessment ECtHR places significant emphasis on the question whether the worker had the possibility to protect his right to privacy (personal data) also in the context of other available procedures under national law. All the presented ECtHR cases have in common that the employer gathered evidence through covert surveillance, with which he justified the dismissal. The worker, in turn, challenged the legality of this dismissal before the national labour courts, inter alia, on grounds of breach of his right to personal data protection (privacy). It is in this context that the ECtHR expressly points out that, in order to assess whether the worker has been afforded adequate safeguards under Article 8 ECHR (one of the criteria for assessing whether there has been a violation of Article 8 ECHR), account is also taken of whether the worker has availed himself of the other remedies available to him for a violation of the right to privacy (personal data protection). The ECtHR states, for example, that they could have brought a claim for damages for breach of the law governing the protection of personal data and could have lodged a

[50] See ECtHR, *Lopez Ribalda and Others v Spain* (Grand Chamber), Case Nos. 1874/13 and 8567/13, ECLI:CE:ECHR:2019:1017JUD000187413, para. 133.

[51] See ECtHR, *Barbulescu v Romania* (Grand Chamber), Case No. 61496/08, ECLI:CE:ECHR:2017:0905JUD006149608, para. 121.

[52] See ECtHR, *Lopez Ribalda and Others v Spain* (Grand Chamber), Case Nos. 1874/13 and 8567/13, ECLI:CE:ECHR:2019:1017JUD000187413, paras. 116, 118, 122.

complaint with the competent supervisory authority, which could have imposed a fine on the employer. Therefore, protection of worker's privacy (personal data) can also be achieved through civil, administrative and criminal law procedures (rules) – and not solely through labour law.[53]
Moreover, the above adequately illustrates the main issue of the topic. On the one hand, it is thus possible in a specific labour dispute (and later before the ECtHR) that the courts would uphold the employer's dismissal (based on covert surveillance) and decide that there was no violation of Article 8 ECHR (if the set criteria in *Barbulescu* and *Lopez Ribalda* cases are met). The employer may thus succeed in an employment dispute on the legality of the dismissal. On the other hand, in its judgments ECtHR explicitly states that the worker has other options (not only based on labour law) to protect his right to privacy (personal data). ECtHR does not further elaborate on possible results of these other procedures – it only highlights the fact that the worker did not resort to these procedures available under national law (although he could have done so). This means that, in practice, the employer may succeed before the employment tribunals after exercising covert control. However, the worker may initiate other parallel proceedings against the employer to protect his right to data protection – e.g., a complaint before the competent national Data Protection Authority for breaches of GDPR. These proceedings may result in very high administrative fines being imposed, which is certainly an undesirable outcome for the employer.
Third, even if, according to ECtHR jurisprudence, certain criteria are available to the employer to give guidance on the conditions under which there is no breach of Article 8 of the ECHR in case of covert surveillance – there are several indications that ECtHR by no means offers a uniform and consolidated approach to this problem. It is clear from the cases discussed that the judges are sharply divided among themselves, with close voting results (e.g., 11 for, 6 against (*Barbulescu* v *Romania*); 4 for, 3 against (*Libert* v *France*) etc.) and changes in ECtHR decisions after appeal (e.g., in the *Barbulescu* and *Lopez Ribalda* cases). Moreover, the judges' approach is also changing over time in line with the evolution of technology, as exemplified by the judges' stricter approach in the substantially similar recent *Lopez Ribalda* case, as opposed to the approximately 10 years older *Köpke* case.[54]

[53] See Ibidem, paras. 135-136.
[54] See ECtHR, Köpke v Germany, Case No. 420/07, ECLI:CE:ECHR:2010:1005DEC000042007, where the ECtHR has explicitly stated that it allows for the possibility that the conflicting interests of the worker and the employer

Therefore, the above suggests that judges are becoming more and more stringent in assessing the permissibility of interference with a worker's right to privacy (personal data protection) by new technologies. Moreover, it is reasonable to assume that the adoption of GDPR has only accelerated this trend, as will possibly be evident from the first cases that will come before the ECtHR, where the GDPR was already in force at the time of the national proceedings. Indeed, it should be borne in mind that in all the cases discussed in this paper, the predecessor of the GDPR, Directive 95/46/EC[55], was still in force at the time of the alleged violation of worker's rights and national proceedings. In the light of all the above, there is a serious question whether the ECtHR case law in this area is clearly consolidated and whether further changes are possible in the future which will tip the balance in favour of the protection of the worker's personal data – and thus further subject the employer's exercise of covert control to legal uncertainty.

Fourth, contrary to ECtHR, CJEU has not yet developed case law in the area of worker's personal data protection in the context of employer's workplace surveillance – including the question of (im)permissibility to carry out covert surveillance (in line with GDPR) under specifically justified circumstances. Consequently, it is not yet clear whether it is possible to fully transpose the standards developed in ECtHR case law into GDPR framework. As a result, there is considerable legal uncertainty as to in which cases such covert surveillance could be found legally permissible under GDPR. However, as outlined in this article, under GDPR, the employer has several legal obligations before imposing surveillance (e.g., video surveillance, which implies the processing of worker's personal data). These are mainly related to the justification of the surveillance on an appropriate legal basis (see Article 6 GDPR), the provision of several information to workers before the imposition of the surveillance (see Articles 12 to 14 GDPR), as well as the possible mandatory performance of a DPIA. A breach of all these GDPR provisions may have serious legal consequences for employers (heavy administrative fines, damages claim, etc.). In this vein, the recent documents adopted by the Article 29 Data Protection Working Party and the European Data Protection Board do not address such exceptional

may be given a different weight in the future (in the light of the intrusion into worker's private life by new advanced technologies.

[55] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281.

cases where it would be permissible to derogate from the above GDPR requirements (transparency principle, prior notification before the start of surveillance, etc.).

Fifth, considering the aforementioned, a paradigm shift in the area of worker's personal data protection at the supranational level would be (in my view) highly desired. Meaning that in practice workers, their representatives or lawyers should not bring such cases only before the ECtHR (after exhausting national remedies), but also before the CJEU in the context of the questions referred for a preliminary ruling (during ongoing procedures on the national level). In these preliminary ruling proceedings the relevant questions regarding the interpretation of GDPR and EU Charter could be raised. It is striking that, while there have been a number of "worker's personal data protection" cases before the ECtHR, there has not yet been a single(!) case before the CJEU concerning worker' personal data protection at the workplace. Moreover, it is worth noting that, *inter alia*, *Köpke*, *Lopez Ribalda* and *Barbulescu* cases could have also been decided from an EU law perspective through a preliminary reference to CJEU – regarding the interpretation of the provisions of Directive 95/46/EC (predecessor of GDPR) and EU Charter. Why the national courts did not have recourse to a preliminary reference to the CJEU under Article 267 TFEU is also questioned by *Eklund* (2019)[56] and *Peers* (2016)[57] in the context of the *Barbulescu* case.

5. Conclusion

The paper addresses the issue of (im)permissibility and consequences of covert surveillance at the workplace – from ECtHR case law and GDPR perspective. In the first part the relevant ECtHR case law is examined. It follows that covert surveillance at the workplace is (under certain conditions) compliant with Article 8 ECHR – although the developments in ECtHR reasoning from case *Köpke* (2010) to case *Lopez Ribalda* (2019) show a more stringent ECtHR approach towards covert surveillance. Moreover, ECtHR itself highlighted in *Lopez Ribalda* (where there was no violation of Article 8 ECHR) that workers had (and should have resorted to) other available administrative, civil and criminal procedures (besides the employment dispute) to protect their right to personal data (privacy). Therefore, while ECtHR case law provides some guidance for possible

[56] Eklund, 2019, p. 126.
[57] Peers, 2016.

outcomes of unjustified dismissal employment disputes – it by no means provides guaranteed guidance (without significant uncertainties) on possible outcomes of parallel administrative/punitive (administrative fines etc.) procedures for breaches of data protection rules (GDPR).
In this vein, the analysis showed that covert surveillance runs in contrast with the fundamental obligations under GDPR (transparency principle, right to prior notification etc.) and the relevant data protection guidelines issued on EU level. Consequently, since covert surveillance at the workplace has in its essence become a question of interpretation of EU law (GDPR in light of EU Charter) a paradigm shift in worker's personal data protection litigation is required – where the CJEU (instead of ECtHR) would be given the decisive role for setting new legal standards, which will be applicable in all EU Member States. Nevertheless, to achieve this turnaround, workers' representatives (legal counsel) will have to start to request the national courts to refer questions for preliminary ruling to the CJEU on these issues. It is striking that, while there have been a number of "worker's data protection" cases before the ECtHR, there has not yet been a single(!) case before the CJEU concerning worker' personal data protection at the workplace.

Bibliography:

Article 29 Data Protection Working Party, Working document on the surveillance of electronic communications in the workplace, No. 5401/01/EN/Final WP 55, 2002, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp55_en.pdf (accessed March 13, 2023).

Article 29 Data Protection Working Party, Opinion 2/2017 on data processing at work, No. 17/EN WP 249, 2017a, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169 (accessed March 13, 2023).

Article 29 Data Protection working party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, No. 17/EN, WP 248, 2017b, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 (accessed March 13, 2023).

J. Atkinson, Workplace Monitoring and the Right to Private Life at Work, in The Modern Law Review, 2018, vol. 81, no. 4, 688-700,

https://onlinelibrary.wiley.com/doi/full/10.1111/1468-2230.12357 (accessed March 13, 2023).

T. Bagdanskis, P. Sartatavičius, Workplace Privacy: Different Views and Arising Issues, in Jurisprudence, 2012, vol. 19, no. 2, 697–713, https://repository.mruni.eu/handle/007/11090 (accessed March 13, 2023).

P. Bhave, Devasheesh, H. Laurel Teo, S. Reeshad Dalal, Privacy at Work: A Review and a Research Agenda for a Contested Terrain, in Journal of Management, 2020, vol. 46, no. 1, 127-164, DOI: https://doi.org/10.1177/0149206319878254 (accessed March 13, 2023).

M. Brkan, Introduction: Employee's Privacy at the Forefront of Privacy Debates, in European Data Protection Law Review (EDPL), 2017, vol. 3, no. 4, 543-544, DOI: https://doi.org/10.21552/edpl/2017/4/19 (accessed March 13, 2023).

C. Calomme, Monitoring of employees' communications: ECtHR spells out positive obligations to protect employees' privacy, in European Data Protection Law Review (EDPL), 2017, vol. 3, no. 4, 545-549, DOI: https://doi.org/10.21552/edpl/2017/4/20 (accessed March 13, 2023).

Charter of Fundamental Rights of the European Union, OJ C 326, 26. 10. 2012.

M. D'Aponte, New technologies and respect for the worker's privacy in ECHR case law, in Revue de droit comparé du travail et de la sécurité sociale, 2021, no. 4, 192-203, DOI: https://doi.org/10.4000/rdctss.2718 (accessed March 13, 2023).

D. Dimitrova, Video surveillance at work in need of regulation?, in European Data Protection Law Review (EDPL), 2020, vol. 6, no. 1, 152-157, DOI: https://doi.org/10.21552/edpl/2020/1/21 (accessed March 13, 2023).

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281.

ECtHR, *Barbulescu v Romania* (Grand Chamber), Case No 61496/08, ECLI:CE:ECHR:2017:0905JUD006149608.

ECtHR, *Barbulescu v Romania* (Grand Chamber), joint dissenting opinion of Judges Raimondi, Dedov, Kjølbro, Mits, Mourou-Vikström and Eicke, Case No 61496/08, ECLI:CE:ECHR:2017:0905JUD006149608.

ECtHR, *Copland v the United Kingdom*, Case No. 62617/00, ECLI:CE:ECHR:2007:0403JUD006261700.

ECtHR, *Halford v the United Kingdom*, Case No. 20605/92, ECLI:CE:ECHR:1997:0625JUD002060592.

ECtHR, *Köpke v Germany*, Case No 420/07, ECLI:CE:ECHR:2010:1005DEC000042007.

ECtHR, *Libert v France*, Case No. 588/13, ECLI:CE:ECHR:2018:0222JUD000058813.

ECtHR, *Lopez Ribalda and Others v Spain* (Grand Chamber), Case Nos 1874/13 and 8567/13, ECLI:CE:ECHR:2019:1017JUD000187413.

ECtHR, *Lopez Ribalda and Others v Spain* (Grand Chamber), joint dissenting opinion of Judges Gaetano, Grozev, and Yudkivska, Case Nos 1874/13 and 8567/13, ECLI:CE:ECHR:2019:1017JUD000187413.

L. Edwards, L. Martin, T. Henderson, Employee Surveillance: the Road to Surveillance Is Paved with Good Intentions, Amsterdam Privacy Conference, Amsterdam, Netherlands, 2018, https://research-repository.st-andrews.ac.uk/handle/10023/17297 (accessed March 13, 2023).

J. Eichenhofer, Internet Privacy at Work the EctHR Barbulescu Judgment, in European Data Protection Law Review (EDPL), 2016, vol. 2, no. 2, 266-271, DOI: https://doi.org/10.21552/EDPL/2016/2/23 (accessed March 13, 2023).

M. C. Eklund, Monitoring workers' e-mail correspondence and Internet use – A Finnish perspective – PART I, in European Labour Law Journal, 2019, vol. 10, no. 2, 116-133, https://journals.sagepub.com/doi/pdf/10.1177/2031952519852110 (accessed March 13, 2023).

European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), 1950, as amended by Protocols Nos. 11, 14, 15 and supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13 and 16.

European Data Protection Board, Guidelines 3/2019 on processing of personal data through video devices, Version 2.0, Adopted on 29 January 2020, 2020, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en (accessed March 13, 2023).

V. Grentzenberg, J. Kirchner, Data Protection and Monitoring, in J. Kirchner, P. R. Kremp and M. Magotsch (eds.), Key Aspects of German Employment and Labour Law: Second Edition, Springer, Berlin, 2019, 135-152.

H. A. Halefom, A pragmatic compromise? The role of Article 88 GDPR in upholding privacy in the workplace, in International Data Privacy Law, 2022, vol. 12, no. 4, 276-296, DOI: https://doi.org/10.1093/idpl/ipac015 (accessed March 13, 2023).

E. Kaiser, Monitoring Employees with Hidden Surveillance Cameras Breaches Their Right to Privacy, in European Data Protection Law Review (EDPL), 2018, vol. 4, no. 3, 396-399, DOI: https://doi.org/10.21552/edpl/2018/3/22 (accessed March 13, 2023).

T. Katsabian, Employees' Privacy in the Internet Age, in Berkeley Journal of Employment and Labor Law, 2019, vol. 40, no. 2, 203–255, DOI: https://doi.org/10.15779/Z38NG4GS3G (accessed March 13, 2023).

E. Keane, The GDPR and Employee's Privacy: Much Ado but Nothing New, in King's Law Journal, 2019, vol. 29, n. 3, 354-363, DOI: https://doi.org/10.1080/09615768.2018.1555065 (accessed March 13, 2023).

S. Klein, Libert v. France: EctHR on the Protection of an Employee's Privacy Concerning Files on Work Computer, in European Data Protection Law Review (EDPL), 2018, vol. 4, no. 2, 250-251, DOI: https://doi.org/10.21552/edpl/2018/2/16 (accessed March 13, 2023).

K. Lenaerts, I. Maselis, K. Gutman, EU procedural law, Oxford University Press, New York, 2014.

J. Letnar Černič, Realising the Charter of Fundamental Rights of the European Union in national and European fora, Dignitas, 2015, No. 65-66, 79-108, http://revije.nova-uni.si/index.php/dignitas/article/view/229 (accessed March 13, 2023).

G. Lockwood, Workplace Monitoring and Surveillance: The British Context, in Athens Journal of Law, 2018, vol. 4, no. 3, 205-228, https://www.athensjournals.gr/law/2018-4-3-1-Lockwood.pdf (accessed March 13, 2023).

L. Munteanu, M. Povey, Data Protection A Firewall between Employers and Trade Unions?, in European Data Protection Law Review (EDPL), 2022, vol. 8, no. 1, 41-51, DOI: https://doi.org/10.21552/edpl/2022/1/8 (accessed March 13, 2023).

C. Ogriseg, GDPR and Personal Data Protection in the Employment Context, in Labour & Law Issues, 2017, vol. 3, no. 2, 1-24, DOI: https://doi.org/10.6092/issn.2421-2695/7573 (accessed March 13, 2023).

S. Peers, Is Workplace Privacy Dead? Comments on the Barbulescu judgment, in EU Law Analysis, 2016, http://eulawanalysis.blogspot.com/2016/01/is-workplace-privacy-dead-comments-on.html (accessed March 13, 2023).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119.

W. Schabas, The European Convention on Human Rights: A Commentary, Oxford University Press, Oxford, 2015.

S. Stanev, Monitoring of Employees' Personal Communications at Work. Practice of the ECtHR, in E-Journal of International and Comparative Labour Studies, 2019, vol. 8, no. 1, 94-103, https://ejcls.adapt.it/index.php/ejcls_adapt/article/view/646 (accessed March 13, 2023).

A. Stone Sweet, H. Keller, The Reception of the ECHR in National Legal Orders, in A. Stone Sweet, H. Keller (eds.), A Europe of Rights: The Impact of the ECHR on National Legal Systems, Oxford University

Press, New York, 2008, 3-28, DOI: https://doi.org/10.1093/acprof:oso/9780199535262.003.0001 (accessed March 13, 2023).

E. Sychenko, D. Chernyaeva, The Impact of the ECHR on Worker's Privacy Protection, in Italian Labour Law e-Journal, 2019, vol. 12, no. 2, 171-188, DOI: https://doi.org/10.6092/issn.1561-8048/10015 (accessed March 13, 2023).

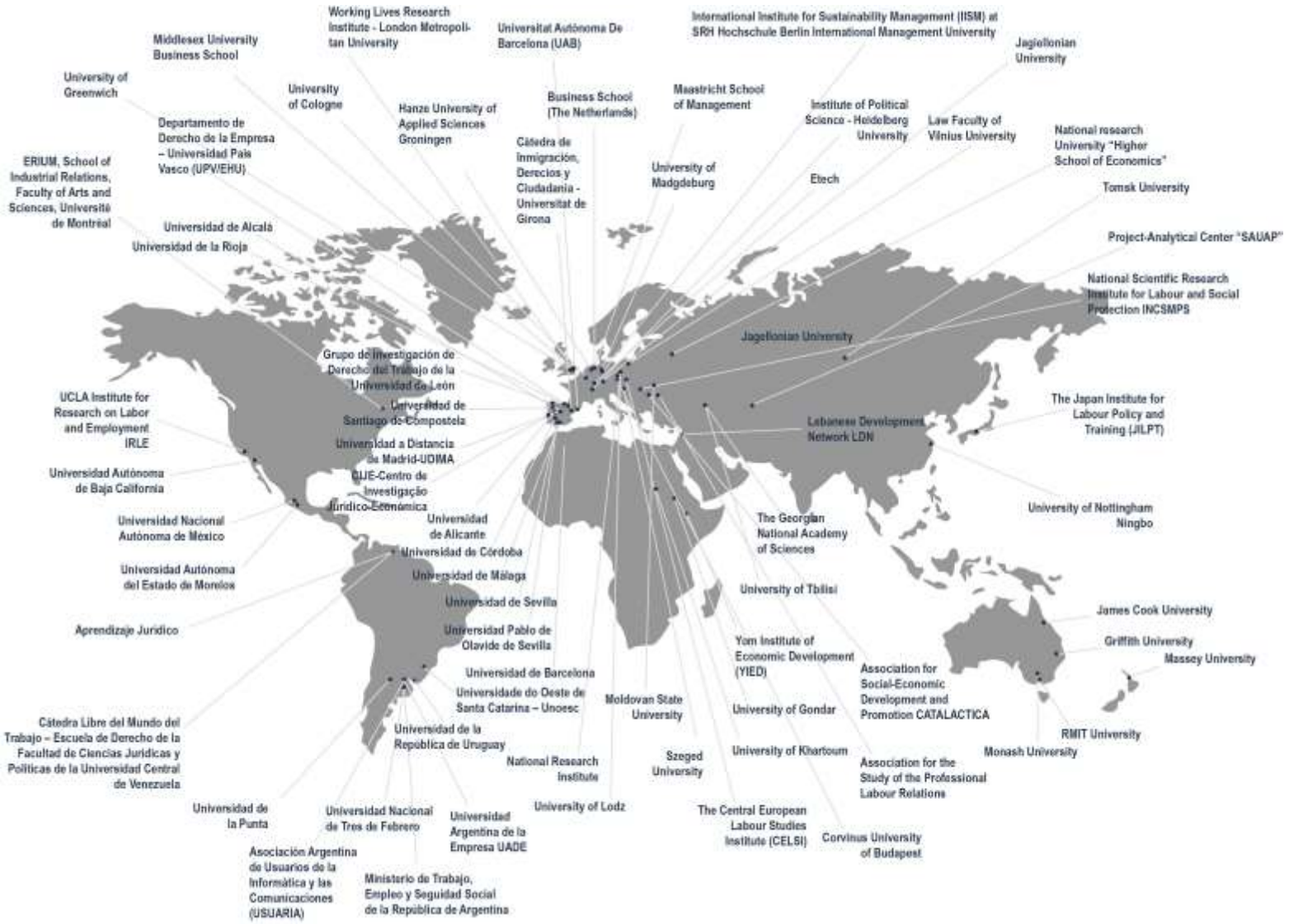
Treaty on the Functioning of the European Union, OJ C 326, 26. 10. 2012.

V. Trstenjak, M. Brkan, Pravo EU: ustavno, procesno in gospodarsko pravo EU (EU law: constitutional, procedural and commercial law of the EU), GV založba, Ljubljana, 2012.

V. Turanjanin, Video Surveillance of the Employees between the Right to Privacy and Right to Property after Lopez Ribalda and Others v. Spain, in University of Bologna Law Review, 2020, vol. 5, no. 2, 268-293, DOI: https://doi.org/10.6092/issn.2531-6133/10514 (accessed March 13, 2023).

P. Voigt, A. von dem Bussche, The EU General Data Protection Regulation (GDPR): A Practical Guide, Springer International Publishing, Cham, 2017.

ADAPT International Network



ADAPT is a non-profit organisation founded in 2000 by Prof. Marco Biagi with the aim of promoting studies and research in the field of labour law and industrial relations from an international and comparative perspective. Our purpose is to encourage and implement a new approach to academic research, by establishing ongoing relationships with other universities and advanced studies institutes, and promoting academic and scientific exchange programmes with enterprises, institutions, foundations and associations. In collaboration with the Centre for International and Comparative Studies on Law, Economics, Environment and Work, (DEAL) the Marco Biagi Department of Economics, University of Modena and Reggio Emilia, ADAPT set up the International School of Higher Education in Labour and Industrial Relations, a centre of excellence which is accredited at an international level for research, study and postgraduate programmes in the area of industrial and labour relations. Further information at *www.adapt.it*.

For more information about the E-journal and to submit a paper, please send a mail to *LS@adapt.it*.

DEAL Centre for International and Comparative Studies Law Economics Environment Work
THE MARCO BIAGI DEPARTMENT OF ECONOMICS
UNIVERSITY OF MODENA AND REGGIO EMILIA

ADAPT International.it
Building the Future of Work