UDK 349.22:004]: 342.7
Review article

WORKPLACE PRIVACY IN THE EU: THE IMPACT OF EMERGING TECHNOLOGIES ON EMPLOYEE'S FUNDAMENTAL RIGHTS

Adrienne Komanovics, PhD, Assistant Professor
Corvinus University of Budapest
Budapest, Fővám tér 8. Hungary
adrienne.komanovics@uni-corvinus.hu

ABSTRACT

Over the last decade, several new technologies have been adopted that enable more systematic surveillance of employees, creating significant challenges to privacy and data protection. The risks posed by the new devices and methods were exacerbated with the advent of Covid, with the involuntary introduction of digital tools to measure work output and efforts to get visibility back in the workplace through new means.

Against this backdrop, the article aims to examine the main issues in workplace surveillance. After a brief overview of the range of surveillance methods, such as video surveillance, network and e-mail monitoring, and employee tracking softwares (the so-called "bossware"), as well as the challenges posed by the new technologies, the paper goes on to individually analyse the legal aspects of monitoring employees for security or performance-related reasons. The phenomenon is examined in light of relevant EU legislation (the General Data Protection Regulation of 2016 being the most relevant one), as well as the opinions adopted by the Article 29 Working Party established by Directive 95/46 and the guidelines drawn up by the European Data Protection Board, established by the GDPR and replacing the WP. In doing so, the paper will elaborate on the concept of transparency, consent, purpose limitation, data minimization, data retention, the so-called expectation of privacy, and the lawfulness of processing, especially the issue of balancing the legitimate interests of the employer against the interests or fundamental rights of the data subject.

The results of the analysis suggest that new and emerging technologies developed to monitor employees in order to address productivity issues, security risks, and sexual harassment, combined with the fact that remote and hybrid work becomes the norm inevitably increase the porosity between work and private life and blur the line between public and private. Such an extensive intrusion into privacy calls for enhanced institutional efforts to protect workers from the surveillance overreach of the new digital devices.

***Keywords**: data protection; fundamental rights, GDPR, surveillance, workplace privacy*

1. INTRODUCTION

The spread of modern information technology throughout society, the increasing importance of information, and the transformation of workplace has a strong impact on our life. Although the use of new technologies admittedly results in greater efficiency and productivity, improved healthcare, and increased opportunities for education, they raise a host of privacy and other concerns. Vital information of clients and customers, including names, addresses, emails, phone numbers, health information or bank details, is collected, stored, and processed. Apart from security concerns, the collection of the traces we leave when browsing the Internet can be compiled into a comprehensive digital profile based on the analysis of our behaviour, to be used for targeted advertising or targeted political ads. Our profile might include sensitive data such as health data, financial situation, political orientation, and sexual orientation.

This is no different in the employment complex. With the rise of sophisticated and accessible workplace surveillance techniques, massive amounts of personal data are collected. Employers can implement surveillance measures for purposes such as promoting productivity or improving security. New, increasingly intrusive technologies enable more stringent scrutiny of the employees to monitor the work of staff or to check their presence, creating significant challenges to privacy and data protection. Surveillance intensified with the onset of the pandemic, as employers sought greater control of employees working remotely. However, working from home blurred the contours of public and private spheres.

This paper will not venture to provide a comprehensive analysis of the threats of technology to privacy; it has a narrower scope: it aims to outline the privacy risks of workplace surveillance in the Member States of the European Union. Since at the moment there is no specific EU legislation on the issue, the analysis builds upon GDPR (and its predecessor, Directive 95/46/EC) as well as the guidance provided by the EDPB (and its predecessor, the Article 29 Working Group, the opinions of which have mostly been endorsed upon, and sometimes developed further, by the EDPB). In doing so, the paper will borrow from the case law of the European Court of Human Rights and its interpretation of Article 8 ECHR in the context of workplace surveillance.

The article is structured as follows. The second section outlines the origins of data protection with a focus on Europe and highlights the salient features of data processing in the specific context of employment. The third section examines the various methods used in workplace surveillance and then goes on to analyse the relevant articles of the GDPR. The fourth section gives an overview of the current practice through the lens of the European Court of Human Rights, the CJEU so

far not being seized of this particular aspect of data protection. The fifth section finally addresses some concluding remarks on the legislative framework and the caselaw.

This paper is based on several methods. Desk research included the identification and analysis of relevant treaties and legislation, jurisprudence, and the interpretation provided by the EU data protection bodies. During the literature research, relevant academic publications were collected. The online research focused on several academic blogs and the database of Luxembourg and the Strasbourg Courts.

The research is qualitative and is concerned with the interpretation and assessment of how the interests relating to the protection of personal data could be reconciled with the interests relating to the processing of such data by the employer. Thus, after exploring the problem, i.e., data protection in Europe in general, and workplace surveillance, in particular, the paper goes on to critically describe the relevant legislation and, finally, to explain and interpret how the principles formulated either by the legislator or developed through jurisprudence were applied in cases reaching European tribunals.

It is argued that new and emerging technologies developed to monitor employees in order to address productivity issues, security risks, and sexual harassment, combined with the fact that remote and hybrid work becomes the norm inevitably increase the porosity between work and private life and blur the line between public and private. Such an extensive intrusion into privacy calls for enhanced institutional efforts to protect workers from the surveillance overreach of the new digital devices.

2. HISTORY OF DATA PROTECTION IN EUROPE: A BRIEF OVERVIEW

The authors of the European Convention on Human Rights could not have foreseen the inconceivable variety of situations where Article 8 might be engaged. The spread of evolutive interpretation, of the idea that "the Convention is a living instrument" has, however, allowed the Court to adapt the text of the Convention to legal, social, ethical or scientific developments,[1] thus expanding the scope of the Convention has been extended to scenarios not envisaged in the late 1940s.[2] Thus,

[1] *Tyrer v. the United Kingdom*, Application no. 5856/72, April 1978, para. 31.

[2] The storage of DNA profiles (*Aycaguer v. France*, Application no. 8806/12, 22 June 2017); private health data leaked to journalists (*Biriuk v. Lithuania*, Application no. 23373/03, 25 Nov 2008); protections for journalists and their sources (*Ernst and Others v. Belgium*, Application no. 33400/96, 15 July 2003) or the Court's finding in *López Ostra* that severe environmental pollution may affect indi-

the Court was given the opportunity to pronounce on various aspects of data protection, including, as will be demonstrated in Section 4, workplace surveillance.

As contemporaneous national legislations gave insufficient protection to individual privacy, the Council of Europe decided to draw up a specific instrument with the aim to guarantee adequate protection to the right of personal privacy vis-à-vis modern science and technology. Convention 108 of the Council of Europe[3] provided guarantees in relation to the collection and processing of personal data, contained special safeguards in case of "sensitive" data on a person's race, politics, health, religion, sexual life, criminal record and provided for the right to know and the right to correct. One of the main motivations for the Convention was to replace the predominant non-interference approach of the ECHR with a more positive, proactive and more structural approach.[4] Convention 108 is open to non-members of the Council of Europe and relies on national legislation for its implementation. In 2001, it was complemented by an additional protocol aiming at increasing the protection of personal data and privacy by providing for the establishment of national supervisory authorities, and transborder data flows to third countries, allowing it only if the recipient State or international organisation can provide an adequate level of protection.[5] A thoroughly revised Convention, referred to as Convention 108+, was adopted in 2018,[6] addressing the challenges to privacy resulting from the use of new information and communication technologies, and strengthening the Convention's mechanism to ensure its effective implementation.

The EU's first comprehensive data protection instrument was Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and

---

viduals' well-being and prevent them from enjoying their homes in such a way as to affect their private and family life adversely (*López Ostra v. Spain*, Application no. 16798/90, 9 Dec 1994), just to name a few cases.

3 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), 1981.

4 Hustinx, P., *Data protection and international organizations: a dialogue between EU law and international law*, International Data Privacy Law, Vol. 11, No. 2, 2021, pp. 77-80. – Parallel to Convention no. 108, the OECD also prepared a document titled Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, which was adopted in 1980 and was updated in 2013, C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79. See also See also: UN Personal Data Protection and Privacy Principles, adopted 11 October 2018, available at: [https://unsceb.org/sites/default/files/imported_files/UN-Principles-on-Personal-Data-Protection-Privacy-2018_0.pdf], Accessed 15 April 2023.

5 Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (ETS No. 181), 2001.

6 Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223), 2018.

on the free movement of such data (European Data Protection Directive). Over the years, data protection developed into a distinct value, data protection now being recognised as a fundamental right, separate from the right to respect for private life. The main elements of the current *corpus* of EU data protection law include Article 16 of the Treaty on the Functioning of the European Union (TFEU) providing that the EU shall lay down data protection rules for the processing of personal data, Article 8 of the Charter of Fundamental Rights containing an explicit right to the protection of personal data and providing for the establishment of national data protection authorities, Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation),[7] and Directive (EU) 2016/680 on the protection of natural persons regarding processing of personal data connected with criminal offences or the execution of criminal penalties, and on the free movement of such data (Data Protection Law Enforcement Directive).[8] In addition, the issue of harmonisation of data protection rules in the employment context was raised, but the Member States could not reach an agreement on the adoption of such sector-specific regulation.[9] In line with Article 98 GDPR requiring the EU legislator to update other Union legal acts, in 2017 the Commission published a proposal[10] a new regulation on privacy and electronic communications, with a view of replacing the so-called ePrivacy Directive.[11]

---

7 Regulation (EU) 2016/679 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), [2016] OJ L119/1. – In 2012 the European Commission proposed a comprehensive reform of the EU's 1995 data protection rules.

8 Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Data Protection Law Enforcement Directive), [2016] OJ L119/89.

9 "… a combination of legal, pragmatic, political, cultural, and constitutional factors hindered efforts of adopting such sector-specific legislation at the EU level." Abraha, H.H., *A pragmatic compromise? The role of Article 88 GDPR in upholding privacy in the workplace*, International Data Privacy Law, Vol. 12, no. 4, 2022, pp. 276-296, at p. 277. – See also *Bărbulescu* v. *Romania* [GC], Application no. 61496/08, 5 September 2017 (hereinafter *Bărbulescu*), para. 118, noting that there is no European consensus on the issue of how to regulate the question of the exercise by employees of their right to respect for their private life and correspondence in the workplace.

10 Proposal for a Regulation of The European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 final – 2017/03 (COD).

11 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications' sector (Directive on privacy and electronic communications), [2002] OJ L 201/37.

Regarding the GDPR, which is at the heart of our investigation, the EU legislature has chosen to use a regulation as the form of legal instrument in order to increase the degree of uniformity of the EU data protection law.[12] The GDPR had been drafted in a technology neutral way, as a "flexible tool to ensure that the development of new technologies is in compliance with fundamental rights".[13] The GDPR has a dual purpose: the protection of natural persons with respect to the processing of personal data, on the one hand, and rules relating to the free movement of personal data in the internal market, on the other.[14] The GDPR requires Member States to legislate in some areas and provides them with the possibility to further specify the GDPR in others, leading to a considerable fragmentation of data protection law.[15]

The implementation costs of the introduction of the GDPR are estimated to have been significant.[16] Compliance with the GDPR is secured via the designation of a Data Protection Officer by the data controller or processor, while external supervision is secured with the establishment of independent national supervisory authorities.[17]

The measure to deal with data protection in the EU institutions and bodies is Regulation 2018/1725 on the protection of natural persons with regard to the pro-

---

12 Opinion of Advocate General Szpunar in Case C-439/19 *Latvijas Republikas Saeima*, ECLI:EU:C:2020:1054, para. 46.

13 European Commission, Commission Staff Working Document accompanying the document Communication from the Commission to the European Parliament and the Council. Data protection rules as a pillar of citizens empowerment and EUs approach to digital transition – two years of application of the General Data Protection Regulation, COM(2020) 264 Final, p. 10.

14 GDPR Art. 1.

15 European Commission, Commission Staff Working Document, *op. cit.*, note 13, p. 7.

16 "The average implementation cost of Fortune 500 companies was estimated to be 16 million USD." Lintvedt, M.N., *Putting a price on data protection infringement*, University of Oslo Faculty of Law Research Paper No. 2022-56, Vol. 12, No. 1, 2022, pp. 1-15, at p. 9.

17 GDPR Arts 37 and 51. – Custers, B.; Louis, L.; Spinelli, M.; Terzidou, K., Quis custodiet ipsos custodes? Data protection in the judiciary in EU and EEA Member States, *International Data Privacy Law*, Vol. 12, No. 2, 2022, pp. 93-112, at p. 96. See, however, the controversy in 2011, in which the Hungarian PM terminated the term of the data protection commissioner, available at: [https://www.reuters.com/article/us-eu-hungary-idUSBREA370TX20140408], accessed 15 April 2023; and Komanovics, A., *Hungary and the Luxembourg Court: The CJEU's Role in the Rule of Law Battlefield*. In: EU and Comparative Law Issues and Challenges Series (ECLIC), Vol. 6, 2022, pp. 122-157. On the enforcement challenges of data protection law, see e.g. Veale, M.; Binns, R.; Ausloos, J., *When data protection by design and data subject rights clash*, International Data Privacy Law, Vol. 8, No. 2, 2018, pp. 105-123, and Kuner, C.; Cate, F.H.; Lynskey, O.; Millard, C.; Ni Loideain, N.; Svantesson, D.J.B., *If the legislature had been serious about data privacy …*, International Data Privacy Law, Vol. 9, No. 2, 2019, pp. 75–77.

cessing of personal data by the Union institutions, bodies, offices, and agencies,[18] also establishing a European Data Protection Supervisor.

It is worth noting that data protection in the employment context displays several specific traits, not apparent in other data protection scenarios. To begin with, employment relationships are characterised by the intrusiveness and scale of technologies introduced under the guise of legitimate interests. Employers are increasingly deploying sophisticated technologies, a trend that has been exacerbated by the COVID-19 pandemic. This has normalized employee monitoring and surveillance in unprecedented ways and has increasingly blurred the line between work and private life. Furthermore, the employer-employee relationship is characterised by legal subordination.[19] The inherent inequality of power discredits consent as a legitimate basis for data processing. Finally, the collective nature of labour law does not easily fit with the individualistic approach of the GDPR, where rights are granted to the person concerned on an individual basis.[20]

Having clarified these differences, it should also be noted that individuals enjoy the right to their private lives, even in the workplace and in public spaces shared with others. In *Bărbulescu*, the European Court of Human Rights held that "an employer's instructions cannot reduce private social life in the workplace to zero".[21] The Court noted that the notion of private life "enshrines the possibility of approaching others in order to establish and develop relationships with them" and added that "it is in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity to develop relationships with the outside world …".[22] For example, employees have a right to private communications in the workplace even if those communications occur on the employer's equipment or happen during work hours.

3. WORKPLACE SURVEILLANCE: THE RELEVANT RULES AND PRINCIPLES

The section starts with an overview of the various technology used in workplace surveillance, followed by the examination of the legitimate reasons set out in Ar-

[18] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, [2018] OJ L295/39.

[19] *Bărbulescu* para. 17.

[20] Abraha, *op. cit.* note 9, pp. 278-279.

[21] *Bărbulescu* para. 80.

[22] *Bărbulescu*, para. 71.

ticle 6 GDPR, and the identification of those which can provide a valid basis for data processing at the workplace. After a brief reference to the issue of sensitive data necessitating the application of more stringent rules, the section examines how the principles relating to the processing of personal data apply in the employment context.

3.1. Modern technology and the rise of employee monitoring

The intrusiveness and scale of technologies have increased during the last decades. Employers use a wide and constantly evolving variety of surveillance devices, including keyloggers and other tracking software, closed circuit cameras, radio-frequency identification badges, and methods such as saving screenshots, measuring the frequency of employers' clicks and keystrokes, taking webcam photos of the workers, laptops, or smartphones. Many gadgets contain recorders and cameras that can be remotely activated, while fitness and health tracking devices provided to employees as part of "wellness" programmes collect data on employee physical activity, heart rate, and sleep patterns.[23] The information extracted threatens not only the employees' right to privacy and data protection, but can lead to the violation of anti-discrimination provisions, as such health information could affect the employer's decision about promotion and dismissal.[24]

The proliferation of home-based telework, though already on the rise before Covid,[25] violently imposed on the world due to the pandemic in 2020-2022, accelerated the transition from a regular organisation of work to working from home and "fostered the porosity between work and private life".[26] While the shift to tele-

---

[23] Garden, C., *Labor Organizing in the Age of Surveillance*, Saint Louis University Law Journal, Vol. 63, 2018, pp. 55-68, at p. 56-59. See also Collins, P.; Marassi, S., *Is That Lawful? Data Privacy and Fitness Trackers in the Workplace*, International Journal of Comparative Labour Law and Industrial Relations, Vol. 37, No. 1, 2021, pp. 65-94; Brassart Olsen, C., *To track or not to track? Employees' data privacy in the age of corporate wellness, mobile health, and GDPR*. International Data Privacy Law, Vol. 10, No. 3, 2020, pp. 236–252.

[24] Brassart Olsen, *op. cit.*, note 23, at p. 236. See also Collins, Marassi, *op. cit.*, note 23, at pp. 65-94.

[25] "According to data from the 2015 European Working Conditions Survey, the overall proportion of people teleworking was high in the Nordic countries – Denmark (37%), Sweden (33 %) – and the Netherlands (30%); it was average in countries such as Luxembourg (26%), France (25%), Estonia (24%), Belgium (24%) and Finland (24%); and it was low in half of EU countries, ranging from 12-13% (Germany, Spain, Bulgaria, Lithuania and Romania) to 7-11% (Italy, Czechia, Poland, Slovakia, Portugal and Hungary)." European Economic and Social Committee, Opinion on 'Challenges of teleworking: organisation of working time, work-life balance and the right to disconnect' (Exploratory opinion at the request of the Portuguese Presidency), EESC 2020/05278, [2021] C 220/01, para. 2.11.

[26] Leccese, V. S., *Monitoring working time and Working Time Directive 2003/88/EC: A purposive approach*, European Labour Law Journal, Vol. 14, No. 1, 2022, pp. 21-34, at p. 11.

working proved essential to combating the health crisis, and helped to ensure that the economy has continued to function and has saved jobs, it inherently attracted the application of increased surveillance and control, including measures such as monitoring the websites accessed, monitoring the employee's activity by regular screenshots, webcam surveillance, some of them remaining with us afterward. It is argued that surveillance whilst working from home almost reverses the original problem with workplace privacy: while in normal circumstances data protection at workplace relates to the protection of privacy in a public sphere, monitoring home office activities involves the monitoring of a private sphere which is rendered quasi-public through the surveillance. The employee's home becomes a public place, at least during working hours, leading to the convergence of two usually distinct spaces, namely the workplace and the private sphere.[27] Needless to say, the data protection implications are massive.

3.2. Lawfulness of processing

Before monitoring their workers, employers must determine the lawfulness of processing personal data. Employers do have a legitimate interest to protect their property from theft and engage in a certain level of monitoring to ensure the smooth running of the company.[28] The types of data processing range from application forms, payroll and tax, social benefits information, sickness records, annual leave records, annual assessment records, records relating to promotion, disciplinary matters, etc.[29] While a certain level of privacy should be guaranteed at workplace, employers have lawful reason to scrutinize their employees. However, drawing the line between acceptable and unacceptable data practices is not an easy task.

The lawful reasons for processing data are set out in Article 6(1) of the GDPR as follows.

Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

---

27 Collins, P., *The Right to Privacy, Surveillance-by-Software and the "Home-Workplace"*, 3 September 2020, available at: [https://uklabourlawblog.com/2020/09/03/the-right-to-privacy-surveillance-by-software-and-the-home-workplace-by-dr-philippa-collins/], Accessed 15 April 2023.

28 See e.g. *Bărbulescu* para. 124.

29 Article 29 Data Protection Working Party, Opinion 8/2001 on the processing of personal data in the employment context, 5062/01/EN/Final, WP48, p. 2, fn. 5.

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

From these, four situations might be relevant in the employment context, namely consent, necessity based on the performance of a contract, compliance with legal obligation, and the legitimate interest pursued by the controller.[30] It is possible that there are multiple legal bases on which a controller can rely at the same time ("at least one of the following applies"). There is no hierarchy between the various bases.

As far as *consent* is concerned, it means "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".[31] The request for consent must be presented in an intelligible and easily accessible form, using clear and plain language,[32] and must be clearly distinguishable from the other matters. The consent of the data subject must be given in relation to "one or more specific" purposes and the data subject must have a choice in relation to each of them. Furthermore, the the consent must be "informed". Therefore, the data subject must be informed, *inter alia*, of the identity of the controller, the purpose of each of the processing operations for which consent is sought, what type of data will be collected and used,

30 GDPR Art 6(1) points points (a), (b), (c) and (f).

31 GDPR Art 2(11).

32 Information must be "easily understandable for the average person and not only for lawyers; controllers cannot use long privacy policies that are difficult to understand or statements full of legal jargon", see European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679. Version 1.1, 4 May 2020, para. 67.

and the existence of the right to withdraw consent.[33] Providing information to data subjects before obtaining their consent is essential in order to allow them to make informed decisions. Unambiguous indication of wishes denotes that "consent requires a statement from the data subject or a clear affirmative act, which means that it must always be given through an active motion or declaration".[34] The controller must demonstrate that it is possible to refuse or withdraw consent without detriment.[35] In addition, data subjects shall have the right to withdraw their consent at any time. Finally, the burden of proof is on the data controller to demonstrate that consent has been given.[36]

However, the Article 29 Working Party, as well as the European Data Protection Board, has consequently maintained that "[e]mployees are almost never in a position to freely give, refuse or revoke consent, given the dependency that results from the employer/employee relationship."[37] In 2017, the Article 29 Working Party adopted specific guidelines on consent (revised in 2018), noting that:

> An imbalance of power also occurs in the employment context. Given the dependency that results from the employer/employee relationship, it is unlikely that the data subject is able to deny his/her employer consent to data processing without experiencing the fear or real risk of detrimental effects as a result of a refusal. It is unlikely that an employee would be able to respond freely to a request for consent from his/her employer to, for example, activate monitoring systems such as camera-observation in a workplace, or to fill out assessment forms, without feeling any pressure to consent. Therefore, WP29 deems it problematic for employers to process personal data of current or future employees on the basis of consent as it is unlikely to be freely given. For the majority of such data processing at work, the lawful basis cannot and should not be the consent of the employees (Article 6(1)(a)) due to the nature of the relationship between employer and employee.[38]

---

33 *Ibid.*, para. 64.

34 *Ibid.*, para. 75.

35 *Ibid.*, para. 46 and recital 42.

36 GDPR Art 7, Conditions for consent.

37 Article 29 Data Protection Working Party, Opinion 2/2017 on data processing at work, 8 June 2017, 17/EN, WP 249, para. 6.2.

38 Article 29 Data Protection Working Party, Guidelines on consent under Regulation 2016/679, 28 November 2017, last revised 10 April 2018, 17/EN, WP 259 rev. 01, at. p. 7. – See also para. 47 of European Data Protection Board, Guidelines 3/2019 on processing of personal data through video devices. Version 2.0, 29 January 2020; or para. 21 of the EDPB Guidelines 05/2020 on consent, *op. cit.* note 32.

In conclusion, workplace surveillance should not be based on consent, given the imbalance of power between employers and employees.

The next two lawful reasons are *contract* and *compliance with legal obligations*. In fact, various personal data, such as date of birth, address, bank details, social security number, are indispensable for the processing of payroll. Additionally, national legislation can require the provision of tax information, data on social security payments or on maternity and paternity leave. The "legal obligation" must have the force of law; soft measures, such as guidelines, are insufficient.[39]

The fourth potential basis, the most probable scenario, and the most interesting from our perspective is the *legitimate interest* of data processing of the employer in relation to a wide range of data. This is a flexible clause, covering all instances which are not covered by the other exceptions. In relation to all other exceptions, it is assumed that balance between interests is satisfied while, in contrast, this last exception contains a balancing test.[40] As the site GDPRhub, set up by European Center for Digital Rights, argues,

> "Article 6(1)(f) GDPR is the 'catch all' balancing test for anything not foreseen by Articles 6(1)(b) to (e) GDPR, where the controller does not seek consent, but takes the view that the rights of the controller or a third party override the rights of the data subject."[41]

The balancing involves a multi-step process and is entirely in the hands of the data controller. Controllers must verify the "legitimate" nature of their interests,[42] then identify the rights and interests of the data subject. Finally, the actual balancing between the two opposed positions must be carried out.[43] In doing so, several issues must be taken into consideration, including the nature of personal data (e.g. sensitive data, like biometric data, genetic information, communication data,

---

39 Article 29 Data Protection Working Party, Opinion 8/2001 on the processing of personal data in the employment context (WP48), *op, cit.*, note 29, at pp. 6-7; Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 9 April 2014, 844/14/EN, WP 217; European Data Protection Board, Guidelines 05/2020 on consent *op. cit.*, note 32, paras. 30 and 31.

40 Indeed, other provisions of the GDPR also contain balancing tests, including the provisions on necessity, proportionality, and purpose limitation, data minimisation, Article 9(2)f), Article 13 and Article 85. Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller, *op. cit*. note 39, at p. 11.

41 GDPRhub, European Center for Digital Rights, available at: [https://gdprhub.eu/index.php?title=Article_6_GDPR], Accessed 15 April 2023.

42 The most common examples are the monitoring of employees to improve safety and productivity.

43 See Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller, *op. cit.* note 39, at pp. 23-33.

location data), the way the information is being processed (whether the data are made accessible to a large number of persons), the reasonable expectations of the data subjects, as well as the status of the data subject (children and other vulnerable natural persons may require special protection).[44]

If the preliminary analysis, carried out by the data controller, does not give a clear answer as to which way the balance should be struck, the data controller may introduce additional measures to secure appropriate balance, including the possibility for unconditional opt-outs, immediate deletion of data after use, functional separation and anonymisation techniques, or other privacy-enhancing technologies.[45] It should be noted that specific rules apply if the data processed come under the special categories provided for by Art. 9 GDPR.

3.3. Specific rules in case of special categories of data

Article 9 contains a general prohibition for the processing of special categories of data; data that are considered to be particularly sensitive such as those revealing racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership as well as genetic data, biometric data, data concerning health or data concerning sex life or sexual orientation. Furthermore, Article 10 of the GDPR contains specific rules on personal data relating to criminal convictions and offences, thus also allowing for derogation from the general rules.

In the case of sensitive data, the GDPR provides for stricter standards: processing is prohibited with a few exceptions. For us, Art. 9(2)(b), (f) and (h) might be of interest, allowing data processing if data are necessary for employment and social security purposes, for the establishment, exercise or defence of legal claims as well as for medicinal purposes, and for the provision of health services.

3.4. Principles relating to the processing of personal data

As noted above, workers have to accept a certain degree of intrusion in their privacy; nevertheless, the level of acceptable interference is circumvented by various principles, set out in Article 5, such as (1) lawfulness, fairness and transparency; (2) purpose limitation; (3) data minimisation; (4) accuracy, (5) storage limitation, and (6) integrity and confidentiality.

---

44 *Ibid*., pp. 36-41. See also GDPR recital 75.

45 Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller, *op. cit.* note 39, at pp. 41-42.

(1) Lawfulness, fairness, and transparency. The data subject, workers in our case, must be properly informed about the data processed by their employers. Such processing might violate the GDPR not because the processing in itself is unlawful but because of the lack of information about them. The information must be provided in a concise, transparent, intelligible, and easily accessible form, using clear and plain language.[46]

Article 29 Working Party recommends the use of layered privacy notices. *The first layer*, a warning sign, must set out the purposes of processing, the identity of the controller, a description of the rights of the data subject, and a reference to the second layer. The sign must be placed so that the data subject can easily recognize the circumstances of the surveillance before entering the monitored area. *The second layer*, put at an easily accessible place or accessible easily, shall contain in a detailed manner all the mandatory information set by the GDPR.[47] For instance, in the case of video surveillance, workers should be aware of its existence, the places monitored, and the purposes of the surveillance (security-related, performance-related, etc.). In addition, controllers shall specify the consequences of processing, e.g. whether it might lead to disciplinary or criminal consequences. Transparency is applicable regardless of the legal basis for processing and throughout the processing life cycle.[48]

(2) Purpose limitation. The purpose limitation principle embodies the proportionality principle and serves as a safeguard against function creep. The data collected must not be used for purposes that are incompatible with the specified, predefined original purpose. Therefore, if surveillance is used for security purposes, the data collected in this way cannot be used for performance-related purposes. The aim of data collection must be legitimate and must be specific – broadly defined purposes are incompatible with this requirement.[49]

(3) Data minimisation. Article 5(1)c) is another manifestation of the principle of proportionality, whereby it provides that personal data shall be adequate, relevant, and limited to what is necessary. This is a stricter requirement than its counterpart in the Data Protection Directive (Article 6(1)c)), where the test could be passed

---

46 GDPR Art 12.

47 Article 29 Data Protection Working Party, Guidelines on transparency under Regulation 2016/679, 29 November 2017, last revised 11 April 2018, WP260rev.01, paras. 17, 35-36 and 38. See also European Data Protection Board, Guidelines 3/2019 on processing of personal data through video devices, *op. cit.*, note 38, para. 111.

48 Article 29 Data Protection Working Party, Guidelines on transparency, *op. cit.*, note 47, para. 5.

49 "Video surveillance based on the mere purpose of "safety" or "for your safety" is not sufficiently specific.", European Data Protection Board, Guidelines 3/2019 on processing of personal data through video devices, *op. cit.*, note 38, p. 9. See also Article 8(2) of the EU Charter.

with the collected data not being "excessive". Arguably, data protection law contains "an overarching proportionality principle, meant to even out the power and information asymmetry running between data controllers and data subjects."[50]

(4) Accuracy. Data must be accurate and kept up to date; and, since inaccurate information can have a harmful impact on data subjects, such data must be erased or rectified without delay. Although this principle is applicable to objective facts, as well as forecasts and correlations, value judgments cannot be required to be "corrected".

(5) Storage limitation. The temporal dimension of data minimisation, the principle of storage limitation requires that data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. This creates a positive obligation for the data controller to delete the data. The GDPR provides for an exception, thus storage in the public interest, scientific or historical research purposes, or statistical purposes is allowed.[51]

(6) Integrity and confidentiality. The last principle stipulates that data shall be processed in a manner that ensures appropriate security of personal data. Data must be protected against unauthorised access and unauthorised processing. In order to comply with this principle, the controller is obliged to introduce appropriate technical or organisational measures, having regard to the substantive and organisational contours specified in Article 32 GDPR.

Finally, it should be noted that Article 88 GDPR expressly authorizes Member States to regulate the processing of data in the context of employment. The list is open-ended and includes processing personal data for the purposes of recruitment, performance of the contract of employment, including management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of the property of the employer or customer. However, such special rules must comply with certain requirements regarding human dignity, legitimate interests, and fundamental rights.[52]

---

50 Dalla Corte, L., *On proportionality in the data protection jurisprudence of the CJEU*, International Data Privacy Law, Vol. 12, No. 4, 2022, pp. 259-275, at p. 264.

51 GDPR Art. 89(1).

52 On the relation between the first and the second paragraph of Art. 88, see Case C-34/21 *Hauptpersonalrat der Lehrerinnen und Lehrer beim Hessischen Kultusministerium v. Minister des Hessischen Kultusministeriums*, judgment of 30 March 2023, ECLI:EU:C:2023:270, paras. 73 and 74.

4. WORKPLACE SURVEILLANCE TESTED: RECENT CASE LAW OF THE STRASBOURG COURT

4.1. Preliminary comments

Before embarking on an analysis of European case law, the following points should be clarified. First, based on the search on the Court's website and EUR-Lex,[53] the Luxembourg Court apparently has not yet had the opportunity to pronounce on workplace surveillance. Several aspects of the GDPR have been addressed, including email marketing, online sale, customers' rights, the systematic recording of biometric and genetic data by the police,[54] the parallel exercise of administrative and civil remedies provided for in the GDPR,[55] the information regarding the recipients of personal data,[56] the identification of the holders of IP addresses suspected of online copyright infringement,[57] the right to erasure,[58] the general and indiscriminate retention of traffic data by operators providing electronic communications services,[59] and general and indiscriminate retention of traffic and location data relating to customers telecommunications,[60] just to name a few from the last year. Workplace surveillance, however, was not raised before the Court. Thus, further examination will focus on the ECHR case law, based on the premise that such an interpretation is also relevant for EU law. The right to protection of personal data is guaranteed by Article 8 of the EU Charter of Fundamental Rights. The Charter provisions are binding on the Member States when they implement Union law, which clearly includes the GDPR. Thus, Member States must have due regard to Article 8 of the Charter when implementing the GDPR. These provisions, read in conjunction with Art. 52(3) of the Charter[61] entails the obligation

---

53 The links:
[https://curia.europa.eu/juris/recherche.jsf?language=en] and
[https://eur-lex.europa.eu/homepage.html], respectively. The text searched was "workplace surveillance". The GDPRhub site was also consulted.

54 Case C-205/21 *Ministerstvo na vatreshnite raboti,* 26 Jan 2023, ECLI:EU:C:2023:49.

55 Case C-132/21 *BE v. Nemzeti Adatvédelmi és Információszabadság Hatóság*, 12 January 2023, ECLI:EU:C:2023:2.

56 Case C-154/21 *RW v. Österreichische Post*, 12 Jan 2023, ECLI:EU:C:2023:3.

57 Case C-470/21 *La Quadrature du Net et al. v. Premier ministre, Ministère de la Culture*; pending.

58 Case C-129/21 *Proximus NV v. Gegevensbeschermingsautoriteit*, 27 October 2022, ECLI:EU:C:2022:833.

59 Case C-339/20 *Criminal proceedings against VD*, *SR* (C-397/20), 20 September 2022, ECLI:EU:C:2022:703.

60 Joined Cases C-793/19 and C-794/19, *Bundesrepublik Deutschland v. SpaceNet AG and Telekom Deutschland GmbH*, 20 Sep 2022, ECLI:EU:C:2022:702.

61 Charter of Fundamental Rights of the European Union, OJ C 202, 7.6.2016, p. 391–407, Art. 52(3): "In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights

that the case law of the European Court of Human Rights be taken into account when interpreting the GDPR.

The most relevant (and recent) ECHR case law is concerned with emails (*Bărbulescu* v. *Romania* [GC]),[62] interception of telephone communications during criminal intelligence investigation (*Adomaitis*),[63] images (e.g. *López Ribalda and Others* v. *Spain* [GC]),[64] computer files (*Libert* v. *France*)[65] and geolocation data (*Florindo de Almeida Vasconcelos Gramaxo* v. *Portugal*).[66]

Second, as mentioned above, it is unreasonable to assume that an employer does nothing private in his workplace during work. The Court is clearly of the view that the right to private life encompasses activities that take place at work,[67] and the reasonable expectation of privacy of workers in those particular circumstances is an important element to be considered during the balancing act.[68]

Third, new technology, the appearance of more intrusive methods, coupled with the (sometimes involuntary) spread of teleworking, poses new challenges to the protection of privacy. Finally, our investigation is limited to one type of data processing, namely, workplace surveillance, more specifically, monitoring employees for security or performance-related reasons. Thus, personal data related to payroll, taxation, social security contributions, etc. do not form part of our investigation.

4.2. The test developed in *Bărbulescu*

The cases lodged with the Strasbourg Court relating to workplace surveillance involved both public authorities and private companies as employers. Therefore, the Court had the opportunity to pronounce on situations involving the State's negative obligations (no interference of a public authority in private life), as well as positive obligations (the positive obligations of States to ensure effective respect

shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.".

62 *Bărbulescu*.

63 *Adomaitis v. Lithuania,* Application no. 14833/18, 18 January 2022 (hereinafter: *Adomaitis*).

64 *López Ribalda and Others v. Spain* [GC], Applications nos. 1874/13 and 8567/13, 17 October 2019. (hereinafter: *López Ribalda).*

65 *Libert v. France*, Application no. 588/13, 22 February 2018 (hereinafter *Libert*).

66 *Florindo de Almeida Vasconcelos Gramaxo v. Portugal*, no. 26968/16, 13 December 2022.

67 "The sphere of professional activities and premises does not, therefore, in principle fall outside the protection afforded by Article 8 of the Convention." *Gottfried Niemietz* v. *the Federal Republic of Germany*, no. 13710/88, Report of the Commission of 29 May 1991, para. 56. See also *Bărbulescu* paras. 70-72 and 80.

68 *Bărbulescu*, paras 73-81.

of the rights protected by Article 8).[69] Although in *Bărbulescu*, France argued that States had to enjoy a wide margin of appreciation in this sphere since the aim was to strike a balance between competing private interests, the Court found that "[w]hile the boundaries between the State's positive and negative obligations under the Convention do not lend themselves to precise definition, the applicable principles are nonetheless similar."[70] However, the Court has apparently shown a marked restraint when assessing States' positive obligations.[71]

As has been noted, consent cannot serve as the legal basis for workplace surveillance. The opinions and guidelines adopted by the Article 29 Working Party and the EDPB are consequent in arguing that due to the imbalance in the employment context, consent cannot generally be assumed to form the legal basis,[72] and the most adequate ground is the legitimate interest of the employer to protect its property interests, to guarantee safe working environment, and to monitor employee performance.

Surveillance can be both overt and covert, that is, carried out with or without the subject's knowledge. In the case of overt surveillance, for example, where cameras are visible or the worker is informed that his correspondence is monitored, the crucial issue is the transparency of the employer's policy. Thus, in *Libert*, relating to the opening of personal files stored on a professional computer, the applicant lost the case due to mislabelling his personal files on his computer at work. The User's Charter (the employer's regulation) specifically stated that private information must be clearly identified as such. The employer tolerated the occasional and reasonable use of the computer for personal purposes and could not surreptitiously open files identified as being personal "unless there was a serious risk or in exceptional circumstances". Furthermore, personal files could only be opened in the presence of the employee concerned or after the latter had been duly informed.[73] Here, as the files containing pornographic files and forged certificates drawn up for third persons had not been duly identified as being private, the employer could justify the opening of files based on the protection of the rights

---

69 *Bărbulescu*, para. 108; *Libert*, para. 41.

70 *Bărbulescu*, paras. 106 and 112.

71 See *López Ribalda* below.

72 See e.g. Article 29 Data Protection Working Party Opinion 8/2001on the processing of personal data in the employment context, *op. cit*., note 29, at p. 3, Article 29 Data Protection Working Party, Opinion 2/2017 on data processing at work (WP249), *op. cit.* note 37, para. 6.2.; Article 29 Working Party, Guidelines on consent under Regulation 2016/679, *op. cit.* note 38, at p. 7.; para. 47 of the European Data Protection Board, Guidelines 3/2019 on processing of personal data through video devices, *op. cit*. note 38, or para. 21 of the European Data Protection Board, Guidelines 05/2020 on consent, *op. cit.* note 32.

73 *Libert* para. 48.

of the employer,[74] however, only in the presence of the employee, a condition not satisfied here. Thus, the no-infringement decision was based on the argument that the files at issue had not been duly identified as being private.

In any case, the *Libert* case does not change the rule laid down in *Niemietz* that employees are entitled, even during working time and at the workplace, to respect for their privacy. Even when the computers are provided to the workers for exclusively professional purposes, the employer must tolerate occasional private use. In such circumstances, the employer must demonstrate compelling legitimate grounds underpinning surveillance measures. In *Bărbulescu*,[75] the Court has developed a six-point test to assess whether employee monitoring is justified. The test, relating to notification, extent of surveillance, level of intrusion, consequence for the employee, and the safeguards in place, provides guidance to strike a balance between the employer's interest in supervising its staff and the individual's right to respect for their private life.

In fact, in *Bărbulescu*, the ECtHR set out a six-point test to assess whether the national authorities had struck a fair balance between the competing interests at issue.[76] The test, relating to notification, extent of surveillance, level of intrusion, consequence for the employee, and the safeguards in place, provides guidance in striking a balance between the employer's interest in supervising its staff and the individual's right to respect for their private life.

First, it must be determined whether the employee has been notified of the possibility that the employer might take measures to monitor correspondence. The notification must be clear about the nature of the monitoring and be given in advance. However, the practical significance of the information element is reduced by several factors. First, the underlying assumption of notification is that the workforce makes choices based on a more complete set of information. Indeed, sufficient information about the nature of surveillance may serve as a basis to make an informed employment choice; nevertheless, all too often the feasibility of seeking an alternative job is illusory. Second, the notification factor is a double-edged sword. If failure to inform is contrary to human rights and EU law, is the

---

74 Legitimate aim of guaranteeing the protection of "the rights ... of others", in this case the rights of employers (*Libert* para. 46). The other justification raised – legitimate aim of preventing crime – was refused by the Court since "the opening of the files in question was not done in the context of the criminal proceedings", *Libert* para. 45.

75 *Bărbulescu*, para 121.

76 *Bărbulescu*, para 121.

opposite true? Can it be argued that actual information justifies surveillance?[77] The answer is obviously negative: monitoring harms the worker even when he knows it is happening;[78] and thus, information should be regarded as a threshold, a point of departure for the compatibility analysis.

The second principle focuses on the extent of the surveillance and the degree of intrusion into the employee's privacy, with various elements to be taken into account, including a distinction between the monitoring of the flow of communication and its content, whether all communications or only part of them have been monitored, the temporal and spatial limits of surveillance, and the number of people who had access to the results.

Third on the list, but arguably better positioned before the second criterion, is whether the employer has provided legitimate reasons to justify monitoring of the communications and accessing of their actual content. The fourth criterion is a proportionality-related one: the employer must establish that the monitoring system is implemented in the least intrusive manner possible. The expectation of privacy varies depending on the place scrutinized and surveillance must be tailored accordingly. In the Court's analysis, this expectation is very high in places that are private in nature, such as toilets or cloakrooms, where increased protection or even a complete ban on video-surveillance, is justified. It remains high in closed working areas, such as offices, while it is significantly lower in places that are visible or accessible to colleagues or the general public.[79]

The fifth criterion relates to the consequences of the monitoring for the employee who is subjected to it, while the sixth provides for the assessment of whether the employee had been provided with adequate safeguards to ensure that the employer cannot access the actual content of the communications concerned unless the employee has been notified in advance of that eventuality.[80]

---

77 Collins, P., *The Right to Privacy, Surveillance-by-Software and the "Home-Workplace"*, 3 September 2020, available at:
[https://uklabourlawblog.com/2020/09/03/the-right-to-privacy-surveillance-by-software-and-the-home-workplace-by-dr-philippa-collins/], Accessed 15 April 2023.

78 See e.g. Jervis, C.E.M., *Barbulescu v Romania: Why There is no Room for Complacency When it Comes to Privacy Rights in the Workplace*, 26 September 2017, available at:
[https://www.ejiltalk.org/barbulescu-v-romania-why-there-is-no-room-for-complacency-when-it-comes-to-privacy-rights-in-the-workplace/], Accessed 15 April 2023, or Ramasundaram, A.; Gurusamy, R., George, A., *Employees and workplace surveillance: Tensions and ways forward*, Journal of Information Technology Teaching Cases, 2022, pp. 1-5. Systematic monitoring has a marked impact on the individual's well being, productivity at work, causing anxiety and discomfort.

79 *López Ribalda* para. 125.

80 To this, the Court adds the requirement of adequate judicial remedy (access to a remedy before a judicial body, *Bărbulescu,* para. 122).

4.3. Covert surveillance

The test can also be applied to *covert* surveillance, as evidenced by *López Ribalda* where, after noticing irregularities between the stock in the shop and its sales and finding losses over five months, the manager of a supermarket installed both visible and hidden CCTV cameras. Although the employer had given workers notice of the installation of visible cameras, the employees were not informed for obvious reasons of the hidden ones. Soon afterwards, the manager showed a film of the applicants and other staff participating in the theft of goods in the shop to a union representative. The applicants were dismissed on disciplinary grounds, which they challenged, arguing that the covert video material collected in violation of their privacy rights could not be admitted in evidence.

The Chamber's conclusion was that, having regard to the extent of the surveillance – not being limited in time, affecting all employees working at the tills and covering all working hours – and to the lack of prior information, Spain has violated Article 8.[81] This decision was, however, reversed by the Grand Chamber, which concluded that the national authorities did not fail to fulfil their positive obligations under Article 8.

The Grand Chamber found that since the applicants worked in a supermarket that was a public place, their expectation of protecting their private life was necessarily limited.[82] The Court's analysis was based on the assumption that the principles developed in *Bărbulescu* relating to the monitoring of the correspondence and communications of employees were transposable to the installation of video-surveillance in the workplace.[83] After a rather perfunctory examination, the Court concluded that the Spanish authorities (the Employment Court) had not overstepped the margin of appreciation afforded to them. While the lack of information is in principle not acceptable, there might be certain exceptions, such as in the present case, justified by the existence of reasonable suspicion that serious misconduct has been committed and by the extent of the losses.[84]

In terms of the extent of the surveillance and the degree of intrusion into the employee's privacy, the Court found that the monitoring had been limited to what was necessary in relation to both the area and the employees being monitored. Surveillance took place in an area that was open to the public and involved permanent contact with customers. Therefore, employees' expectation of privacy was lower

81 *López Ribalda* para. 79.

82 *López Ribalda* para. 93.

83 *López Ribalda* para. 116.

84 *López Ribalda* para. 134.

than in places that were private. The duration of surveillance had not been excessive and did not go beyond what was necessary to confirm the suspicions of theft. The recordings had only been viewed by certain individuals before the employees had been informed (the manager, the employer's legal representative, and a trade union representative).[85] Regarding the employer's legitimate reasons, the Court took into account the significant losses recorded over several months and the intention to punish those responsible. The aims of ensuring the protection of its property and the smooth functioning of the company were found to be legitimate.[86]

Unfortunately, the fourth criterion regarding the intrusiveness of the measures was investigated in a rather half-hearted manner. The "European supervision" by the Court of the domestic margin of appreciation was arguably rather unsatisfactory. The Court accepted the assessment of the national authorities without much ado, despite the admission that "it would have been desirable for the domestic courts to examine in a more in-depth manner the possibility for the employer to have used other measures entailing less intrusion into the private life of the employees".[87]

The Court conceded that the consequences of the monitoring for the employees were very serious, nevertheless, it found that the surveillance had not been used for any purposes other than to investigate the thefts and to take the disciplinary measures against those responsible,[88] and the Court was also satisfied with the safeguards prescribed by domestic law.[89]

On the whole, *López Ribalda* is disconcerting inasmuch as the Court seemed to underestimate the risks of digital means of surveillance and its high level of intrusiveness.[90] Although the national courts failed to address the issue of whether a less restrictive measure could have been used by the employer to pursue the same aim, the Court was quick to accept the conclusions of the national authorities without a thorough analysis.

---

85 *López Ribalda* paras. 124 to 126. The monitoring lasted for ten days, which does not appear excessive: even though originally the employer had not set the duration but ceased as soon as the employees responsible had been identified.

86 *López Ribalda* para. 123.

87 *López Ribalda* para. 128. – See pee para. 49 of *Handyside v. the United Kingdom*, no. 5493/72, 7 December 1976, providing that "[t]he domestic margin of appreciation … goes hand in hand with a European supervision.".

88 *López Ribalda*, para. 127.

89 *López Ribalda*, para. 129.

90 Bregiannis, F.; Chatzinikolaou, A., *López Ribalda and Others v. Spain – covert surveillance in the workplace: attenuating the protection of privacy for employees*, 6 December 2019, available at: [https://strasbourgobservers.com/2019/12/06/lopez-ribalda-and-others-v-spain-covert-surveillance-in-the-workplace-attenuating-the-protection-of-privacy-for-employees/], Accessed 15 April 2023.

In *Adomaitis v. Lithuania*, another covert surveillance case, the governor of a prison was suspected of abusing his office in order to offer better conditions for some inmates. In the course of a criminal investigation, during one year his telephone communications were monitored and intercepted. Subsequently, lacking sufficient evidence to charge the applicant, the criminal intelligence investigation was discontinued. However, the information collected was allowed in a disciplinary proceedings that ultimately led to his dismissal. The applicant contested the lawfulness of using the information collected through covert surveillance.

The Court accepted the necessity of covert surveillance, since the applicant was the director of a protected incarceration facility, which significantly reduced other means for a criminal investigation.[91] A different issue is whether the use of that information in the disciplinary proceedings was proportionate. Here, the decisive elements were the applicant's position as the director of a prison, and the seriousness of the acts that were investigated, thus the Court agreed with the conclusions of the national authorities.[92] The Court also noted that the dismissal of the applicant was based not only on the intercepted communications, but also on other evidence, including contracts with the telecommunications company and witness testimony.[93] Even so, one cannot but challenge the accuracy of the Court's finding that the handing-over of the information thus obtained for the purposes of non-criminal proceedings was legitimate.[94]

The Court's assessment of the surveillance measures in *Florindo de Almeida Vasconcelos Gramaxo* v. *Portugal*[95] is also disconcerting. The case was related to data on the mileage of the applicant's company vehicle, collected using a GPS device originally installed by the applicant's employer to his full knowledge. Therefore, workers, including the applicant, were informed of the reasons for the measure (to monitor the distances travelled), as well as that disciplinary measures can be brought against them based on the data thus collected. Employees were not allowed to deactivate the geolocation system. The company allowed the use of the vehicle for private journeys and trips outside work hours, although the expenses associated with private trips had to be reimbursed.

When the employer became aware that the applicant had tampered with the system, a second hidden GPS was installed. The applicant was dismissed when it

---

91 *López Ribalda*, paras. 7 and 85.

92 *Adomaitis*, para. 87.

93 *Adomaitis*, para. 71.

94 See e.g. the partly dissenting opinion of Judge Koskelo.

95 No English translation of the judgment is available, but a the ECtHR's summary is available here: [https://bit.ly/41zwW5W].

was disclosed that he manipulated the device. At first instance, the dismissal was found to be justified, a conclusion supported by the appeal court, but on different grounds. The appeal court found that GPS constituted a means of remote surveillance prohibited by the Portuguese Labour Code. However, although GPS could not be used to monitor the observance of the required working hours, the employer was justified to use it to determine the distances travelled. By interfering with the operation of the GPS, the applicant breached his duty of loyalty to his employer.

The majority of the Strasbourg Court found that the interpretation of the appeal court significantly reduced the extent of intrusion. In these circumstances, the monitoring did not overstep what was strictly necessary to protect the legitimate aim of the employer, namely to monitor expenditure. However, in our view, the Court's assessment of the extent of intrusion continues to be problematic. The Court failed to consider that there had been a permanent 24/7 surveillance for three years, and that the GPS monitored the employees outside of working hours, during their free time as well. This seems hardly to be reconcilable with the principle of proportionality.

5. CONCLUSIONS

In this paper, we have described the European legislative framework and outlined the current practice of the European Court of Human Rights. The principles in the GDPR and the test developed in *Barbulescu*, while not identical, seem to address the same important concerns, including the lawfulness and legitimacy of data processing, notification, and several aspects of proportionality. Furthermore, both regimes appear to be flexible enough to cover a wide range of situations and to adapt to rapid changes in technology.

No doubt, prevention is better than cure. Before the introduction of surveillance measures or the installation of devices, employers should consider whether preventive measures are available, such as the use of filters in the case of monitoring of personal data relating to Internet or intranet pages accessed by the employee.[96] Admittedly, this is not always feasible.

So far, the Court of Justice of the European Union had no possibility to pronounce upon workplace surveillance; nevertheless, it has emphasised that the right

[96] Committee of Ministers, Recommendation CM/Rec(2015)5 to member states on the processing of personal data in the context of employment, April 2015, point 14.2.

to data protection is not absolute, and must be considered in relation to its function in society.[97]

In its judgments of the last few years, the European Court of Human Rights was called upon to assess whether the monitoring of telephone and internet use (*Bărbulescu*, *Adomaitis*), the opening of personal files on a professional computer (*Libert*), video surveillance (*López Ribalda*), and the use of geolocation system (*Florindo*) are compatible with the right to privacy.

Setting out specific factors to assess the proportionality of monitoring activities in *Bărbulescu* is a welcome development. However, in subsequent cases, the Court granted an inexplicably wide margin of appreciation to States, which resulted in insufficient protection to workers. Our research has demonstrated that in *López Ribalda* and *Florindo*, the Strasbourg Court showed an unexplainable restraint in the "supervision" of the domestic margin of appreciation. It is disappointing to see the blow the information criterion has suffered in López Ribalda, where the Court found no violation of Article 8 *even in the absence of notification* of the employees; it simply claimed that the other factors were all the more crucial if no notification had taken place. The employers' interests were deemed a necessary means to achieve legitimate and proportionate purposes of the employer.

Despite the increasing acceptance of surveillance technologies in society, employee monitoring must meet strict requirements and remain within what is legitimate and necessary. National legislators should modernise national regulatory frameworks, including the correct implementation of the GDPR in the case of the EU Member States, and addressing the challenges posed by modern forms of intrusive surveillance. Employers should ensure that their monitoring policy is clear and transparent, complies with national law, and preferably is developed through consultation with employees. Finally, given the imbalance of power between employers and employees, European supervision should show a certain restraint in the application of the margin of appreciation principle, and strike a proper balance between the competing interest.

REFERENCES

JOURNALS

1. Abraha, H.H., *A pragmatic compromise? The role of Article 88 GDPR in upholding privacy in the workplace*, International Data Privacy Law, Vol. 12, no. 4, 2022, pp. 276-296

[97] See e.g. Case C-311/18 *Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems*, 16 July 2020, ECLI:EU:C:2020:559, para 172, Case C-511/18 *La Quadrature du Net*, 6 October 2020, para. 120.

2. Atkinson, J., *Workplace Monitoring and the Right to Private Life at Work*, Modern Law Review, Vol. 81, No. 4, 2018, pp. 688-700
3. Ball, K., *Workplace surveillance: an overview*, Labor History, Vol. 51, 2010, pp. 87-106
4. Brassart Olsen, C., *To track or not to track? Employees' data privacy in the age of corporate wellness, mobile health, and GDPR*. International Data Privacy Law, Vol. 10, No. 3, 2020, pp. 236–252
5. Collins, P.; Marassi, S., *Is That Lawful? Data Privacy and Fitness Trackers in the Workplace*, International Journal of Comparative Labour Law and Industrial Relations, Vol. 37, No. 1, 2021, pp. 65-94
6. Custers, B., Louis, L., Spinelli, M., Terzidou, K., Quis custodiet ipsos custodes? Data protection in the judiciary in EU and EEA Member States, *International Data Privacy Law*, Vol. 12, No. 2, 2022, pp. 93-112
7. Dalla Corte, L., *On proportionality in the data protection jurisprudence of the CJEU*, International Data Privacy Law, Vol. 12, No. 4, 2022, pp. 259-275
8. Garden, C., *Labor Organizing in the Age of Surveillance*, Saint Louis University Law Journal, Vol. 63, 2018, pp. 55-68
9. Gonçalves, M.E., *The risk-based approach under the new EU data protection regulation: a critical perspective*, Vol. 23 No. 2, 2020, pp. 139-152
10. Hustinx, P., *Data protection and international organizations: a dialogue between EU law and international law*, International Data Privacy Law, Vol. 11, No. 2, 2021, pp. 77-80
11. Komanovics, A., *Hungary and the Luxembourg Court: The CJEU's Role in the Rule of Law Battlefield*. In: EU and Comparative Law Issues and Challenges Series (ECLIC), Vol. 6, 2022, pp. 122-157
12. Koops, B.J., *The concept of function creep*, Law, Innovation and Technology, 2021, Vol. 13, No. 1, pp. 29-56
13. Kuner, C., Cate, F.H., Lynskey, O., Millard, C., Ni Loideain, N., Svantesson, D.J.B., *If the legislature had been serious about data privacy …*, International Data Privacy Law, Vol. 9, No. 2, 2019, pp. 75–77
14. Leccese, V. S., *Monitoring working time and Working Time Directive 2003/88/EC: A purposive approach*, European Labour Law Journal, Vol. 14, No. 1, 2022, pp. 21-34
15. Lintvedt, M.N., *Putting a price on data protection infringement*, University of Oslo Faculty of Law Research Paper No. 2022-56, Vol. 12, No. 1, 2022, pp. 1-15
16. Molè, M., *The Internet of Things and Artificial Intelligence as Workplace Supervisors: Explaining and Understanding the New Surveillance to Employees Beyond Art. 8 ECHR*, Italian Labour Law E-Journal, Vol. 15 No. 2, 2022, pp. 87–103
17. Nogueira Guastavino, M., *Geolocalización lícita, probablemente desproporcionada. La necesidad de una vigilancia cualitativa, no cuantitativa*, Revista de Jurisprudencia Laboral, Vol. 5, No. 2, 2023, pp. 1-11
18. Quelle C., *Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-Based Approach*, European Journal of Risk Regulation, Vol. 9, No. 3, 2018, pp. 502-526

19. Ramasundaram, A.; Gurusamy, R., George, A., *Employees and workplace surveillance: Tensions and ways forward*, Journal of Information Technology Teaching Cases, 2022, pp. 1-5
20. Veale, M., Binns, R., Ausloos, J., *When data protection by design and data subject rights clash*, International Data Privacy Law, Vol. 8, No. 2, 2018, pp. 105-123

WEBSITE REFERENCES

1. Bakos, A.C., *The European Court of Human Rights and Workplace Surveillance: Where is Article 31(3)(c) VCLT?*, 14 November 2019, available at: [https://www.ejiltalk.org/the-european-court-of-human-rights-and-workplace-surveillance-where-is-article-313c-vclt/], Accessed 15 April 2023
2. Ball, K., *Electronic Monitoring and Surveillance in the Workplace*, Publications Office of the European Union, Luxembourg, 2021, available at: [https://publications.jrc.ec.europa.eu/repository/handle/JRC125716], Accessed 15 April 2023
3. Bregiannis, F.; Chatzinikolaou, A., *López Ribalda and Others v. Spain – covert surveillance in the workplace: attenuating the protection of privacy for employees*, 6 December 2019, available at: [https://strasbourgobservers.com/2019/12/06/lopez-ribalda-and-others-v-spain-covert-surveillance-in-the-workplace-attenuating-the-protection-of-privacy-for-employees/], Accessed 15 April 2023
4. Chatzinikolaou, A., *Bărbulescu v Romania and workplace privacy: is the Grand Chamber's judgment a reason to celebrate?*, 19 October 2017, available at: [https://strasbourgobservers.com/2017/10/19/barbulescu-v-romania-and-workplace-privacy-is-the-grand-chambers-judgment-a-reason-to-celebrate/], Accessed 15 April 2023
5. Coe, P., *A Brave New Working World or something more sinister? Employer surveillance of employees working at home*, 4 November 2020, available at: [https://inforrm.org/2020/11/04/a-brave-new-working-world-or-something-more-sinister-employer-surveillance-of-employees-working-at-home-peter-coe/], Accessed 15 April 2023
6. Coe, P., *The European Court of Human Rights and the right to privacy in the workplace, Bărbulescu and Lopez Ribalda*, 15 November 2019, available at: [https://inforrm.org/2019/11/15/the-european-court-of-human-rights-and-the-right-to-privacy-in-the-workplace-barbulescu-and-lopez-ribalda-peter-coe/], Accessed 15 April 2023
7. Collins, P., *The Right to Privacy, Surveillance-by-Software and the "Home-Workplace"*, 3 September 2020, available at: [https://uklabourlawblog.com/2020/09/03/the-right-to-privacy-surveillance-by-software-and-the-home-workplace-by-dr-philippa-collins/], Accessed 15 April 2023
8. GDPRhub / European Center for Digital Rights, available at: [https://gdprhub.eu/index.php?title=Welcome_to_GDPRhub], Accessed 15 April 2023
9. Jervis, C.E.M., *Barbulescu v Romania: Why There is no Room for Complacency When it Comes to Privacy Rights in the Workplace*, 26 September 2017, available at: [https://www.ejiltalk.org/barbulescu-v-romania-why-there-is-no-room-for-complacency-when-it-comes-to-privacy-rights-in-the-workplace/], Accessed 15 April 2023
10. Mansoori, S., *Case Law, Strasbourg: Bărbulescu v Romania – Monitoring of an employee's communications held to be violation of Article 8 ECHR*, 2017, available at: [https://inforrm.

org/2017/09/12/case-law-strasbourg-barbulescu-v-romania-monitoring-of-an-employees-communications-held-to-be-violation-of-article-8-echr-sara-mansoori/], Accessed 15 April 2023

11. Molè, M., *Just more surveillance? Rethinking the 'pressing social need' for AI surveillance under the ECHR*, 14 February 2023, available at: [https://cooperante.uni.lodz.pl/2023/02/14/%EF%BB%BFjust-more-surveillance-rethinking-the-pressing-social-need-for-ai-surveillance-under-the-echr/], Accessed 15 April 2023
12. Mukherjee, G.; Wookey, J., *Resuscitating Workplace Privacy? A Brief Account of the Grand Chamber Hearing in Bărbulescu v. Romania*, 20 December 2016, available at: [https://strasbourgobservers.com/2016/12/20/resuscitating-workplace-privacy-a-brief-account-of-the-grand-chamber-hearing-in-barbulescu-v-romania/], Accessed 15 April 2023
13. Peers, S., *Is Workplace Privacy Dead? Comments on the Barbulescu judgment*, 14 January 2016, available at: [http://eulawanalysis.blogspot.com/2016/01/is-workplace-privacy-dead-comments-on.html], Accessed 15 April 2023
14. Richmond, K., *Case Law, Strasbourg: Barbulescu v Romania, Surveillance of Internet Usage in the Workplace*, 17 January 2016, available at: [https://inforrm.org/2016/01/17/case-law-strasbourg-barbulescu-v-romania-surveillance-of-internet-usage-in-the-workplace-kate-richmond/], Accessed 15 April 2023
15. Rojo, E., *La importancia de la jurisprudencia del Tribunal Europeo de Derechos Humanos en el ámbito laboral y de protección social (III). Arts. 8 y 6 del Convenio Europeo de Derechos Humanos. ¿Cuáles son los limites del control por geolocalización del vehículo de trabajo? Notas a la sentencia de 13 de diciembre de 2022. caso Alfonso Florindo de Almeida Vasconcelos Gramaxo contra Portugal (con tres votos radicalmente discrepantes)*, 5 January 2023, available at: [http://www.eduardorojotorrecilla.es/2023/01/la-importancia-de-la-jurisprudencia-del_5.html], Accessed 15 April 2023
16. Sicilianos, L.A., *Interpretation of the European Convention on Human Rights: Remarks on the Court's Approach*, Seminar on: "The Contribution of the European Court of Human Rights to the Development of Public International Law" on the margins of the 59th CAHDI meeting in Prague, Prague, 23 September 2020, available at: [https://rm.coe.int/interpretation-of-the-european-convention-on-human-rights-remarks-on-t/1680a05732], Accessed 15 April 2023

LEGAL ACTS

1. Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 005), 1950
2. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), 1981
3. Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (ETS No. 181), 2001
4. Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223), 2018

EU TREATIES

1. Treaty on European Union, TEU (Consolidated version 2016) [2016] OJ C202
2. Treaty on the Functioning of the European Union, TFEU (Consolidated version 2016) OJ C 202, 7.6.2016
3. Charter of Fundamental Rights of the European Union, OJ C 202, 7.6.2016, p. 391–407

EU SECONDARY LEGISLATION

1. 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, [1995] OJ L281/31, ELI: http://data.europa.eu/eli/dir/1995/46/oj
2. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications' sector (Directive on privacy and electronic communications), OJ 2002 L 201/37, ELI: http://data.europa.eu/eli/dir/2002/58/oj
3. Regulation (EU) 2016/679 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), [2016] OJ L119/1, ELI: http://data.europa.eu/eli/reg/2016/679/oj
4. Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Data Protection Law Enforcement Directive), [2016] OJ L119/89, ELI: http://data.europa.eu/eli/dir/2016/680/oj
5. Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, [2018] OJ L295/39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj

OTHER EU DOCUMENTS

1. European Commission, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 final – 2017/03 (COD)
2. European Commission, Commission Staff Working Document accompanying the document Communication from the Commission to the European Parliament and the Council. Data protection rules as a pillar of citizens empowerment and EUs approach to digital transition – two years of application of the General Data Protection Regulation, COM(2020) 264 Final

3. European Economic and Social Committee, Opinion on 'Challenges of teleworking: organisation of working time, work-life balance and the right to disconnect' (Exploratory opinion at the request of the Portuguese Presidency), EESC 2020/05278, [2021] C 220/01
4. European Union Agency for Fundamental Rights and Council of Europe, Handbook on European data protection law. Luxembourg: Publications Office of the European Union, 2018
5. Article 29 Data Protection Working Party, Opinion 8/2001 on the processing of personal data in the employment context, 5062/01/EN/Final, WP48
6. Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent, 13 July 2011, 01197/11/EN, WP187
7. Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 2 April 2013, 00569/13/EN, WP 203
8. Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 9 April 2014, 844/14/EN, WP 217
9. Article 29 Data Protection Working Party, Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), 13 April 2016, 16/EN, WP237
10. Article 29 Data Protection Working Party, Opinion 2/2017 on data processing at work, 8 June 2017, 17/EN, WP 249
11. Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679', 3 October 2017, 17/EN, WP251rev.01
12. Article 29 Data Protection Working Party, Guidelines on consent under Regulation 2016/679, 28 November 2017, last revised 10 April 2018, 17/EN, WP 259 rev. 01 – endorsed by the EDPB
13. Article 29 Data Protection Working Party, Guidelines on transparency under Regulation 2016/679, 29 November 2017, last revised 11 April 2018, WP260rev.01
14. European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8 October 2019
15. European Data Protection Board, Guidelines 3/2019 on processing of personal data through video devices. Version 2.0, 29 January 2020
16. European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679. Version 1.1, 4 May 2020
17. European Data Protection Board, Guidelines 10/2020 on restrictions under Article 23 GDPR. Version 2.0, 13 October 2021

CJEU CASE LAW

1. Case C-311/18 *Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems*, 16 July 2020, ECLI:EU:C:2020:559

2. Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others v. Premier ministre and Others*, 6 October 2020, ECLI:EU:C:2020:791
3. Joined Cases C-793/19 and C-794/19 *Bundesrepublik Deutschland v. SpaceNet AG and Telekom Deutschland GmbH*, 20 Sep 2022, ECLI:EU:C:2022:702
4. Case C-339/20 *Criminal proceedings against VD*, *SR* (C-397/20), 20 September 2022, ECLI:EU:C:2022:703
5. Case C-34/21 *Hauptpersonalrat der Lehrerinnen und Lehrer beim Hessischen Kultusministerium v. Minister des Hessischen Kultusministeriums*, 30 March 2023, ECLI:EU:C:2023:270
6. Case C-129/21 *Proximus NV v. Gegevensbeschermingsautoriteit*, 27 October 2022, ECLI:EU:C:2022:833
7. Case C-132/21 *BE v. Nemzeti Adatvédelmi és Információszabadság Hatóság*, 12 January 2023, ECLI:EU:C:2023:2
8. Case C-154/21 *RW v. Österreichische Post*, 12 Jan 2023, ECLI:EU:C:2023:3
9. Case C-205/21 *Ministerstvo na vatreshnite raboti,* 26 January 2023, ECLI:EU:C:2023:49)
10. Case C-470/21 *La Quadrature du Net et al.* v *Premier ministre, Ministère de la Culture*; [2021] OJ C462/25
11. Opinion of Advocate General Szpunar in Case C-439/19 *Latvijas Republikas Saeima*, ECLI:EU:C:2020:1054

ECtHR

1. *Adomaitis v. Lithuania,* Application no. 14833/18, 18 January 2022
2. *Bărbulescu v. Romania* [GC], Application no. 61496/08, 5 September 2017
3. *Florindo de Almeida Vasconcelos Gramaxo v. Portugal*, Application no. 26968/16, 13 December 2022
4. *Gottfried Niemietz v. the Federal Republic of Germany*, Application no. 13710/88, Report of the Commission of 29 May 1991
5. *Handyside v. the United Kingdom*, Application no. 5493/72, 7 December 1976
6. *Libert v. France*, Application no. 588/13, 22 February 2018
7. *López Ribalda and Others v. Spain* [GC], Application nos. 1874/13 and 8567/13, 17 October 2019

OTHER COUNCIL OF EUROPE DOCUMENTS

1. Venice Commission, Opinion on video surveillance by private operators in the public and private spheres and by public authorities in the private sphere and human rights protection (Venice, 1-2 June 2007), CDL-AD(2007)027)
2. Committee of Ministers, Recommendation CM/Rec(2015)5 to member states on the processing of personal data in the context of employment, April 2015

MISCELLANEOUS

1. OECD Guidelines governing the protection of privacy and transborder flows of personal data, (2013). C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79, available at: [https://edps.europa.eu/sites/default/files/publication/2013-09-09_oecd-privacy-guidelines_en.pdf], Accessed 15 April 2023
2. OECD, Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy, 2007, available at: [https://edps.europa.eu/sites/default/files/publication/2013-09-09_oecd_guidelines_en.pdf], Accessed 15 April 2023