Electronic surveillance in the workplace: Employee's privacy in the advent of technology

Paulo Pinto de Albuquerque[1]
Beatriz Albuquerque[2]

Introduction

The right to privacy is one of the biggest concerns nowadays. The commonly held idea that human rights violations mainly occur in less developed countries could not be further from the truth. Today's societies are driven by constant technological developments which greatly impact on the right to privacy of every person.

The workplace has been particularly affected by today's technological society: employers' monitoring of their employees has become increasingly easy and efficient compared to a few years ago, when surveillance was done by other people. Therefore, this topic relates to millions of ordinary people that are affected worldwide in their daily lives by abusive surveillance. It is also an issue in the intersection between human rights law and labour law, which increases its importance, since it becomes a topic of interest in both fields of law.

Europe is experiencing an increasing momentum to improve the existing laws on privacy in the workplace and to create them in the States where they still do not exist. That is why it is so relevant to discuss this topic nowadays.

The purpose of our research is to analyse the burning legal questions related to this European momentum and check if there is a European-wide standard.

For that purpose, in this paper we will address two types of electronic surveillance methods: video surveillance and computer surveillance of emails, social media or hard disk. Due to its importance, we will analyse the most recent case-law of the European Court of Human Rights (hereinafter, ECtHR)

[1] Full Professor at the Faculty of Law of the Portuguese Catholic University, Lisbon, and judge at the European Court of Human Rights.

[2] LLM in Transnational Law, jointly awarded by the Portuguese Catholic University, Lisbon, and the King's College, London. Law degree from the Portuguese Catholic University.

related to monitorization of employees through technological means. In particular, we will focus on the landmark case *Barbulescu*[3], which represented a big step forward in terms of the recognition of the employees' right to privacy in the workplace.

Additionally, we will provide an overview of the current international rules that govern this area, at the European level, including both the European Union and the Council of Europe, and at the global level, regulated by the United Nations.

What are the interests at stake?

Many employers consider that when their employees are at work, they should be expected to be observed by their supervisors[4], since they are not in their private time[5]. Nonetheless, this expectation seems not to be in line with the reality of most of today's workplaces. Workers spend the majority of their lives at work and it becomes implausible to expect employees to put their private lives on hold and devote 100% of working time to work related matters[6]. But what if the employees spend too much time with non-work-related matters via internet or electronic communications? Should the employer not be able to know if his employees are being productive and effective? The question of employees' monitoring by their employers is very interesting and challenging, precisely because it raises legitimate arguments from both sides.

The employer has indeed the prerogative to control what is happening in the workplace and the performance of his employees, but this does not give him a straightforward right to violate the employees' privacy. One could even argue that it does not matter how long an employee is occupied with personal matters, if he does the work he is being paid to do and does not access inappropriate websites. Furthermore, greater employees' freedom might even enhance their productivity since short pauses in work are scientifically proven to improve the ability to concentrate in a task[7]. These arguments would undermine the employer's claim to monitor based on the needs of efficiency control.

---

[3] ECtHR, *Barbulescu v. Romania* (no. 61496/08), 12 January 2016.

[4] Westin (1996), p.276.

[5] Oliver (2002), p.325.

[6] Morgan (1999), p.901.

[7] University of Illinois at Urbana-Champaign, 'Brief diversions vastly improve focus, researchers find', *ScienceDaily*, 8 February 2011.

However, employers have further legitimate concerns. The access to certain websites by their employees might lead to the exposure of the company's computers to viruses. Employees might also breach their duty of confidentiality to the company by releasing business secrets or specific know-how of the company. It is proven that "employees commit more computer crimes against their employers than third parties do"[8]. The employer also has an interest in avoiding any type of reputational damage that employees might cause. This damage may result from situations where employees have inappropriate conduct (e.g. posting drunken pictures of themselves online[9]) or express online criticism about the company and the employer. Monitoring in the latter case, due to its direct consequences to the employer, is seen as more proportional than the former. Additionally, it is well-known that employers might be vicariously held liable for the conduct of their employees. Therefore, employers have an interest in monitoring problematic conduct by the employees that might be associated to the corporation.

These are all practical instances where monitoring has a plausible justification. But is it proportionate to the benefits the employer will take from the interference with the employees' privacy? This is the crucial question one must ask.

The main interest of the employees to be balanced against the above-mentioned ones is the right to privacy. However, it should be noted that their freedom of expression might also be at stake when they are being monitored, because they may feel limited in what they can say or write. Likewise, employees also have an interest in keeping both their private and professional lives separated, which does not occur if employers examine their personal communications.

Additionally, the acceptance of an adequate use of the internet for personal purposes is considered beneficial for the employees' morale and self-esteem. As one scholar puts it, "blocking Net access has a negative effect on employee morale, as employees are likely to feel they are being treated as children"[10]. Having a more flexible approach will increase the employees' confidence that their employer trusts them and that will probably have positive effects in their productivity and motivation. If employees suspect of surveillance,

---

[8] The Harvard Law Review Association (1991), p. 1900.

[9] Svantesson (2012), p. 188.

[10] Policy (2000), p. 11.

they will limit their actions, independence of thought and creativity[11], which tends to be prejudicial for the company. Furthermore, monitoring can have counterproductive consequences, inasmuch as it stimulates employees to try to circumvent the system with more advanced techniques to use it for personal purposes.

The best way to balance the employer's interest to protect his business with the employees' right to privacy is to have a "well-drafted and well-communicated policy, which clearly identifies acceptable workplace practices and use of company equipment as well as personal equipment, both at work and off-work"[12].

What has changed with the advent of technology?

"Technology has helped to shape our experience of the world and has played its own role in shaping consciousness and understandings of human rights"[13]. It is impressive that, according to Richard Wurman, "a person receives and accesses more information today than a Seventeenth Century individual received in his or her entire lifetime"[14].

At the same time, the introduction of computers in the workplace was a remarkable scientific milestone. Yet surveillance in the workplace has been changing and what was before considered as an intrusive interference is today more easily accepted. Indeed, "expectations of privacy in the workplace have displayed a remarkable tendency to change at the same pace as technological developments occur"[15].

Monitoring of employees' conduct has always existed and was considered acceptable if some conditions were fulfilled. Before the advent of technology, surveillance had to be done by human means and that way the employees could see when they were supervised and adapt their conduct accordingly. Today, however, many new, more effective IT means have been created to monitor employees more discretely and efficiently, sometimes even continuously. This can lead to increasingly intrusive practices to the employees' privacy.

---

[11] Oliver (2002), p.326.
[12] Benaroche (2013), p.54.
[13] Joyce (2015), p.514.
[14] Richard Wurman cited in Smith-Butler (2009), p.56.
[15] Svantesson (2012), p.180.

It is very difficult for an employee to notice that his electronic communications are under surveillance. As Oliver relevantly points out, even firewalls can be a way for an employer to know whether the employee has been trying to search for prohibited content on the internet, in case a website is blocked.[16] Nowadays, with so many different technological developments, monitoring technology is very easy and relatively inexpensive to put in place. This technology may include analysing emails or online behaviour or even recording keyboard strokes[17].

Today, employees are even asked to participate actively in their own surveillance. In some corporations, employers are requiring employees to use productivity applications in their mobile phones and enrol in wellness programmes that supposedly are beneficial for them[18]. Frequently employees do not even have the conscience that they are collaborating in their own monitorization. The workplace wellness programmes, for instance, are not a bad project *per se*. They intend to aid workers in living a healthier life, control their weight and bad eating or smoking habits. Nevertheless, employees should be conscious that the information they provide in those applications will be known to the employer and might sometimes potentiate employment discrimination[19]. Productivity applications can also be a very beneficial technique, since it increases motivation and healthy competition between co-workers. Still, they can lead to dangerous, limitless surveillance, for instance when the applications are working 24 hours a day, every single day.

The particular case of social media – monitoring outside workplace's walls?

If computers have changed our life, internet revolutionized it. We now can have an extraordinary amount of information available in microseconds, from all corners of the world. The time and space dimensions of information sharing have dramatically changed. This phenomenon was further promoted by the emergence in the last decade of many social network sites (hereinafter, SNS) on the internet. People start getting digitally connected and the consequences

[16] Oliver (2002), p.328.
[17] Bond and Protokova (2015), p.3.
[18] Ajunwa, Crawford and Schultz (2017), p.739.
[19] Ajunwa, Crawford and Schultz (2017), p.763.

for social relationships have been quite diverse. SNSs can fulfil basic human needs like self-expression, communication and being part of a community[20].

Within the boundaries of the present paper, we will address how the use of social media has been dealt with in the workplace. For example, when hiring a person, what type of online information of the candidates is acceptable for an employer to consider?

One of the main problems with social media is that the delimitation between private and public is blurred. Employees might say things on Facebook that they would not say in the workplace, without considering that that information might be known in the future to their employer or co-workers.

A feature of SNSs is that the online information shared by employees is not necessarily related to their work. Therefore, it is a way for the employer to monitor them outside their workplace and beyond working hours. As a general rule, employers do not have anything to do with what employees do in their own free time. Hence, monitoring of SNSs is especially intrusive and usually considered excessive. Since the collection of personal data must be in some way related to the employment relationship[21], there is no legitimate excuse for such interference. In other words, the legitimacy of the employer's claim to monitor employees in their spare time is much weaker than at work[22].

Moreover, one could argue that it is the SNSs users that voluntarily expose their information to the public, and therefore they should be aware of the possible consequences. But this might not always be true. Third parties, such as Facebook friends, might also be able to share personal information and pictures about a user, sometimes without his or her consent or knowledge[23]. Furthermore, posting content on SNSs is not synonym of allowing free processing of that information.

One interesting issue is the question of background checks of possible candidates. It seems only logical that employers want to verify what type of person they are about to hire for their company. Nowadays it is easy and inexpensive to research for online information on people's lives, habits, likes

---

[20] Lukacs (2017), p. 187.

[21] Lukacs (2017), p. 201.

[22] Svantesson (2012), p. 187.

[23] This is questionable since it is possible to identify people on Facebook and they can afterwards decide if they want to be associated with the information or not by *deidentifying* themselves. About this argument, *see* Clark, and Roberts, Employer's Use of Social Networking Sites. A Socially Irresponsible Practice, 95 *Journal of Business Ethics* 4 (2010), p. 516

and dislikes. It is true that they can help making a wise hiring decision. These background checks tend to be more intrusive due to their invisible nature[24].

But should these background checks count as relevant information when a candidate is being selected for a job? Should this online information not be something from their private sphere that is none of the employer's business? Is it acceptable if the employer seeks the candidate's consent for this background research? The answer to these normative questions is not straightforward: it all depends on the legitimacy of the employer's interest in the background research. According to Bond and Protokova, if the employer can prove it, then the consent is not needed, as long as the research does not interfere with the privacy expectations of the individual[25]. Nonetheless, if the employer is dealing with sensitive information, explicit consent is required.

An original and creative rule that employees can use to decide if they should post something or not is the so-called 'grandmother rule', named by Byrnside[26]. According to it, users should only post information that they would not mind showing to their grandmothers. Moreover, it is advisable that employees avoid the overlap between their private and professional lives by not adding co-workers or employers to their SNSs.[27]

Video surveillance – different device, same problems?

Electronic surveillance includes computer, telephone tapping, video and mobile phone.[28] It can be targeted at a certain person or randomly at all employees in the company, continuously or sporadically.

Video surveillance is a commonly used way of enhancing physical security of the company's premises by detecting unauthorized access.[29] It consists in a network of cameras to monitor a particular area. It is an attractive mechanism because it allows people to supervise one location without being there. Yet, the improvements in the quality of video surveillance technology represent an invasive interference into people's privacy. An interesting project was developed to have a privacy-preserving face recognition system, where authenticated employees would be automatically recognized and their identity would be kept

[24] Lukacs (2017), p.197.
[25] Bond and Protokova (2015) p.3.
[26] Byrnside (2008), p.474.
[27] Svantesson (2012), p.185.
[28] Mahmood and Jensen (2015), p.4.
[29] Carniani (2016), p.20.

private.[30] Only in cases of policy violation would the video be recorded. This project shows how IT companies are aware of this increasing problem and are trying to create innovative solutions to avoid violating the employees' privacy.

As explained in the ECtHR case-law, video surveillance is considered as problematic as any other type of electronic monitoring. In fact, the Court applies similar principles to both types of surveillance, as it will be demonstrated below. Therefore, the recommendations that can be made to have acceptable video surveillance are the same ones applicable to email monitoring.

European and International law applicable to Protection of Employees' Privacy

European and international law have several hard and soft law instruments on protection of personal data. This area of law is being further regulated to include specific situations that arise due to technological developments such as the internet use in the workplace.

In 1990, the United Nations General Assembly established the Guidelines for the regulation of computerized personal data files[31], setting out the minimal protection that should exist in national legislation. In 2013, the General Assembly adopted a new Resolution regarding the right to privacy in the digital age[32], asking the States to make sure their surveillance procedures are in accordance with international human rights standards.

Additionally, the International Labour Office issued a Code of Practice on the Protection of Workers' Personal Data in 1997 with provisions specifically regarding monitoring of workers, as well as their individual rights in relation to the processing of their data.

The Council of Europe has protected personal data since it established the 1981 "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data". This document is very relevant because it is the first hard law instrument setting the international standards for protection of personal data both in the private and public sector.

The Council of Europe Committee of Ministers went a step further when it approved the 1989 "Recommendation on the protection of personal

[30] CARNIANI (2016), p.33.

[31] GA Resolution 45/95 (A/RES/45/95) of 14 December 1990.

[32] GA Resolution 68/167 (A/RES/68/167) of 18 December 2013.

data used for employment purposes"[33], which was recently replaced by the 2015 "Recommendation on the processing of personal data in the context of employment"[34]. The latter document sets out important principles related to transparency of processing, namely by stating the conditions that employers must fulfil to inform the employees when they interfere with their personal data. Furthermore, it regulates the use of internet and electronic communications in the workplace, giving much weight to the necessity principle.

In the European Union, the right to private life and protection of personal data are both set out, respectively, in Articles 7 and 8 of the Charter of Fundamental Rights. The right to data protection is also set out in Article 16 of the Treaty on the Functioning of the European Union. The Directive of the European Parliament and of the Council of the European Union on the protection of individuals with regard to the processing of personal data and on the free movement of such data[35], which was recently repealed, only mentioned employment relationships in its Article 8 regarding the protection of the employees' sensitive data. Otto argues that the categories referred as sensitive data are termed in a surprisingly broad manner for such a special regime of protection[36].

Nonetheless, this Directive is quite relevant in this context, since under its Article 29, a Working Party on Data Protection has been created. It is an independent advisory body of the European Union and has the power to issue opinions on national measures adopted under this Directive[37] and advise the Commission on measures to safeguard the rights and freedoms of natural persons regarding the processing of personal data[38]. In its 2001 Opinion on the processing of personal data in an employment context[39], the Working Party developed the main principles of data protection: finality, transparency, legitimacy, proportionality, accuracy, security and staff awareness[40]. Scholars have criticised these notions for their vagueness and ambiguity[41].

---

[33] Recommendation Rec(89)2 of the Committee of Ministers, adopted on 18 January 1989.
[34] CM/Rec(2015)5, adopted on 1 April 2015.
[35] Directive 95/46/EC, adopted on 24 October 1995.
[36] Otto (2015), p.357.
[37] Article 30(a) of the Directive mentioned above.
[38] Article 30(c) of the Directive mentioned above.
[39] Article 29 Working Party Opinion 8/2001, 5062/01/EN/Final.
[40] ECtHR, *Barbulescu*, §46.
[41] Otto (2015), p.355.

In 2002, the Working Party on Article 29 issued a specific document on surveillance and monitoring of electronic communications in the workplace[42]. This document delimitates the employer's legitimate monitoring of electronic communications through several principles: transparency, necessity, fairness and proportionality. It specifically addresses the situation where the employer accesses his employee's email account, by stating that "it would only be in exceptional circumstances that the monitoring of a worker's email or Internet use would be considered necessary"[43], such as to prove criminal activity, protect the security of the employer's electronic system or when the employee is out of office and his correspondence must be checked.

The above-mentioned Directive was repealed on May 25th 2018, when a new Regulation[44] entered into force. The GDPR establishes on Article 6 limited legal grounds on which the processing of personal data must be based. Purpose limitation and data minimisation are two core interrelated principles of the GDPR stated on Article 5 and applied throughout it. Due to the innate imbalance of power in an employment relationship, the legislator decided to expand on the definition of consent. Under the GDPR, it will be more difficult for an employer to rely on consent as a ground for processing personal data, since it must be "unambiguous", "by a statement or clear affirmative action", "freely given", "specific" and "informed". It will be a hard task for an employer to prove that these requirements have been fulfilled.

Furthermore, a privacy impact assessment must be performed in certain high-risk situations to evaluate if it is indeed necessary to interfere with one's privacy[45]. In summary, under the GDPR, employees as data subjects have the following rights: the right to be informed, which encompasses the obligation on employers to provide transparency as to how personal data will be used; the right of access; the right to rectification of data that is inaccurate or incomplete; the right to be forgotten under certain circumstances; the right to block or suppress processing of personal data; and the new right to data portability

---

[42] Working Document on the surveillance and the monitoring of electronic communications in the workplace adopted on 29 May 2002, 5401/01/EN/Final.

[43] Working Document, *ibid* p.14.

[44] 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 ("GDPR"). *See* OTTO (2015), p.362 for the list of main innovations of this Regulation.

[45] Article 35 of the GDPR.

which allows employees to obtain and reuse their personal data for their own purposes across different services under certain circumstances.

For the purposes of this paper, Article 88 is the most relevant provision of the GDPR, since it sets out the processing in the context of employment in new terms and it acknowledges *per se* the right to protection of the employee's data regardless of its sensitive nature. Although the GDPR can be considered a milestone for the consolidation of the data protection regime in Europe[46], its Article 88 gives Member States the discretion to establish additional specific rules on the topic. In our view, this might lead to different levels of protection within the European Union and undermine the GDPR's avowed purpose to have coherence in applying data protection principles[47]. It must also be taken into careful consideration by employers with activities in several European countries.

In fact, the current situation at the national level is quite diverse, as proven by the ECtHR in the *Barbulescu* case.

Analysis of recent ECtHR case-law

Barbulescu v. Romania

In this case, the applicant claims his right to respect for private life and correspondence had been breached, relying on the Article 8 of the European Convention on Human Rights (hereinafter, the Convention).

Mr. Barbulescu was an engineer who worked in a private company in Romania. At the request of his employer, the applicant created a Yahoo messenger account to answer clients' enquiries[48] and defined his own password for it. He already had a personal account. The regulations of the company prohibited the use of company's resources for personal use. The employer recorded his communications and realized that he had been using the company's computer for personal purposes. The applicant denied but was presented with the transcript of his communications with his fiancé and brother about intimate issues, such as his health and sexual problems.[49] These transcripts were made

[46] Otto (2015), p.362.

[47] *See* the list of EU Member States that notified the European Commission about the regulation of at national level in: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu/eu-countries-gdpr-specific-notifications_en [March 2019].

[48] ECtHR, *Barbulescu*, §1.

[49] *Ibid*, §21.

available to the applicant's colleagues. Furthermore, the employer also accessed the applicant's personal messenger account, which had a different ID.

The applicant was dismissed for violation of the company's internal regulations. He challenged the employer's decision before the Bucharest County Court, which confirmed the dismissal. The applicant appealed to the Bucharest Court of Appeal, which upheld the first instance judgement.

He then lodged a complaint before the ECtHR. The Fourth Section found in favour of the Government, because the domestic courts did not fail to strike a fair balance between the applicant's right to respect for private life and the employer's interests. The case was then referred to the Grand Chamber which overruled the Chamber judgment.

Firstly, the Grand Chamber considers whether the case concerned a positive or a negative obligation of the State. In this case, the applicant's enjoyment of his Article 8 right was impaired by action of a private employer[50]. By confirming the employer's decision, the domestic courts failed to protect the applicant's right. Therefore, the complaint had to be viewed from the perspective of the domestic courts' omission to comply with the positive obligation to protect Mr. Barbulescu's right to private life.

The Grand Chamber gives special attention to the fact that domestic courts failed to determine whether the applicant had received prior notification of the monitorization of his communications, its extent, nature and degree of intrusion.[51] The Court considers that the warning should have been given before the monitorization started.[52] In the Grand Chamber opinion, there were no justifiable and legitimate aims for the interference with the applicant's right to privacy, and the domestic courts did not assess if any less intrusive measures could have been used and whether the interference could have been done without the employee's knowledge. In consequence, the ECtHR finds that the Romanian authorities did not adequately protect the applicant's right to privacy and therefore that there had been a violation of Article 8.

The Chamber judgment raised enormous controversy among civil society, since it did not pay attention to several important factors of the case and the findings seemed bluntly unfair. Even the New York Times referred that this ruling "had stirred unease in Europe, where privacy is viewed as a fundamental

---

[50] *Ibid* §111.

[51] *Ibid* §133 and 134.

[52] *Ibid* §133.

right"[53]. This shows that not only the issue of privacy protection in the workplace is of worldwide importance, but also that the Strasbourg case-law is taken into consideration in the four corners of the world.

In fact, the Chamber judges were strongly influenced by their American peers. As concluded in the landmark case *O'Connor v. Ortega*[54], the reasonability of the employee's expectation to privacy is context-dependent[55], taking into consideration the operational realities of the workplace[56]. Hence, the American approach to the protection of employee's privacy is very casuistic. The americanization of the Strasbourg case-law would lead to a weak protection of employee's privacy since there would be no clear principles on which interests of the employer would legitimize interference with the employee's privacy and the extent of this interference.

The Chamber neglected the sensitive nature of the communications intercepted by the employer, which dealt with the applicant's health and sex life. These are afforded the most intense protection under Article 8. Moreover, the employer did not only access the applicant's professional account, but also his personal one. In our view, this is very difficult to justify. Specially because the account was called Andra loves you, which obviously did not have connection with Mr. Barbulescu's professional activities. Additionally, the interference was far from necessary since the transcripts became the talk of his colleagues due to their disclosure by the employer.

As the Grand Chamber rightly stated, an employer's instructions cannot reduce private social life in the workplace to zero. Respect for private life and for privacy of correspondence continues to exist, even if these may be restricted in so far as necessary[57]. It would be unrealistic to entirely ban the access for the internet for personal use in the workplace because most of the employees' time is indeed spent in their workplace. In the information era, the lines between work and private life have been blurred.

In our assessment, the Grand Chamber's judgment is indeed remarkable for three reasons. First, it took a principled approach to the protection of privacy in the workplace, by stating the main rules that should govern it[58]. Secondly,

---

[53] SEWELL CHAN, European Court Limits Employers' Right to Monitor Workers' Email, *New York Times*, 5 September 2017.

[54] Supreme Court, O'Connor v. Ortega, 480 US 709 (1983).

[55] SMITH-BUTLER (2009), p.61.

[56] VANTO (2010), p.1.

[57] ECtHR, *Barbulescu v. Romania* (no.61496/08), 5 September 2017 (GC), § 80.

[58] These rules are set out in §§ 121 and 122 of the Grand Chamber *Barbulescu* judgment.

while stating these principles it took into consideration the international and Council of Europe soft law[59]. Thirdly, the Court took a very proactive position, insofar as it imposed a European standard although it explicitly recognised that there was no European consensus on these issues[60]. By so doing, the Court contradicted its usual methodology of waiting for a consensus to exist in Europe to then proceed to establish European-wide principles.

Libert v. France[61]

This judgment is a very recent follow-up to *Barbulescu*, addressing the case of a public employer opening files from the hard disk of the employee's professional computer. The applicant was an employee from the French national railway company (hereinafter, SNCF). He was suspended from his functions due to a complaint filed internally against him by a colleague. During that time, his professional computer was seized and the employer analysed the content of its hard disk, where he found vast pornographic material, together with forged certificates created for third persons[62]. The applicant was subsequently dismissed. In the domestic proceedings he complained that his right to respect for private life had been violated, since the opened documents, entitled 'giggles', were clearly of a personal nature. After the domestic courts rejected the complaint, the ECtHR confirmed that rejection, concluding that there had been no violation of Article 8.

Most importantly, the ECtHR stated that the interference had a lawful basis and a legitimate aim, in the light of the employer's right to ensure that his employees were observing their contractual obligations[63]. Furthermore, the domestic law in this case allowed the employer to open files in the professional computer of the employee if they were not clearly specified as private. Moreover, the interference was proportionate and French authorities had not exceeded their margin of appreciation. The three requirements of Article 8 (lawfulness, legitimate aim and proportionality of the interference) were fulfilled.

In our view, *Libert* extends the Court's case-law on surveillance in the workplace, but it differs from the previous case *Barbulescu* in two main aspects.

---

[59] ECtHR, *Barbulescu* (GC), §§ 42-3.
[60] *Ibid*, § 118.
[61] ECtHR, *Libert v. France* (no. 588/13), 22 February 2018.
[62] Press Unit of the ECtHR, Fact Sheet on Surveillance at Workplace, February 2018, p. 3.
[63] ECtHR, *Libert*, § 46.

Firstly, the employer at stake, SNCF, was a State-run enterprise and therefore there was no need to address the positive obligations of the State. Secondly, in this case the Court considered that there were enough measures to adequately protect the employee's privacy at the workplace. An important point to highlight is that the Court clarified that the employer cannot surreptitiously open files stored in the professional computer if they are clearly identified as 'personal', except in case of 'particular risks or events'[64].

Nevertheless, we do not agree with the Court's argument that Mr. Libert's files entitled 'giggles' are of professional nature, allowing the employer to open them without his consent. The argument that the domestic courts made, and that the ECtHR accepted, that these files could include communications between colleagues or work documents considered funny by the employee[65] does not seem very compelling.

Antovic and Mirkovic v. Montenegro

This case expands the Court's case-law regarding the specific issue of video surveillance. It concerned a complaint filed by two professors of the Mathematics School of Montenegro arguing that their right to respect for private life had been violated by the unlawful installation of video surveillance technology in the auditoriums without their prior knowledge and consent. The domestic courts rejected their complaint based on the public nature of the surveilled area, which excluded any interference with the applicants' private lives.

In order to dismiss the domestic court's argument, the ECtHR firstly stated that 'the notion of 'private life' may include professional activities or activities taking place in a public context'[66]. Furthermore, it also stated that 'covert video surveillance of an employee at his or her workplace must be considered, as such, as a considerable intrusion into the employee's private life'[67]. The Court appeared to rely on the fact that there seemed to be a lack of a legitimate aim for the employer's interference. The employer argued that it was a security measure, but there was no evidence of any danger for either people or property.

---

[64] *Ibid*, § 48.
[65] *Ibid*, § 51.
[66] ECtHR, *Antovic and Mirkovic v. Montenegro* (no. 70838/13), 28 November 2017, § 42.
[67] *Ibid*, § 44.

The only reason for surveillance seemed to be the will to monitor teaching, which was no ground for surveillance according to domestic regulations[68].

Concluding, the ECtHR found a violation of Article 8, since the interference in question lacked a lawful basis.

In our view, this case is of paramount importance since it is the first case about video surveillance of employees since *Barbulescu*. Nevertheless, like the dissenter, we believe it is worth mentioning that the Court did not take into account that the surveillance was remote, that there was no audio recording and thus no recording of the teaching or discussions, that the pictures were blurred and the persons could not easily be recognised, that the video recordings were only accessible to the dean and were automatically deleted after 30 days[69]. These factors should have weighted in the proportionality test.

López Ribalda and Others v. Spain[70]

This case is a follow-up to *Antovic and Mirkovic* and addresses a covert video surveillance made by the owner of a supermarket due to his suspicion that some of his employees were stealing. The employer warned them that he would install cameras directed to the exits of the store to monitor customers, but hided some other cameras pointing to the checkout counters. Having confirmed his suspicions, the employer dismissed several employees that had been stealing from the store. They brought proceedings for unfair dismissal based on a video obtained by means of violation of their right to privacy. The Spanish courts rejected their complaint.

The ECtHR established there had been a violation of Article 8, highlighting the existence of domestic legislation that specifically obliged the employer to inform his employees that they are under surveillance, which did not happen. This contrasted with an older case on video surveillance, *Köpke v. Germany*, which had very similar facts, but where the conditions to carry out video surveillance had not been established in domestic law[71]. This was the most contrasting fact that made the Court decide differently in *López Ribalda*. The different criteria applied in both cases derive from the Court's consideration that the employees'

---

[68] *Ibid* § 59.

[69] Dissenting Opinion in *Antovic and Mirkovic*, *supra* note 62, § 10.

[70] ECtHR, *López Ribalda and Others v. Spain* (nos. 1874/13 and 8567/13), 9 January 2018. The case is now pending before the Grand Chamber.

[71] *Ibid* § 67.

expectation of privacy would be more intense in *López Ribalda* than in *Köpke*, as there was no legal requirement in the latter for employers to report to employees that they were recorded by video surveillance[72]. Furthermore, in the Spanish case, the employer's suspicion was not directed specifically at the applicants but at all employees and the surveillance had no time limit.[73] The Court departed from the previous and almost identical case and considered the measure was not proportional and therefore found a violation of Article 8.

To our mind, this judgment is not realistic. we argue that this judgement did not consider why the employer decided to monitor his employees. He had a strong suspicion that someone from inside the supermarket was stealing. Had he informed his employees that they would be under surveillance, as the Court suggests, his purpose would be defeated, since they would obviously stop stealing. It seems a little unbalanced to have such a categorical judgement in this case.

Conclusion from the case-law

From all the above-mentioned recent case-law, one can conclude that the ECtHR is narrowing down the employer's right to monitor, establishing strict conditions for the interference with the employees' right to privacy to be legitimate. These conditions are twofold. On the one hand, employers must inform the affected employees in advance. On the other hand, a proportionality test must be carefully performed to evaluate if the interference with the employee's right to privacy is justifiable.

Some comments on adequate monitoring

The right to privacy is a fundamental human right that should be limited only in restricted conditions. It cannot be agreed in an employment contract that the right of privacy will be absolutely waived. One important issue is the requirement of free and informed consent to monitoring that employees are asked to give. This requirement of consent is put at stake whenever employees feel pressured to accept what the employers are demanding, in order to get or keep the job. In these circumstances, their consent is not necessarily a

---

[72] Alexis Kateifides, International: ECtHR workplace surveillance decision 'tips the scales' in favour of employees, *Privacy This Week*, 18 January 2018.

[73] ECtHR, *López Ribalda*, *supra* note 66, § 68.

synonym that they are comfortable with the monitoring, it might just mean they do not feel they have any other option. Due to the great power imbalance typical of employment contracts[74], requiring truly free and informed consent to monitoring is a crucial guarantee.

The reasonable expectation of privacy is the current standard in the case-law that we have analysed. There are various elements which are relevant for the assessment of this standard, such as lack of previous warning of the interception or assurance that the device used is private or might be used for private purposes[75]. The expectation will not only depend on the nature of the communication, but also on the type of role the employee performs within the company.

Most importantly, employees must be previously informed that their data will be collected, why and when that will happen and who will access the data. Covert surveillance, as previously showed, is very problematic and hardly acceptable. The collection and processing of the employee's information must have a lawful basis and be done for legitimate and specified purposes. The right to privacy must be limited only to the absolutely necessary extent, meaning that they must be limited in time, as less intrusive as possible. Additionally, they must be submitted to a rigorous proportionality test, which implies a balancing of the contradictory interests at stake. The employer should consider reducing monitoring to situations where complaints have been made, carrying out on a departmental rather than individual basis, automating monitoring, (...) monitoring email headings or traffic rather than email content[76]. Content access is submitted to a stricter proportionality test. Not only must the employer have a legitimate reason to monitor the communications, he must also have specific legitimate reasons for accessing their content[77].

In addition to a domestic legal framework, it is essential to have a clear and detailed policy in the company about the use of email, internet and telephone, which must be consistently applied. Employees must be aware of changes in those policies. An example of a good practice is the implementation of a system whereby employees are asked if they agree with the company's policy every time they log into the company's computer[78]. Furthermore, it is

---

[74] SVANTESSON (2012), p. 181.

[75] OLIVER (2002), p. 336.

[76] SAKROUGE (2011), p. 215.

[77] Emily Fedeles and Nichole Sterling, European Court Provides Further Clarity on Employee Monitoring, *Data Privacy Monitor*, 20 September 2017.

[78] SVANTESSON (2012), p. 186.

advisable to conduct a privacy impact assessment before monitoring to ensure the justifiability of the interference, to be aware of possible adverse effects and consider alternatives. Creating technological and administrative safeguards to reduce the possibility of misuse of the system, together with training and education for system operators to protect individuals' privacy[79] are further recommendations to minimize privacy intrusions.

Conclusion

Data protection related concerns are increasingly coming under the spotlight. In relation to the workplace, rules have been changing and employers should pay attention to new developments both in the domestic legislation and in the international arena. New legal questions are appearing due to technological innovations and they need further study.

One important conclusion of our research is that there was no consensus in the domestic legislation of European States. This is precisely what the research done by the ECtHR in its Grand Chamber *Barbulescu* case states[80]. Nonetheless, the ECtHR in its recent case-law has established European-wide standards, contradicting its usual process of waiting for a consensus to exist in Europe to then proceed to establish principles. This reveals the extreme importance of this topic and the urgency in defining general principles for it. The European Union has also been attentive to the protection of employees' privacy and data protection in general.

It is time for the Member States to act in accordance with their international law obligations. Employees must have the same guarantees of privacy throughout Europe.

References

AJUNWA, Ifeoma, Kate Crawford and Jason Schultz, "Limitless Worker Surveillance", *California Law Review*, vol. 105, 2017, pp. 735-776; BENAROCHE, Patrick, "Loyalty, Privacy and Free Expression in the Digital Workplace", *Employment and Industrial Relations Law*, vol. 23, number 2, 2013, pp. 51-54; BOND AND PROTOKOVA, "Monitoring in the workplace – damned if you do and damned if you don't!", COMPLIANCE *and Risk*, vol. 4, number 3, 2015, pp. 2-5; BYRNSIDE, Ian, "Six Clicks of Separation: The Legal Ramifications of Employers Using Social Networking Sites to Research Applicants", *Vanderbilt Journal of*

[79] MAHMOOD AND JENSEN (2015), p. 19.

[80] ECtHR, *Barbulescu* (GC), § 118.

Entertainment and Technology Law, vol. 10, number 2, 2008, pp. 445-477; CARNIANI, Enrico *et al.*, "Enhancing Video Surveillance with Usage Control and Privacy-Preserving Solutions", *J. of Wireless Mob. Netw., Ub. Comp., and Dep. App.*, vol. 7, number 4, 2016, pp. 20-40; CHAN, Sewell, "European Court Limits Employers' Right to Monitor Workers' Email", *New York Times*, 5 September 2017; FEDELES, Emily and Nichole Sterling, "European Court Provides Further Clarity on Employee Monitoring", *Data Privacy Monitor*, 20 September 2017; JOYCE, Daniel, "Internet Freedom and Human Rights", *EJIL*, vol. 26, 2015, pp. 493-514; KATEIFIDES, Alexis, "International: ECtHR workplace surveillance decision 'tips the scales' in favour of employees", *Privacy This Week*, 18 January 2018; LUKACS, Adrien, "To post or not to post – That is the Question: Employee Monitoring and Employees' right to Data Protection", *Mas. Uni. J. Law Techno.*, vol. 11, number 2, 2017, pp. 185-209; MAHMOOD, Qasim and Christian Jensen, "Video Surveillance: Privacy Issues and Legal Compliance" in *Promoting Social Change and Democracy through Information Technology*, Eds. Kumar & Svensson, DTU Library, Denmark, 2015; MORGAN, Charles, "Employer Monitoring Of Employee Electronic Mail And Internet Use", *McGill Law Journal*, vol. 44, 1999, pp. 849-902; OLIVER, Hazel, "Email and internet monitoring in the workplace: information privacy and contracting-out", *Industrial Law Journal*, vol. 31, number 4, 2002, pp. 321-352; OTTO, Marta, "The Right to Privacy in Employment – In search for the European Model of Protection", *European Labour Law Journal*, vol. 6, number 4, 2015, pp. 343-363; POLICY, Sindy, "The Employer as Monitor: Keeping an Eye on Net Use and E-mails Can Prevent Litigation", *Bus. L. Today*, Nov./Dec. 2000, p. 11; SAKROUGE, Anthony *et al.*, "Monitoring employee communications: data protection and privacy issues", *Computer and Telecommunications Law Review*, vol. 17, number 8, 2011, pp. 213-216; SMITH-BUTLER, Lisa, "Workplace Privacy: We'll Be Watching You", *Ohio N.U.L. Rev.*, vol. 35, 2009, pp. 53-81; SVANTESSON, Dan, "Online workplace surveillance – the view from down under", *International Data Privacy Law*, vol. 2, number 3, 2012, pp. 179-191; THE HARVARD LAW REVIEW ASSOCIATION, "Addressing the New Hazards of the High Technology Workplace", *Harvard Law Review*, vol. 104, number 8, 1991, pp. 1898-1916; UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN, "Brief diversions vastly improve focus, researchers find.", *ScienceDaily*, 8 February 2011; VANTO, Jarno, Maria Teixeira and Mami Hino, "Employee Expectation of Privacy with Respect to Use of Employer-Owned Workplace Computers and Other Electronic Devices and Files Stored on Such Devices – Global Cases", *International Human Rights Journal*, vol. 19, number 4, 2010, art. 2; WESTIN, Alan, "Privacy in the Workplace: How well does American Law Reflect American Values?", *Chicago-Kent Law Review*, vol. 72, number 1, 1996, pp. 271-283.