UiO : Faculty of Law
University of Oslo

Redefining Employee Privacy

Defining the Boundaries of Employee Monitoring in the Light of the European Court of Human Rights Judgment in the Case of Bărbulescu v. Romania

Candidate number: 8019

Submission deadline: 01.12.2017

Number of words: 16 881

Table of contents

Acknowledgements

I would like to express my gratitude to my mother, who made this amazing quest for knowledge and personal growth to Norway and the University of Oslo possible; to Roey Barnir for the inspiration, help, and guidance every step of the way; and to Ezra Weygant for supporting me in the toughest times. I also want to thank my supervisor Maryke Silalahi Nuth for the understanding and patience, through all those months.

1 Introduction

1.1 Background and Context

The continual digitalization and emergence of new information and communications technologies have an impact on every aspect of modern society including the way people carry out their jobs. Individuals have opportunities to work from home or use their own devices at the office blurring the line between work and personal space more than ever before.

The question about protecting the employee's right to privacy is not a new one. In 1997, the European Court of Human Rights (ECtHR, the Court, Strasbourg) in *Halford v. the United Kingdom*[1] defined that phone calls made on office premises are covered by the notions of "*private life*" and "*correspondence*" under Article 8 of the European Charter of Human Rights.[2] In 2001and 2002 the Article 29 Working Party issued opinions on "*processing of personal data in the employment context*."[3]

However, the perspective has changed in the past few years since employers now have easy and cheap access to automation, allowing them to supervise their employees in innovative ways including systematic and potentially intrusive monitoring[4]. Companies such as Bloomberg Finance L.P. [5] provide state of the art surveillance products infiltrating various sources of e-communications including corporate mail, instant messaging, voice recordings and even files and documents. In the finance sector, regulators expect companies to implement systems and controls based on the retention, review, and supervision of communications[6]. A growing number of surveillance products rely on machine learning and "*metadata profiling with predictive coding*"[7] to ensure efficiency. A recent German Federal Labour court case addressed the legality of installing keyboard-tracking software on employee computers[8]. Newly emerging practices like microchips implanting[9] broaden the scope of the discussion of employee privacy

---

[1] Judgment on the merits and just satisfaction, delivered by a Chamber, *Halford v. The United Kingdom*, no. 20605/92, ECHR, 1997

[2] ECtHR, Factsheet – Surveillance at workplace

[3] See Article 29 Working Party, Opinion 8/2001 on the processing of personal data in the employment context & Article 29 Working Party, working document on the surveillance of electronic communications in the work-place (Adopted May 2002)

[4] Article 29 Working Party, Opinion 2/2017 on data processing at work, p. 3

[5] Bloomberg Finance L.P., A Bloomberg Professional Services Offering, retrieved from https://data.bloomber-glp.com/professional/sites/10/Surveillance-Fact-Sheet-1.pdf

[6] Erns & Young, Considerations for your e-communications surveillance program, p.2

[7] Ibid. p. 3

[8] The Local (27 July 2017), *German court rules bosses can't use keyboard-tracking software to spy on workers, Retrieved from https://www.thelocal.de*

[9] Associated Press (2017), *Would YOU let your employer implant an ID chip in your arm?*, retrieved from http://www.dailymail.co.uk

even further.

In the light of these developments, it is critical to set a balance between the employer's *legitimate interests* to ensure efficiency, productivity, and security at the workplace and the employees' right to privacy. The debate recently resurfaced as a result of the following judicial and regulatory outcomes:

On September 5th, 2017 the ECtHR issued a ruling labeled as a *landmark* by both legal scholars and privacy professionals[10]. In *Bărbulescu v. Romania*[11] the Grand Chamber of the ECtHR found that the Romanian judicial system failed to protect Mr. Bărbulescu's right of a private life by not acheving a "fair balance" between a private company's right to monitor its employees' electronic communications and the right to respect of private life and correspondence stipulated in Article 8 of the European Charter of Human Rights.

This decision was preceded by the Article 29 Working Party's Opinion 2/2017 on data processing at work, reassessing the "*the balance between legitimate interests of employers and the reasonable privacy expectations of employees by outlining the risks posed by new technologies.*"[12]

Moreover, the upcoming General Data Protection Regulation[13] (GDPR, the Regulation) – a legal instrument expected to reshape[14] the future of data protection not only in Europe but worldwide, adds several new implications to the question of employee privacy.

1.2 Problem Definition

The objective of this work is to analyse how the above judicial and regulatory developments shape and continue to shape the parameters of the right to private life in an employment context from the perspective of the limitations imposed on monitoring practices at the workplace.

This thesis will first establish how the nature of the right to private life at the workplace is derived from the overarching right to respect of private life and family set in Article 8 of the

---

[10] Deutsche Welle (2017), *European court sides with worker in landmark privacy ruling*, retrieved from http://www.dw.com and Wilhelm, E.-O., (2017), *Bărbulescu ruling: Workplace privacy is alive and kicking*, IAPP Privacy Tracker, retrieved from https://iapp.org

[11] Judgment on the merits and just satisfaction, delivered by the Grand Chamber, *Bărbulescu v. Romania*, no. 61496/08, ECHR, 2017

[12] Article 29 Working Party, Opinion 2/2017

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

[14] Zhang, E. (2017), How GDPR Will Reshape Your Data Protection Strategy, Digital Guardian, retrieved from https://digitalguardian.com

ECHR, and the contributions of the European data protection regime in shaping this right. The findings will be based on the review of the case law of the ECtHR on surveillance and monitoring at the workplace, the Data Protection Directive[15] (DPD, the Directive) and the GDPR. This thesis will explore the different elements of the employee's right to privacy through the lenses of the ECtHR's case law, the relevant data protection rules and the scholarly research on the application of the well-defined data protection principles of necessity, purpose limitation, transparency, legitimacy, and proportionality.

Further, this work will analyse how the criteria set by the European court of human rights in *Bărbulescu v. Romania* for balancing the interests in the employer-employee relationship, read in line with the data protection legislation, amount to a coherent framework ensuring workplace privacy through personal data protection.

The scope of the research includes legal instruments and case law relevant to privacy and data protection in Europe.

1.3 Clarification of Notions

1.3.1 The Right to Privacy and Data Protection

The notions of privacy and private life subject to this work are derived from the right to privacy, family, home or correspondence, stipulated in Article 17 ICCPR and the right to respect of private life and family in Article 8 ECHR.

There is an agreement in the human rights doctrine that the scope of the private life is not strictly defined.[16] It is seen as "one of the most open-ended[17]" rights, which until this day has not received a comprehensive definition by the human rights case law[18]. The reason for this interpretation is to allow Article 8 to remain adaptable to the ever-changing social, economic and technological developments[19].

In Communication No. 453/1991, *Coeriel and Aurik v. The Netherlands* The Human Rights Committee establishes that '*the notion of privacy refers to the sphere of a person's life in which he or she can freely express his or her identity, be it by entering into relationships with others or alone.*[20]' The case law of ECtHR extends the range of the right to respect of private life and

[15] 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

[16] Human Rights Education Project, What is private life?, retrieved from http://www.humanrights.is

[17] Roagna, I.(2012), *Protecting the right to respect for private and family life under the European Convention on Human Rights*, Council of Europe human rights handbooks, p. 9

[18] Ibid.

[19] Ibid.

[20] Human Rights Education Project, What is private life?, retrieved from http://www.humanrights.is

family to areas such as "*bearing a name, the protection of one's image or reputation, awareness of family origins, physical and moral integrity, sexual and social identity, sexual life and orientation, a healthy environment, self-determination and personal autonomy, protection from search and seizure and privacy of telephone conversations*"[21]. Personal data protection has never been explicitly added to the scope the right to a private life, although the court on numerous occasions in its cases on unauthorised surveillance, dealt with the issue of unlawful processing of personal data.

From the opposite perspective it seems evident that data protection laws are intended to ensure privacy[22]. The Data Protection Directive explicitly states that its objective is to "*protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data*."[23] However, there this position has changed and the GDPR establishes a right to data protection separate to the right to privacy (see recital 2 GDPR)[24]. Nonetheless, this thesis aims to defend that there is an overlap between the European court of human right's stand on workplace privacy and the Data Protection legislation, resulting in a coherent regime of safeguarding the employees' right to a private life through the protection of their personal data.

1.3.2 Data Privacy and Data Protection

The terms *data privacy* and *data protection* are practically synonyms[25], both referring to the regulation of the processing of personal data – information that allows the identification or relates to an identifiable natural person (individual)[26]

The use of *data privacy* is typical of the tradition in the United States. For example, section 501, of the Gramm-Leach-Bliley Act (GLB), regulating the protection of non-public personal information, falls under "Title V – Privacy".

The term data protestation is typical for the European nomenclature[27], the obvious example being the "General ***Data Protection*** *Regulation*."

The focus of this thesis will be on the privacy at the workplace aspect of the right to private life

---

[21] Roagna, p. 12

[22] See Bygrave, L. A. (2001). *The Place of Privacy in Data Protection Law*., (UNSW Press, Volume 2, No 1, 2001), 256 pp

[23] DPD, Article 1 (1)

[24] I believe that this issue call for further discussion and research form the data protection academics.

[25] See Bygrave, L. A. (2014). *Data privacy law: an international perspective*. Oxford: Oxford University Press, p.2

[26] Article 2 (a) Data Protection Directive

[27] Bygrave, L. A. (2014) p.2

and family under Article 8 of the ECHR, but also how the data protection principles and regulations contribute to shaping and protecting the above right.

1.3.3 Employee

The term *employees* used in this paper is not limited to only the individuals bound by a contract of employment in the strict sense of the labour laws, but also includes the types of employment based of *freelance agreements,* that nevertheless show the characterises of a regular work relationship.[28]

1.4 Methodology and Thesis Outline

This thesis defends that the right to a private life at the workplace is shaped by the case law of the ECtHR on employee surveillance and monitoring, the Data Protection and the GDPR and that the human rights and data protection regimes exist in symbiosis safeguarding workplace privacy through personal data protection.

This would be achieved through examination of ECtHR's case law that contributed to the accommodation of workplace privacy under the notions of private *life* and *home* within the meaning of Article 8 ECHR (Chapter Two).

Further, Chapter Three will review the employee monitoring as a form of processing of personal data and will explore how the data protection principles of lawful and fair processing, transparency, purpose limitation, necessity, proportionality and integrity help shape the right to employee privacy.

Finally, Chapter Four will analyse the similarities and correlations between the general principles applicable to the assessment of the State's positive obligation to ensure respect for private life and correspondence in an employment context laid out by the ECtHR in *Bărbulescu v. Romania* and the principle of data protection outlined above.

2 Employee Monitoring and the European Court of Human Rights

"Everyone has the right to respect for his private and family life, his home and his correspondence."- European Convention on Human Rights, Article 8 Right to respect for private and family life

"Workers do not abandon their right to privacy and data protection every morning at the

[28] Article 29 Working Party, *Opinion 2/2017*, p. 4

doors of the workplace."[29]*- The Article 29 Working Party*

The right to a private life at the workplace is a derivative of the right to private and family life, home and correspondence (Article 8 ECHR), established by ECtHR's case law on searches and surveillance at the workplace[30].

This chapter is dedicated to examining how the ECtHR contributed to creating an interface between work and private life, and attempts to answer how situations that occur at the workplace amount to *private life* and *home* within the meaning of Article 8 ECHR. This will be achieved through a critical discussion of the scope of the afforded protection and the criteria considered by the court when deciding whether the employee monitoring results in a violation of the right to a *private life*.

The chapter begins with an outline of the method used by the court when applying Article 8 ECHR, followed by a discussion of the ECtHR case-law on employee monitoring - from the moment that professional activities fell within the remits of Article 8 to the setting of the standards of reasonable expectation to privacy and a fair balance of rights.

2.1 Method of Applying Article 8 of the European Convention on Human Rights

Article 8 is structured in a manner that requires several stages of interpretation prior to establishing its applicability to the circumstances of the case and whether the conduct in question amounts to a violation. There are different views on the number of steps that the ECtHR undertakes in its assessments. There are different views on the number of steps that the ECtHR undertakes in its assessments. The ECtHR itself in its Guide on Article 8 of the European Convention on Human Rights – refrains from discussing the number of steps it undertakes.According to H. Tomas Gomez-Arostegui, it entails a three-step analysis including (i) whether the circumstances at stake fall under at least one of the notions of private life, family life, home or correspondence, (ii) whether there is an interference by the State or a failure to provide protection against the interference from others and (iii) whether there is a justification for the State's actions or lack of oversight[31].

---

[29] *Article 29 Working Party,* 2002 *Working Document on the surveillance of electronic communications in the workplace* (WP55), p. 4

[30] Roagna, p.20

[31] Gómez-Arostegui, H. Tomás (2005) "Defining Private Life Under the European Convention on Human Rights by Referring to Reasonable Expectations," California Western International Law Journal: Vol. 35 : No. 2 , Article 2., p.3

Contrariwise, Ivana Roagna and Ursula Kilkelly[32] define the court's assessment as a "two-stage test."[33] The first stage requires a positive answer to whether the facts of the case concern "private life" or "family life," "home" or "correspondence."[34] The second stage examines whether there is an interference by the State and, if so, whether it is in accordance with the law, pursuing a legitimate aim or is necessary for a democratic society[35]. If there is no interference, the court will proceed with identifying whether the State complied with its positive obligations to ensure the application of the rights granted by the Convention.

In my view, using the three-step test is more beneficial when analysing the ECtHR's case law. Identifying whether the case concerns a breach of the State's negative obligation to refrain from interference or a breach of the States positive obligations to adopt measures, ensuring the protection of the right to a private life is decisive in directing the discussion. The factors taken into consideration by the Court differ based on whether the case concerns a positive or a negative obligation.

It is self-evident that the first step entails an assessment whether the circumstances of the case concern private family life, home or correspondence. Strasbourg has refrained from giving a precise definition to either of the above notions, and their scope is decided on a case by case basis[36]. This approach has allowed the court to accommodate the remits of Article 8 to the constant development of moral values, law, and technology[37]. In the light of employee monitoring, this flexibility allowed the court to expand the reach of private life and correspondence from telephone conversations in *Halford v. The United Kingdom* to messages exchanged on an Internet messaging application in *Bărbulescu v. Romania.*

The second step of applying Article 8, as mentioned above, includes an evaluation of whether the State breached either its negative or positive obligations specified in the provision. The essential objective of Article 8 is of a negative kind – posing an obligation to the State to refrain from unjustified interference in the individuals' right to a private life[38]. However, the Court in *Marckx v. Belgium*[39] establishes that Article 8 also imposes positive obligations on the State –

---

[32] Kilkelly, U.(2003), *The right to respect for private and family life. A guide to the implementation of Article 8 of the European Convention on Human Rights*, Human rights handbooks, No. 1

[33] Roagna, p.10

[34] Ibid., p.11

[35] Ibid.

[36] Ibid., p. 10

[37] Ibid., p.10

[38] European Court of Human Rights, *Guide on Article 8 of the Convention – Right to respect for private and family life*, p.8

[39] Judgment on the merits and just satisfaction, delivered by a Chamber, *MARCKX v. BELGIUM*, no. 6833/74, ECHR, 1979

to ensure that by adopting specific measures, individuals can effectively exercise their rights in the relationships between themselves[40]. The Court justified the existence of such positive obligations through the use of the "respect" in the first paragraph of Article 8[41].

The last step establishes whether there is a breach of Article 8. This requires an assessment of whether the actions undertaken by the State (in case of negative obligations) or the State's lack of actions (in case of positive obligations) are justified. According to the ECtHR "*The principles applicable to assessing a State's positive and negative obligations under the Convention are similar*", requiring the balancing of competing interests[42]. If the case concerns the State's negative obligations, the interests opposed to the right to a private life are listed in Article 8, paragraph 2, namely "*national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others*" and the interference will be justified only if it is in accordance with the law and necessary in a democratic society[43].

In the case of positive obligations, the Court must establish whether the importance of the interests of the individual requires the State to adopt measures to ensure the respect for private life[44]. In cases conserving the conflicting interests of individuals or groups of individuals, it is sufficient for the Court to establish that the State has failed to balance the rights at stake.[45] For example in *Köpke v. Germany*[46] Strasbourg clearly states that State's positive obligation is to strike "*a fair balance between the applicant's right to respect for her private life and both her employer's interest in protection of its property rights, guaranteed by Article 1 of Protocol no. 1 to the Convention, and the public interest in the proper administration of justice*."[47]

In this work, when analysing the ECtHR cases regarding the state's negative obligations in respect to searches and surveillance at the workplace, the focus will fall on the first stage of the test – as it brings the most value to the discussion about the scope of the employee's right to privacy. When the subject of the case is the State's positive obligations to protect the right to a private life, both stages will be reviewed as the court gives essential guidance on how the balancing test should be conducted which has a significant impact on defining the scope of the

[40] ECtHR, Guide on Article, p.8

[41] Roagna, p. 60

[42] European Court of Human Rights, Guide on Article 8 of the Convention – Right to respect for private and family life, p.8

[43] ECHR, Article 8, paragraph 2

[44] ECtHR, Guide on Article 8, p.8

[45] Roagna, p.60

[46] Decision on admissibility delivered by a Chamber, *Köpke v. Germany*, no.420/07, ECHR, 2010

[47] Köpke v. Germany, §2

right to a private life at the workplace.

2.2 Professional Activities

ECtHR's Judgment on *Niemietz v Germany*[48] is the cornerstone of the concept that the right to respect of private life oversteps the boundaries of an "inner circle" to include the person's professional activities.[49] I have to agree with Marta Otto 's conclusion that this case sets "*The Foundations of Employee's Right of Private Life.*"[50]

The particular circumstances of the case concern the search of the law office of Gottfried Niemietz, a German lawyer, as part of the proceedings against Klaus Wegner, who was under investigation for "*insulting behaviour, contrary to Article 185 of the Criminal Code*"[51] for sending a letter with offensive content to Judge Miosga of the Freising District Court – including accusations that the judge was incompetent. The German police obtained a court order and conducted a search of Mr. Niemitez's office premises, including his client's files[52]. The case was brought before the ECtHR, whose arguments in sustaining the complaint would reshape the purview of the right to a private life and the notion of home in an unprecedented manner[53]. The court stated that:

"[However] it would be too restrictive to limit the notion to an "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings."[54]

This concept was based on the Court's conclusions in *X v. Iceland*. By stating that the right to a private life "*comprises also, to a certain degree, the right to establish and develop relationships with other human beings especially in the emotional field, for the development and fulfilment of one's own personality*" Strasbourg for the first time expands the scope of the right to a private life beyond the individual's personal sphere.

In *Niemietz*, the court uses a very pragmatic argument to justify why the professional or business activities should fall within the range of Article 8. The court points out the evident fact that "*it is, after all, in the course of their working lives that the majority of people have a significant, if*

---

[48] Judgment on the merits and just satisfaction, delivered by a Chamber, *Niemietz v Germany*, no. 13710/88, ECHR, 1992

[49] Niemietz v. Germany § 9

[50] Otto, M. (2016). The right to privacy in employment: a comparative analysis. Oxford, UK: Hart Publishing

[51] The Right to Privacy in Employment: A Comparative Analysis

[52] Global Labor and Employment Law for the Practicing Lawyer, p. 279

[53] Global Labor and Employment Law for the Practicing Lawyer, p.280

[54] Niemietz v. Germany § 29

not the greatest, opportunity of developing relationships with the outside world."[55]

It is easy to recognize the importance of this case. Prior to the ECtHR's judgment in *Niemietz v. Germany,* even the Court of Justice of the European Communities accepted that the protection offered by Article 8 of the ECHR applies to a "*the development of man's personal freedom*" and therefore is not relevant to circumstances occurring on business premises[56]. Thanks to the ECHR's contribution, *Niemietz* enables the creation of the right to privacy at the workplace by expanding the concepts of private life and home to accommodate professional activities and office premises[57].

2.3 The Reasonable Expectation of Privacy

Following *Niemietz*, the topic of workplace privacy has been addressed by the ECtHR on numerous occasions. A common thread noticeable in Strasbourg's case law dealing with employee privacy is the court's reliance on the "*reasonable expectation of privacy test*" to determine whether the circumstances of the case fall under the notion of *private life.*

The "reasonable expectation to privacy" test was formulated for the first time by the United States Supreme Court the in the 1967 case[58] *Katz vs. the United States*[59]. The case discussed the application of the Fourth Amendment[60] to the surveillance of electronic communications[61]. Katz was convicted for "*transmitting wagering information by telephone across state lines.*"[62]The evidence introduced in the trial included wiretap records of Katz' telephone conversations made from a public telephone booth[63]. The Fourth Amendment of the U.S. Constitution stipulates that *"[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*" [64] The judicial opinion in *Katz* sought to protect the right against warrantless "searches" on forms of

---

[55] Niemietz v. Germany § 29,

[56] Judgment of the Court of 21 September 1989. Hoechst AG v Commission of the European Communities, Joint Cases 46/87 and 227/88, § 18.

[57] Shaping Rights in the ECHR: The Role of the European Court of Human Rights, p. 323

[58] Winn, Peter A. (2008), *Katz and the Origins of the 'Reasonable Expectation of Privacy' Test*, McGeorge Law Review, Forthcoming. Available at SSRN: https://ssrn.com/abstract=1291870

[59] Katz v. United States, 389 U.S. 347, 360-61 (1967) (Harlan, J., concurring)

[60] U.S. Const. amend. IV

[61] *Aynes*, R.L. (1974) *Katz and the Fourth Amendment: A Reasonable Expectation of Privacy or, a Man 's Home Is His Fort*, p. 66

[62] Katz v. United States, (1967) (Harlan, J., concurring),

[63] Katz v. United States, (1967) (Harlan, J., concurring)

[64] U.S. Const. amend. IV

communications by defining such protected communications as those for which an individual has a reasonable expectation of privacy.[65] In his opinion, Justice Harlan outlined the *reasonable expectation to privacy test* in its two steps[66]: "*first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable."*"[67]

In the European context, the ECtHR utilizes "*the reasonable expectation to privacy*" as a benchmark for the application of Article 8 ECHR for the first time in 1997 in Halford vs The United Kingdom[68]. Ms. Halford, a United Kingdom eminent police officer, filed a discrimination case for being denied a promotion for over seven years. As a result, her personal and work phones were subject to interception as part of the Merseyside Police's efforts to gather evidence against her allegations of sexual discrimination. The case has been brought before the ECtHR for violations of Article 8 ECHR[69].

Strasbourg's justification on why Ms. Halford's telephone calls made from her office phone fall "*within the scope of the notions of "private life" and "correspondence" and that Article 8 (art. 8) is therefore applicable*"[70] create a new standard in the ECtHR's jurisprudence, which will become the touchstone of the right to private life at the workplace. The court sustained:

> *"There is no evidence of any warning having been given to Ms Halford, as a user of the internal telecommunications system operated at the Merseyside police headquarters, that calls made on that system would be liable to interception. She would, the Court considers, have had a reasonable expectation of privacy for such calls, which expectation was moreover reinforced by a number of factors. As Assistant Chief Constable she had sole use of her office where there were two telephones, one of which was specifically designated for her private use. Furthermore, she had been given the assurance, in response to a memorandum, that she could use her office telephones for the purposes of her sex-discrimination case…"*[71]

---

[65] Plourde-Cole, H. (2010). *Back to Katz: Reasonable Expectation of Privacy in The Facebook Age*, 38 Fordham Urb. L.J. 571, p.577

[66] Ibid, p.580

[67] Katz v. United States, p. 389 U. S. 362 (1967) (Harlan, J., concurring)

[68] Bygrave, L.A. (1998), *Data Protection Pursuant to the Right to Privacy in Human Rights Treaties*, International Journal of Law and Information Technology, volume 6, pp. 12

[69] ECtHR, Factsheet – Surveillance at workplace

[70] Halford v. The United Kingdom § 46

[71] Halford v. The United Kingdom § 45

It should be noted that the *reasonable expectation privacy* was actually first articulated by the government of the United Kingdom, which in its defence arguments stated that the "*telephone calls made by Ms Halford from her workplace fell outside the protection of Article 8 (art. 8), because she could have had no reasonable expectation of privacy in relation to them*". [72]

In my view, it is not surprising that the "*reasonable expectation of privacy test*" was utilized for the first time by the ECtHR in an employee monitoring case. While *Niemietz* expands the scope of Article 8 to accommodate professional activities, the question where to draw the line between public and private at the workplace still proved to be a challenging one. In the context of at-will employment, the individual steps out of his private sphere to enter an environment where his employer has a strong interest in maintaining a professional setting, protecting its property and mitigating risk. Since the sharing of personal information is an integral part of the employment relationship, employees have to accept some degree of interference in their privacy when becoming a part of their employer's organisation[73].

Ten years later another case relating to employee monitoring reached the ECtHR. In *Copland vs. the United Kingdom*[74], the court brought e-mails and Internet usage into the purview of Article 8 ECHR. The applicant Lynette Copland, the personal assistant to the Principle of Carmarthenshire College, complained that her telephone conversations, e-mails, and online activity were subject to monitoring by the college's Deputy Principle[75].

The court's assessment includes two conclusions with substantial influence on shaping the scope of the employee right to privacy.

First, based on previous case law the court determined that telephone conversations carried out from the workplace fall *per se* under the notions of private life and correspondence and it is therefore logical that work e-mails and Internet usage should be granted the same protection.[76] This is an example of how the undefined nature of the right to respect of private life and correspondence allows it to adapt to the continuous progression of society.

Second, the ECHR concluded that Ms. Copland had a "*reasonable expectation*" that her telephone calls, e-mail and Internet activity are going to be private, due to the absence of any

---

[72] Halford v. The United Kingdom § 43

[73] Article 29 Working Party, working document on the surveillance

[74] Judgment on the merits and just satisfaction, delivered by Court (Fourth Section), *Copland vs. the United Kingdom*, no. 62617/00, ECHR, 2007

[75] Rolland, S.E., Sirleaf, M., Telesetsky, A., Scimeca, N. & Behles, C. (2007), European Court of Human Rights Expands Privacy Protections: Copland v. United Kingdom, InSights, Volume:11, Issue: 21, available at https://www.asil.orgd

[76] https://www.asil.org/insights/volume/11/issue/21/european-court-human-rights-expands-privacy-protections-copland-v-united

prior notice that her communications will be subjected to monitoring[77].

The same year Strasbourg issued a judgment on another case related to workplace privacy. Peev v. Bulgaria concerned a search of the office of an expert employed by Bulgaria's Supreme Cassation Prosecutor's Office[78]. The office was situated in the public building of Sofia's Court House ("Съдебна Палата"). This case is indicative of a substantial shift in values. In 1997 as parts of its defence in Halford, the United Kingdom argued that *"an employer should in principle, without the prior knowledge of the employee, be able to monitor calls made by the latter on telephones provided by the employer*."[79] Ten years later the ECtHR notes that the reasonable expectation of privacy in respect of an office desk and its cabinets full of personal belongings is "*implicit in habitual employer-employee relations and there is nothing in the particular circumstances of the case – such as a regulation or stated policy of the applicant's employer discouraging employees from storing personal papers and effects in their desks or filing cabinets – to suggest that the applicant's expectation was unwarranted or unreasonable*".[80] This highlights the immense impact of Halford on the idea of employee privacy – setting its strong foundations to grow to "*implicit in habitual employer-employee relations.*"

Halford v the United Kingdom sets another standard that Strasbourg would hold in future cases regarding employee monitoring. The court states "*There is no evidence of any warning having been given to Ms. Halford, as a user of the internal telecommunications system operated at the Merseyside police headquarters, that calls made on that system would be liable to interception.*"[81] The same construction can be recognised in all the cases concerning employee monitoring to follow – the employee would have a reasonable expectation of privacy as he or she was not made aware of the monitoring activities (See *Copland v. the United Kingdom* § 44; *Köpke v. Germany, §1 in fine; Bărbulescu v. Romania §133*). This is indicative that the ECtHR uses the *prior notification for possible surveillance* as a criterion for classifying what expectations to privacy are "reasonable".

The idea that the reasonable expectation of privacy is dependent on the individual being notified about possible interference creates an intriguing interface between the case law of the ECHR and the European data protection rules. Article 10 of the Data Protection Directive and Article 13 of the GDPR enforce the principle of transparency of data processing. Both provisions require the data controller to provide specific information to the data subjects including *the*

---

[77] Ibid.

[78] Roagna, p. 21

[79] Halford v. The United Kingdom § 43

[80] Judgment on the merits and just satisfaction, delivered by the Court (Fifth Section), Peev v. Bulgaria, no. 64209/01, ECHR, 2007 § 39

[81] Halford v. The United Kingdom § 45

purposes of processing. The GDPR goes one step further and requires the information to be provided the latest "*at the time when personal data are obtained."* In practice, the above rules create an obligation for the employer in his capacity of a data controller to set the *reasonable expectation to privacy* before engaging in any processing of personal data, including monitoring.

2.4 Employee Privacy as a Balancing Exercise

In *Köpke v Germany*, the ECHR faced a different challenge. Now that professional activities and workplace communications are *prima facie* covered by the notions of "private life" and "correspondence" a new question arose about finding the balance between the employees' privacy and the employer's interest to supervise the workplace conduct and to protect its property.

The case concerned the video surveillance and recording of a supermarket employee without prior notice. Several irregular receipts prompted Mrs. Köpke's employer to order covered video surveillance of the area surrounding the cash desk[82]. The surveillance recordings confirmed that Mrs. Köpke committed theft and as a result, she was dismissed.

Since the "*video recording of the applicant's conduct at her workplace was made without prior notice on the instruction of her employer*" and that "*The picture material obtained thereby was processed and examined by several persons working for her employer and was used in the public proceedings before the labor courts*" Strasbourg was satisfied that the circumstances of the case fall within the scope of Article 8[83].

It is worth noting that two aspects differentiate Köpke v Germany from the previous ECtHR's case law on employee privacy.

First, the court takes a step back from the reasonable expectation to privacy test by classifying it as an "*a significant though not necessarily conclusive factor*."[84] Other factors examined by the court were "*the recording of the data and the systematic or permanent nature of the record*", "*whether or not a particular individual was targeted by the monitoring measure*" and "*whether personal data was processed or used in a manner constituting an interference with respect for private life*"[85]. I believe that it will be valuable to observe whether there will be future judgments of the ECtHR that incorporate other factors that would overweigh the "reasonable expectation

[82] Bogg, A. L., & Novitz, T. (2014). Voices at work: continuity and change in the common law world. Oxford: Oxford University Press, p. 451/ 452

[83] Köpke v Germany

[84] Kopke v Germany

[85] Kopke v Germany

to privacy" test and what the impact would be.

Second, the subject of this case was not the government's negative obligation to restrain from unlawful interference with the individual's private life, but the State's positive obligations[86] "*inherent in an effective respect for private life*."[87] The Court points out that the State my adopt different measures to ensure "*respect for private life and that the nature of the State's obligation will depend on the particular aspect of private life that is at issue*."[88] Such measures may include implementing legislation which allows the reconciliation of the competing interests including "*efficient criminal-law provisions*" or "*adequate regulatory framework in order to secure the respect of the physical integrity of hospital patients*". [89]

Strasbourg defines the State's positive obligation in the cases of employee monitoring as striking "*a fair balance between the applicant's right to respect for her private life and both her employer's interest in protection of its property rights, guaranteed by Article 1 of Protocol no. 1 to the Convention, and the public interest in the proper administration of justice*."[90] As such, the Court sets for the first time in the context of workplace privacy the "*fair balance of interests*" standard. This adds an extra layer to the right to employee privacy. It is now defined not only by the employee's *reasonable expectations to privacy* but also by its *proportionality* in respect to the employer's *legitimate interests*. The questions about the interaction between the "fair balance of interest" test and data protection principle of proportionality and what should be considered as the employer's legitimate interests are going to be elaborated in further detail in Chapter four of this work.

On the 5th of September 2017, the Grand Chamber of the ECtHR issued a judgment on the case of *Bărbulescu v. Romania*, overruling the judgment of the Camber of the Fourth Section of the Court, which unanimously declared that there was no violation of Article 8 of the ECHR. Several legal commentators have classified the judgment as "*a landmark privacy ruling*"[91] as it provides a new direction and reduces even further the ambiguity surrounding the legality of employee monitoring.

The applicant Bogdan Bărbulescu was discharged by the private company he was employed at for breaching the internal regulations, prohibiting the personal use of the company's facilities

[86] Voices at Work: Continuity and Change in the Common Law World, p. 451/ 452

[87] Kopke v Germany

[88] Kopke v Germany

[89] Ibid.

[90] Ibid.

[91] Deutsche Welle (2017) & Wilhelm, E.-O., (2017)

(the internet, the phone or the fax machine)[92]. The employer monitored continuingly Mr. Bărbulescu's communications on a Yahoo Messenger account he was responsible for setting up as a means for client communications.[93] As an outcome of the monitoring, it was established that Mr. Bărbulescu exchanged private messages with his fiancée and his brother.[94]

When discussing the applicability of Article 8 of the Convention the Grand Chamber of the court underlined that "*It is clear from the Court's case-law that communications from business premises as well as from the home may be covered by the notions of "private life" and "correspondence" within the meaning of Article 8 of the Convention*"[95]. It also referred to the *reasonable expectation of privacy* test but in the context set by *Köpke,* rehashing that it is "*a significant though not necessarily conclusive factor*"[96]. Similarly, to *Copland*, the court, built upon the open-ended nature of the right to private life[97], accommodating the scope of Article 8 for a new technological medium – an instant messaging application. It classifies it as "*just one of the forms of communication enabling individuals to lead a private social life*"[98] that should be covered by the notion of "correspondence", although it is used on an employer's computer.

Further, the court presents an argument which will redefine the approach to the applicability of Article 8 to employee privacy. The Grand Chamber states:

> *"[…] that it is clear from the case file that the applicant had indeed been informed of the ban on personal internet use laid down in his employer's internal regulations (see paragraph 14 above). However, it is not so clear that he had been informed prior to the monitoring of his communications that such a monitoring operation was to take place […] It is open to question whether – and if so, to what extent – the employer's restrictive regulations left the applicant with a reasonable expectation of privacy. Be that as it may, an employer's instructions cannot reduce private social life in the workplace to zero. Respect for private life and for the privacy of correspondence continues to exist, even if these may be restricted in so far as necessary."*

[92] ECHR, Information Note on the Court's case-law 210

[93] Ibid.

[94] Barbulescu v Romania§ 21

[95] Barbulescu v Romania § 72

[96] Barbulescu v Romania § 73

[97] Roagna, p. 9

[98] Barbulescu v Romania § 74

The employee's reasonable expectation is no longer a decisive factor for the scope of the workplace privacy. The court creates a new benchmark – regardless of the necessary restrictions, the employees should be allowed a certain degree of personal life at work.

I would like to point out a parallel between the reasoning behind the judgments in *Bărbulescu* and *Niemetz*. In *Niemetz* the court expands the scope of the right to private life beyond an inner circle under the argument that employment provides the individuals with a significant opportunity to develop relationships with the outside world[99], outlining the first glimpses of the workplace privacy. In *Bărbulescu*, the court pushes the limits of this right beyond the employee's reasonable expectation of privacy by stating that the "*private social life in the workplace*"[100] should never be limited to zero. In their essence, both decisions aim to protect one of the fundamental concepts of the right to respect of private life - the opportunity of "*developing relationships with the outside world*"[101].

I believe that in *Bărbulescu* does not represent a drastic change in the court's views on the reasonable expectation to privacy test. Although the court leaves unanswered the question whether Mr. Bărbulescu could have reasonably expected his communications to be private in the light of the employer's instructions, it also sets stricter criteria in regard to the notification employers should give to their employees in order to be able to carry out monitoring activities lawfully. As elaborated above the touchstone used by the court to determine the existence of reasonable expectation to privacy in its prior case law is the lack of knowledge of the surveillance measures. In *Bărbulescu* the court narrows the standard even more – the employee must not only be notified about the possible monitoring of his or her communications, but this notification should be provided prior to the introduction of such measures[102]. Strasbourg explicitly states that the "*The domestic courts had omitted to determine whether the applicant had been notified in advance of the possibility that the employer might introduce monitoring measures, and of the scope and nature of such measures*"[103]. In addition, the ECtHR provides a clear definition of what qualifies as a *prior notice* by outlining the two decisive criteria. In the first place, the notification should be provided prior to the beginning of the monitoring activities. Second, the notification should include information about "*the nature or the extent of the monitoring*"[104]. This interpretation is in line with the developments in the Data Protection legislation. According to Article 13 of the GDPR, the data controller should provide the data subject with a detailed set of information about the intended processing activities no later than

[99] Niemetz v Germany

[100] Barbulescu v Romania § 80

[101] Roagna, p.14

[102] Barbulescu v Romania § 80

[103] Information Note on the Court's case-law 210

[104] Ibid.

the "*time when personal data are obtained*". The issues about the correlation between the reasonable expectations of privacy and the data protection principle of transparency as well as my views on what the information about the nature and the extent of the monitoring should include in practice will be discussed in further details at the end of this chapter.

The other significant contribution of *Bărbulescu* to the definition of the scope of workplace privacy is the coherency of the guidance provided by the ECtHR on the factors that need to be considered when balancing the interests of employers and employees.

The legality of the employer's monitoring activities is to be determined by:

> *"whether the employee had been notified of the possibility that the employer might take measures to monitor correspondence and other communications, and of the implementation of such measures; the extent of the monitoring by the employer and the degree of intrusion into the employee's privacy; whether the employer had provided reasons to justify monitoring the employee's communications; whether it would have been possible to establish a monitoring system based on less intrusive methods and measures than directly accessing the content of the employee's communications; the consequences of the monitoring for the employee subjected to it; and whether the employee had been provided with adequate safeguards, especially when the employer's monitoring operations had been of an intrusive nature"*[105]

Legal commentators define the courts finding as an "*essential tool for delineating acceptable monitoring activities within the workplace*"[106] or "*very precise instructions with regard to the monitoring of employees*"[107]. In my view, although the court sets the direction for the future assessments of the legality of employee monitoring, it poses more questions than provides answers. Those questions and their interpretations through the lenses of European data protection rules will be the primary focus of Chapter three of this work.

2.5 Conclusion

The European Court of Human Rights, derives the right to employee privacy for the overarching right to private and family life, home and correspondence under Article 8 ECHR and gives it

---

[105] Ibid.

[106] Chatzinikolaou, A. (2017) *Bărbulescu v Romania and workplace privacy: is the Grand Chamber's judgment a reason to celebrate?,* Strasbourg Observers, available at https://strasbourgobservers.com

[107] Burlacu, E. M. (2017) *Is the monitoring of employees still possible in the light of the ECHR - Barbulescu vs. Romania case and the GDPR?, Lexilogy*, available at https://www.lexology.com

three dimensions. The professional activities defined as one of the forms of creating relationships with the others and the right to workplace privacy is framed by the employee's reasonable expectations and the balance between their interests and the legitimate goals pursued by the employer. The same concepts can be recognised in the data protection principles of transparency, purpose limitation and proportionality, which will be reviewed in the next chapter.

3 Employee Monitoring and Data Protection Rules

As elaborated in the Introduction of this paper, there is a difference between the rights to a private life and data protection. Providing adequate protection of personal data is among the safeguards ensuring privacy, yet both rights are different in scope and objectives. However, an in-depth analysis of the right to a private life in an employment context shows a considerable overlap between the positions of Strasbourg and the European Data Protection legislation. The ECtHR itself includes the particular Data Protection rules in its analysis of the relevant domestic law (see *Copland v. The United Kingdom §24- 28; Köpke v. Germany §1 and Bărbulescu v Romania §45-51).*

In my opinion, as the employer is prevailingly classified as a data controller[108] in regard to its employees' personal data, it is impossible to comprehend the breadth of the workplace privacy without examining the applicable data protection rules. Hence, this subchapter is dedicated to analysing the impact of the Data Protection Directive and the upcoming General Data Protection Regulation on the scope of employee monitoring, allowing a better understanding of employee privacy. This will be achieved through examining employee monitoring as personal data processing, the applicable data protection principles and the corresponding grounds for the lawfulness of such processing.

3.1 Employee Monitoring as Processing of Personal Data

Personal data processing is central to the data protection domain[109]. It defines the subject matter and applicability of the data protection legislation. According to Article 2 (b) of the Data Protection Directive and Article 4 (2) of the General Data Protection Regulation, *"'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection*[110]*, recording,*

[108] According to Article 2 (d) of the Data Protection Directive and Article 4 (7) GDPR ""*controller" shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data*". By virtue of the employment relationship the employer will usually be in the position to define the purpose and the means of processing of its employee's data.

[109] ICO, Guide to Data Protection

[110] Ibid.

organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;". This definition is very broad which enables an indefinite number of activities performed on personal data to be regulated. In fact, The United Kingdom's data protection authority –the Information Commissioner's Office (ICO) concluded that "*it is difficult to think of anything an organisation might do with data that will not be processing."*

The notion of *personal data* is similarly broad. It is defined in the Data Protection Directive (Article 2 (a)) as "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*". This definition has been extended by the General Data Protection Regulation (Article 4 (1)) to expressly include both "*location data",* and *"an online identifier*" as personal identifiers.

Regardless of the existence of a legal definition, identifying which information constitutes personal data is not a clear-cut exercise, and the matter has been a topic of numerous scholarly papers and regulatory guidance. The different views and approaches to categorizing information as personal data will not be discussed in this thesis. Instead, the analysis will be based on the view that *personal data* shall be any information that is linked to a living individual and can , on its own or combined with other information, lead to the identification of that individual[111]. This includes to the contents of the electronic correspondence, browsing history, telephone recordings, video footage, etc.

Consequently, in order to be classified as the processing of personal data, the employee monitoring activities should consist of *operation or set of operations performed on personal data.*

There is no precise definition of *employee monitoring,* and the notion is left to be interpreted by courts, regulators, and data protection practitioners[112]. A review of the existing authoritative guidance on the topic indicates that the regulators have chosen to address the issue by listing examples of activities amounting to employee monitoring. In its Employment Practices Code, the ICO provides the following definition monitoring which will serve as the basis of the for the current analysis:

"activities that set out to collect information about workers by

[111] ICO, What is personal data? – A quick reference guide, p. 7-8.

[112] ICO, The Employment Practices Code, p. 59

keeping them under some form of observation, normally with a view to checking their performance or conduct"[113].

Such activities can be classified in four categories: (i) monitoring of electronic communications, (ii) monitoring of Internet usage (iii) video surveillance and (iv) use of new technologies facilitating intrusive monitoring[114]

3.1.1 Monitoring of Electronic Communications

Traditionally the monitoring of the employees' electronic communications, such as telephone conversations, e-mail and instant messaging has been viewed as the biggest threat to the employee's right to a private life[115]. *Halford v. the United Kingdom* concerns the lawfulness of phone calls interception, *Copland v. the United Kingdom* tackles the issues surrounding the collection of personal data relating to the use of e-mail, and the *Bărbulescu v. Romania* relates to the legality of the recording and accessing the content of messages sent via an Internet-based instant messaging application. Another example is Article 29 Working Party's Working document on the surveillance of electronic communications in the workplace, which includes a section explicitly designated for email monitoring.

Naturally, all the listed forms of electronic communications monitoring involve, at the very least, the collection, recording, consultation and use of personal data. The monitoring of telephone conversations, if not carried out in real time, requires the recording of the telephone numbers of the calling and receiving party, as well as the contents of the conversation, all of which constitute personal data. Monitoring employee emails would require, at minimum, the collection of the sender and recipients email addresses. The same principle applies to messages exchanged via an instant messaging application. Hence, the monitoring of the employee's electronic communications will usually involve processing of personal data, falling within the scope of the data protection legislation.

3.1.2 Monitoring of Internet Usage

The monitoring of employee's Internet usage, subject to ECtHR's decision in *Copland v. the United Kingdom,* has turned into a standard for the modern-day employer. According to a survey presented in "*The Muse*", 64% of the employees use the Internet at work for non-work-related matters[116]. Additionally, 60% of the online purchases and 65% of the YouTube views

---

[113] ICO, The Employment Practices Code, p. 59

[114] Article 29 Working Party, Opinion 2/2017, p. 3

[115] Ibid.

[116] Herman, L. *How Much Time Do We Waste at Work? (Hint: It's Scary)*, The Muse, available at https://www.themuse.com

are generated during regular working hours[117]. The unauthorised use of the Internet at work hampers employee productivity, but also creates security risks, such as exposure to malware or malicious dissemination of company propriety information[118]. Many employers recognise monitoring of the employees' Internet activities as a viable solution. The different Internet monitoring techniques include, but are not limited to, accessing browser history, surveillance of network traffic and the highly intrusive user action monitoring – capturing and recording all actions made on the employee's computer[119]. Apparently, such activities constitute processing of personal data. Note that even access patterns are considered personal data if they allow for the identification of a particular employee[120].

3.1.3 Video Surveillance

Video Surveillance, or the use of CCTV (closed-circuit television), is considered as highly intrusive to employee privacy[121]. Such surveillance will usually result in processing of personal data as the recorded video images allow the identification of distinct individuals[122]. Furthermore, the use of CCTV amounts to the collection, recording, storage, and, use of special categories of personal data defined by Article 9 of the GDPR, as personal information revealing racial or ethnic origin and biometric data[123]. Recorded images will likely allow the determination of the employee's racial or ethnic origin, while facial images are *per se* classified as biometric data under Article 4 (14) of the GDPR.

3.1.4 Use of New Technologies Facilitating Intrusive Monitoring

Several new technologies intended for ensuring network security and data integrity pose high risks of potentially pervasive monitoring[124]. Such technologies include Data Loss Prevention tools, security measures recording the employee access to the employer's facilities, application tracking, keylogging and monitoring of personal devices[125]. The use of technologies for the purpose of detecting and preventing data loss and security breaches often amounts to real-time monitoring of communications, gathering of large amounts of personal data and, potentially, automated decision making[126]. Consequently, such uses must be classified as processing of

---

[117] Ibid

[118] Gogan, M. (2016), *How do Companies Monitor Employee Internet Usage*, TG Daily, available at http://www.tgdaily.com

[119] Ibid.

[120] Article 29 Working Party, Opinion 8/2001, p. 13

[121] Carey, P., & Treacy, B. (2015). *Data protection: a practical guide to UK and EU law*. Oxford: Oxford University Press., p.228

[122] Ibid.

[123] Ibid.

[124] Article 29 Working Party, Opinion 2/2017, p. 13

[125] Article 29 Working Party, Opinion 2/2017, p. 13

[126] Article 29 Working Party, Opinion 2/2017, p. 13

personal data.

In conclusion, workplace monitoring activities – regardless of their form – are naturally designated to gathering formation for the performance and conduct of the employees. In the majority of cases, such activities will amount to the processing of personal data, falling under the scope of the data protection legislation.

3.2 Employee Monitoring in Compliance with the Principles of Data Protection

The processing of personal data is an integral part of the labour relationship Employee monitoring is differentiated from the other workplace-processing activities because of its predisposition to intrude into employee privacy Moreover, the existence of monitoring activities is not as visible as for example the collection of personal information for tax or social security purposes and is therefore easily carried out without the employee's knowledge[127]. Nonetheless, the employer has a legitimate interest to monitor, to a certain extent, its employees in order to maintain a sound work environment and safeguard the security of its business operations[128]. It is impossible to provide a one-size-fits-all solution that guarantees the lawfulness of employee monitoring, and the answer is usually – *it depends*[129]. A good starting point is examining what limits do the principles of data protection impose on such activities, helping to shape the right to employee privacy.

Why are the principles so important? The principles relating to the processing of personal data are abstractions which define the direction of the legislation[130] and form the backbone of the Data Protection Directive and the General Data Protection Regulation. Recital 14 of the DPD explicitly states that the data "*protection principles must apply to all processing of personal data*" and the GDPR introduces a fine of up to 20 000 000 EUR or up to 4% of the global annual turnover of the undertaking for failure to comply with the "*basic principles of processing*". [131] Furthermore, the GDPR creates a new *accountability principle*[132] - requiring data controllers to be able to demonstrate compliance with all other data protection principles. Simultaneously, the principles related to the processing of personal data serve as guidance to the regulators in

[127] Article 29 Working Party, Opinion 2/2017, p. 4

[128] See Article 29 Working Party, Working document on the surveillance, p. 8

[129] Article 29 Working Party, Opinion 8/2001, p. 19

[130] See Bygrave, L. A. (2014). *Data privacy law: an international perspective.* Oxford: Oxford University Press., p. 145

[131] See GDPR, Article 83 (5) (a)

[132] See GDPR, Article 5 (2)

interpreting and enforcing the legislation[133].

3.2.1 Lawful and Fair Processing

The principle of lawful processing requires personal data to be processed in compliance with the provisions of Section II of the Data Protection Directive and Articles 6 to 10 of the General Data Protection Regulation[134], meaning that it needs to fall under one of the conditions for lawfulness. Due to the characteristics of employee monitoring discussed above it is difficult to imagine it classified as "necessary" for the performance of a contract, for compliance with a legal obligation, to protect any vital interests of individuals or for it to be carried out in the public's interests. As a result, the two grounds of relevance to employee monitoring are *consent* (Article 7 (a) DPD and Article 6 (1) (a) GDPR) and the *legitimate interests pursued by the employer* (Article 7 (f) DPD and Article 6 (1) (f) GDPR).

Article 4 (11) GDPR provides an extensive definition of consent:

> *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*.

The requirement for the consent to be freely given is of particular significance for the legality of employee monitoring. According to recital 42 of the Regulation, the consent "*should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment*". If there is an imbalance in the relationship between the controller and the data subject, it will be impossible to classify the consent as freely given, making it highly unlikely for the employer to be able to obtain a valid permission from its employees for any type of workplace monitoring[135].

This position has been defended multiple times by the Article 29 Working Party which in its *Opinion 2/2017 on data processing at work*, rehashes that for the most types of workplace processing activities "*the legal basis cannot and should not be the consent of the employees (Art 7(a)) due to the nature of the relationship between employer and employee*"[136].

The requirement of the consent to be freely given with no imbalance in the relationship between controller and individual is one of the manifestations of the principle of fair processing of

---

[133] See Bygrave, L. A. (2014)., p. 145

[134] Article 29 Working Party, Opinion 8/2001, p.14

[135] ICO (2017), *Consultation: GDPR consent guidance*

[136] Article 29 Working Party, Opinion 2/2017, p.6

personal data[137]. Fairness entails that controllers should not abuse their "*monopoly position*" and should not press data subjects to provide personal data without justifications[138]. This means that if employee monitoring is based on consent, it will not only be unlawful but also unfair. The employer should not be given the opportunity to use its disciplinary powers to "persuade" employees into agreeing to be subject to monitoring.

Ergo, employers are most likely to rely on Article 7 (f) of the Data Protection Directive and Article 6 (1) (f) from the General Data Protection Regulation to legitimise employee monitoring as necessary for the purpose of their legitimate interests[139]. The application of this lawful ground calls for balancing the interest of the employer with interests and fundamental rights of employees[140], similarly to the exercise carried out by the ECtHR in *Bărbulescu v Romania*. The Article 29 Working Party has issued guidance on the factors that need to be taken into account when carrying out that balancing exercise[141].

The notion of the *interest* in Article 7 (f) of the Data Protection Directive and Article 6 (1) (f) of the General Data Protection Regulation relates to benefits the controller derives from the processing[142] and an interest should be considered as legitimate as long as it is in accordance with the law in its broadest sense[143]. In its Opinion, the Article 29 Working Party explicitly lists "*prevention of fraud, misuse of services, or money laundering, employee monitoring for safety or management purposes*" and "*physical security, IT and network security*" [144] as an example of situations that may amount to legitimate interests of the employer.

When carrying out the balancing exercise required by Article 7 (f) of the Data Protection Directive and Article 6 (1) (f) from the General Data Protection Regulation the employees' interests or fundamental rights and freedoms need to be taken into account. It should be noted that both the Directive and the Regulation use only the word *interests* instead of *legitimate interests* meaning that the data subject has been provided with a wider protection.[145]

Assessing the employer's legitimate interests in the light of the employee monitoring requires one to establish: (i) whether the monitoring is intended to protect the employer's exercise of

---

[137] See See Bygrave, L. A. (2014)., p. 146

[138] Ibid.

[139] Article 29 Working Party, Working document on the surveillance, p. 21

[140] Article 29 Working Party in its *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC.* p.1

[141] Ibid.

[142] Ibid., p. 24

[143] Ibid, p. 24

[144] Ibid, p. 25

[145] Ibid, p.30

fundamental rights[146] such the property rights, guaranteed by Article 1 of Protocol no. 1 to the ECHR; (ii) or its carried out in the public interest, for instance when it is aimed at prevention of fraud and financial crime[147]; (iii) it is related to another legal ground without being able to fully qualify for it[148] which is the case with monitoring of ensuring network security in compliance with the requirements of Article 32 of the GDPR.

The second step of the balancing exercise is establishing the impact of the monitoring on the employees. This assessment includes establishing the potential consequences for the employee – including the creation of privacy-related risk[149]. Recital 75 of the GDPR provides a list of the possible risks that need to be taken into account, namely:

> "*physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects*."

The impact assessment requires an estimation of the likelihood of the risk materialising and its severity[150]. Next, the nature of the data that is to be processed needs to be taken into account[151].

---

[146] Ibid, p. 34
[147] Ibid, p. 35
[148] Ibid.
[149] Ibid, p. 37
[150] Ibid, p. 38
[151] Ibid.

As a rule of the thumb if the monitoring of employee's activities requires collection and recording of sensitive data, it is more likely to have adverse effects on the employee and overthrow the employeer's interests.[152]

One should also take into account the means of monitoring and the extent to which they intrude into the employees' privacy. For instance, the monitoring of e-mail correspondence for prevention of unauthorised disclosure of company proprietary information through utilising a firewall that notifies the security team for any attempts of sending messages bigger than 5 MB, resulting in the security team checking the content of such messages is more likely to be lawful under Article 7 (f) of the Data Protection Directive and Article 6 (1) (f) from the General Data Protection Regulation than the recording and accessing the contents of all messages sent from company e-mails.

Another critical factor to consider is the *reasonable expectations* of the employees concerning whether they will be subject to monitoring and to the extent of the monitoring activities. Going back to the example with e-mail monitoring – it is more likely that the employees expect their e-mail correspondence to subject to monitoring that the installation of keylogging software on their devices. This criterion can be traced back to the *reasonable expectation of privacy* doctrine established by the ECtHR, but it is also another manifestation of the principle of fairness[153].

An additional element that it is of particular importance in regard to workplace monitoring is the balance of the relationship between the data subject and the controllers[154]. As previously elaborated, the employer will always be in a dominant position in respect of its employees.

It should be noted that the purpose of the assessment of the impact of the workplace monitoring is not to erase any possibility for negative consequences for the employees but to ensure that the impact is proportionate[155]. Similarly, to the circumstances in *Köpke v Germany* – as a result of the covert video surveillance, Mrs. Köpke was dismissed from her job, but the monitoring activities are still considered lawful as they were carried out in the interest of the employer to protect its property.

The last step is the actual balancing exercise – establishing the provisional balance by asserting whether the legitimate interests of the employer outweigh the interests and fundamental rights of the employees[156]. In the cases where there is not a clear-cut answer, it is advisable for the employer to the introduce additional safeguards that go beyond the requirements of the data

---

[152] Ibid., p. 39

[153] See See Bygrave, L. A. (2014).,p.146

[154] Article 29 Working Party in its *Opinion 06/2014*, p. 39

[155] Ibid, p. 41

[156] Ibid, p. 41

protection legislation as such safeguard may mitigate the adverse effects on employees and *tilt the balance* in favour of the employer.[157]

In conclusion, it should be underlined that the proper balancing of the employer's legitimate interests and the employee's interests and fundamental rights will ensure that workplace monitoring will not only be lawful but also compliant with the principle of fairness of processing.

One dimension of the principle of fairness of processing has been deliberately left out the presentation so far. There has been an agreement in the scholar literature[158] and the regulatory guidance[159] that, in order to be fair, the processing should be transparent, thus accommodating the principle of transparency under the notion of fairness. This is understandable as the Data Protection Directive only implicitly introduces this principle through the requirements for the provision of information to the data subject stipulated it Article 10 and 11. As the General Data Protection Regulation sets forth transparency as a distinct principle of data protection in Article 5 (1) (a), it will be elaborated separately in the next point.

3.2.2 Transparency

The principle of transparency, although not clearly defined in the Directive, has always been central to ensuring adequate data protection[160]. Providing information about the data processing activities gives the data subjects the opportunity to act upon that knowledge, including the possibility to exercise the rights provided by the data protection legislation.[161] Transparency can be seen as a precondition for the legality of the processing, as even it falls under one of the criteria prescribed by Article 7 of the DPA and Article 6 (1) of the GDPR, there still will be a breach of the data protection rules if the data subjects are not appropriately notified for it[162].

The principle of transparency is specified through the requirement to the provide information under Section IV of the DPA and Article 13 and 14 of the GDPR. As the provisions of the Regulation require more detailed information than the Directive, those provisions will be the focus of the following discussion.

The requirement to provide information when the personal data is collected from the data

---

[157] Ibid, p.51

[158] See Bygrave, L. A. (2014), p. 146

[159] See ICO, Guide to Data Protection, Processing personal data fairly and lawfully (Principle 1)

[160] European Data Protection Supervisor, Transparency available at https://edps.europa.eu/data-protection/our-work/subjects/transparency_en

[161] Wayland, K., Armengol, R., Johnson, D.G., *When Transparency Isn't Transparent. Campaign Finance Disclosure and Internet Surveillance* in Fuchs, C., Boersma, K., Albrechtslund, A., & Sandoval, M. (2013). *Internet and Surveillance The Challenges of Web 2.0 and Social Media*. Florence: Taylor and Francis.

[162] Article 29 Working Party, Opinion 08/2001, p. 20

subject (Article 13 GDPR) is applicable to the majority of employment relationships, as it is a standard practice for the employer to be in direct contact with its employees. However, Article 14, titled "*Information to be provided where personal data have not been obtained from the data subject*" is relevant when the employer uses a third party recruitment to manage its employment relations.

In order to ensure compliance with the Article 13 and 14 of the GDPR, the employer must provide the employees with the required information "*at the time the personal data are obtained*", meaning no later than the beginning of monitoring activities. If the emails, phone calls, and Internet activities are subject to real-time monitoring or there is a CCTV installed at the office premises, the employer should notify its employees, without undue delay, during their very first day of employment. It is a standard practice for the information required by Article 13 and 14 of the GDPR to the delivered in the form of a privacy policy. To be compliant with the Regulation the privacy policy needs to be in a "*concise, transparent, intelligible and easily accessible form, using clear and plain language*"[163] which means that it shouldn't be buried somewhere in the contract of employment or in a hundred-page long employee manual.

To meet the standards of the GDPR, the employee privacy policy needs to include information about "*the purposes of the processing for which the personal data are intended"*[164]. The employees should be informed about the particular form of monitoring as well as the purpose it is intended for[165]. Furthermore, the purpose of the employee monitoring needs to be communicated in combination with the legal basis justifying it. [166] As it was determined above the most likely ground for the lawfulness of employee monitoring is the legitimate interest pursued by the employer. Therefore, the employer is obligated to list all its legitimate interest justifying the monitoring activities.

Next, employees need to be informed of their rights as data subjects, including the right to request access to all of the information gathered through the monitoring practices, the right to erasure of personal data or restriction of the monitoring or the right object to be the subject of monitoring[167]. The information gathered through employee monitoring inevitably includes company confidential data. Thus it would be interesting to follow how the conflict between business confidentiality and data portability will be resolved.

It is questionable whether Article 13 (2) (e) and Article 14 (2) (e) of the GDPR, requiring the

---

[163] GDPR, Article 12 (1)

[164] GDPR, Article 13 (1) (c) and Article 14 (1) (c)

[165] Article 29 Working Party, Working document on the surveillance of electronic communications in the work-place, p. 15

[166] GDPR, Article 13 (1) (c) and Article 14 (1) (c)

[167] GDPR, Article 13 (2) (b) and Article 14 (2) (b)

provision of information "*whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data*" would be applicable to employee monitoring. The use of the verb "*provide"* implies the an actual behavior form the individual. However, the nature of electronic communications monitoring, monitoring of Internet access or the use of CCTV, involves the employer collecting information without the employee actually providing it. As a result, a failure to provide such data is impossible in practice. This question requires further research and analysis, which is outside the scope of this discussion.

The GDPR requires several additional pieces for information to be provided to the employees including (i) the identity and contacts details of the employer[168]; (ii) when there is an appointed data protection officer – his or her contacts[169]; (iii) the recipients of the data gathered as a result of the employee monitoring[170]; (iv) whether the data will be transferred outside of the European Economic Area[171]; (v) the data retention period[172], (vi) the right to submit a complaint before the data protection authority[173] and (vii) where the monitoring will result in automated decision making[174] at they do not present any specifics regarding to employee monitoring, they will not be discussed in detail.

Additional information, falling outside the scope of the GDPR which should be added to a privacy policy as good practice includes information on whether the private use of the company's information technology facilities (such as email and the Internet) is allowed and to what extent, what information security safeguards have been put in place and what will be consequences of the monitoring activities (for example, the consequences of an employee attempting to send sensitive company information to his or her personal e-mail).[175]

3.2.3 Purpose Limitation and Necessity (Data Minimisation)

The next principle of crucial importance for the legitimacy of employee monitoring is the purpose limitation in particular reviewed in combination with the principle of necessity (data minimisation). Purpose limitation is one of the core principles of data protection[176]. It requires personal data to be "*collected for specified, explicit and legitimate purposes and not further*

---

[168] GDPR, Article 13 (1) (a) and Article 14 (1) (a)

[169] GDPR, Article 13 (1) (b) and Article 14 (1) (b)

[170] GDPR, Article 13 (1) (e) and Article 14 (1) (e)

[171] GDPR, Article 13 (1) (f) and Article 14 (1) (f)

[172] GDPR, Article 13 (2) (a) and Article 14 (2) (a)

[173] GDPR, Article 13 (2) (d) and Article 14 (2) (d)

[174] GDPR, Article 13 (2) (f) and Article 14 (2) (f)

[175] See Kuner, C. (2007). European data protection law: Corporate compliance and regulation. Oxford: Oxford University Press, p. 269-270

[176] Article 29 Working Party, Opinion 03/2013 on purpose limitation, p. 4

processed in a way incompatible with those purposes".[177] Designating the purpose of the monitoring is vital for defining its lawful grounds under Article 7 DPD or Article 8 GDPR and for achieving compliance with the other data protection principles[178]. The other function of this principle is to limit the further processing in a manner incompatible with the initial purpose. For example, if the employer's privacy policy states that the employee's Internet activity will be monitored to ensure information security, but the gathered data is further used to evaluate work performance, this second purpose would be in breach of the purpose limitation principles.[179]

The necessity or data minimisation principle requires the data gathered through the employee monitoring to be "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*".[180] For instance, if a CCTV surveillance system is introduced to ensure the security of a server room, it will be contrary to the necessity principle to install cameras in the spaces designated for leisure time, such as the office kitchen. In order to comply with the necessity principle, the monitoring should "must be carried out in the least intrusive way possible".[181]

3.2.4 Proportionality

The principle of proportionality although not explicitly mentioned in the legislation is reflected in the principles of the lawfulness of processing, purpose limitation and necessity as well as in multiple data protection rules[182]. The balancing test carried out under Article 7 (f) of the Data Protection Directive and Article 6 (1) (f) of the General Data Protection Regulation requires an assessment whether the impact of processing carried out for the purposes of the legitimate interests pursued by the employer is proportionate to the impact on the employees. Simply put, the more intrusive the monitoring is, the less likely it is to be considered proportionate[183]. For instance, it will be proportionate if the employer chooses to block the access to social media websites instead of relying on user action monitoring applications that capture and record all actions made through the employee's personal social media account[184].

---

[177] DPD, Article 6 (1) (b) and GDPR Article 5(1) (b)

[178] Article 29 Working Party, Opinion 03/2013, p. 4

[179] Ibid.

[180] GDPR, Article 5 (1) (c)

[181] Article 29 Working Party, Opinion 8/2001, p. 25

[182] See Bygrave, L. A. (2014)., p. 148

[183] Article 29 Working Party, Opinion 8/2001, p. 21

[184] Article 29 Working Party, Working document on the surveillance of electronic communications in the workplace, p. 18

3.2.5 Integrity and Confidentiality

In contrast to the Data Protection Directive, the General Data Protection Regulation includes data security as one of the principles relating to the processing of personal data. The employer will be obligated to introduce "*appropriate technical or organisational measures*"[185] in order to prevent "*unauthorised or unlawful processing and against accidental loss, destruction or damage*".[186] Such measures may encompass the introduction of written policies and procedures, governing the employee monitoring activates [187] or using access control, encryption or even implementing the International Organization for Standardization's ISO/IEC 27000 information security standards.[188] Minimising the data breaches caused by human error should be a high priority.[189] According to the United Kingdom's Information Commissioner's Office, the two most common reasons for data security incidents are a loss of paperwork and unlawful disclosure of data being sent via email to the wrong recipient[190]. A possible solution is providing access to the data gathered through the employee monitoring to a very limited number of employees.

3.3 Conclusion

Employee monitoring as a form of data processing is framed the principles of lawful and fair processing, transparency, purpose limitation, necessity, proportionality and integrity. However, those principles serve a more universal purpose than just being a basis for compliance with the data protection legislation. Read in the conjunction with the ECtHR's case law on employee surveillance they help shape and safeguard the workplace privacy.

4 The Boundaries of Employee Monitoring

The right to Employee Privacy is a multidimensional one. On the one hand, as it was elaborated in the second chapter of this thesis, it is one of the many offshoots of the Right to respect for private and family life as stipulated in Article 8 of the European Charter of Human Rights. It evolves significantly based on judgements of the European Court on Human Right's focused on cases of employee surveillance. In *Niemietz v. Germany,* the court accommodates the professional actives in the purview of Article 8, based on the belief that the workplace provides

---

[185] GDPR, Article 5 (1) (f)

[186] Ibid

[187] GDPR, Article 24 (2)

[188] See International Organization for Standardization, ISO/IEC 27000 family - Information security management systems, available at https://www.iso.org/isoiec-27001-information-security.html

[189] Carey, P., & Treacy, B. (2015). *Data protection: a practical guide to UK and EU law*. Oxford: Oxford University Press., p.228

[190] ICO (2017), Data security incident trends by sector and type 2017/18, London

the individuals a ground for establishing relationships with the outside world. More than twenty years later in *Bărbulescu v Romania* the court sets a new standard that the employees not only have the right to a private life at the workplace but also this right should not be limited to zero.

The interest of the employer should always be balanced with the rights and freedoms of the workers[191], and this judgment provides guidance on the factors that need to be taken into account in order to ensure proportionality and avoid arbitrariness. Those factors include:

> *"(i) whether the employee has been notified of the possibility that the employer might take measures to monitor correspondence and other communications, and of the implementation of such measures […]; (ii) the extent of the monitoring by the employer and the degree of intrusion into the employee's privacy […]; (iii) whether the employer has provided legitimate reasons to justify monitoring the communications and accessing their actual content […]; (iv) whether it would have been possible to establish a monitoring system based on less intrusive methods and measures […]; (v) the consequences of the monitoring for the employee subjected to it*"[192] and *"(vi) whether the employee had been provided with adequate safeguards, especially when the employer's monitoring operations were of an intrusive nature".*[193]

On the other hand, employers – in their capacity of data controllers regarding the personal data of their employees – are subject to the data protection legislation. These means that any kind of processing activity performed on the employees' personal information, including monitoring of their electronic communications, Internet access, and video surveillance, should comply with the principles of lawful and fair processing, transparency, purpose limitation and necessity (data minimisation), proportionality and integrity and confidentiality.[194]

This chapter will review the general principles applicable to ensuring respect for private life and correspondence in an employment context as set forth by the ECtHR in conjunction with the above principles of data protection. The result is a demonstration of how the two regimes coexist[195] – creating a sound framework that safeguards employee privacy.

---

[191] ECtHR, *Bărbulescu v Romania, §121*

[192] Ibid.

[193] Ibid.

[194] Article 29 Working Party, Working document on the surveillance of electronic communications in the work-place, p. 8

[195] See further Bygrave, L.A. (1998), *Data Protection Pursuant to the Right to Privacy in Human Rights Treaties,* International Journal of Law and Information Technology, volume 6, pp. 247–284

4.1 Prior Notification and Transparency

The first criterion set by the ECtHR is the employee to be notified in advance of the existence of the surveillance and/or monitoring measures and for their nature and extent[196]. In the case of *Bărbulescu v. Romania,* the employer has communicated twice the prohibition of the personal use of the company's resources[197]. However, the employer failed to notify the employees that the ban would be enforced through the monitoring of their communications[198], breaching the above principle.

The requirement for prior notification is not a novelty for the case law of the ECtHR on employee monitoring and can be traced back to *Halford v. the United Kingdom*[199]. When examining the question about the employee's reasonable expectation of privacy the court bases its conclusions on whether the employee has been notified of the surveillance or monitoring. It can be concluded that prior notification is definitive for the expectations of employees. If they are not made aware of monitoring activities, then it is reasonable for them to expect that their communications will be private. From the opposite perspective, the employers may use such notification to set clear boundaries for the employees' expectation of privacy.

Such prior notification can be achieved through the introduction of a "*concise, transparent, intelligible*"[200] privacy policy. The contents of such policy are predefined by the information requirements under Article 12 of the Data Protection Directive and Article 13 and 14 of the GDPR – one of the manifestations of the principle of transparency. As it was elaborated in Chapter three, those rules require detailed information to be provided to the employees "*at the time the personal data are obtained*"[201] meaning no later than the beginning of monitoring activities. The employees need to be notified about the monitoring activities as well as the purposes of the monitoring and the employer's interest justifying it.[202]

Next, the employees need to be informed of their rights as data subjects and how to exercise such rights. Further the GDPR requires several additional pieces for information to be provided to the employees including: (i) the identity and contacts details of the employer[203]; (ii) the

---

[196] ECtHR, *Bărbulescu v Romania, §121*

[197] ECtHR, *Bărbulescu v Romania, §121 (i)*

[198] ECtHR, *Bărbulescu v Romania, §13 (i)*

[199]See further Bygrave, L.A. (1998), *Data Protection Pursuant to the Right to Privacy in Human Rights Treaties*, International Journal of Law and Information Technology, volume 6, p. 12

[200] GDPR, Article 12 (1)

[201] GDPR, Article 13 (1) and Article 14 (1)

[202] Article 29 Working Party, Working document on the surveillance of electronic communications in the work-place, p. 15

[203] GDPR, Article 13 (1) (a) and Article 14 (1) (a)

contacts of the data protection if one is appointed[204]; (iii) the individuals having access to data through the employee monitoring[205]; (iv) whether there will be a data transferred outside of the European Economic Area[206]; (v) the data storage period[207], (vi) the right to submit a complaint before the data protection authority[208] and (vii) where the monitoring will result in automated decision making[209].

However, transparency is not a silver bullet[210]. There mere knowledge about the existence of monitoring activities does not protect employee rights if they are not provided with a means to object to and prevent such activities. The value of the transparency princple under the data protection legislation, as well as the notification requirements as set by the ECHR, is that they serve as a gateway allowing employees to exercise their data subject rights in particular the right of access by the data subject under Article 14 of the DPD and Article 15 of the GDPR and the right to object under Article 14 of the DPD and Article 21 of the GDPR, which is supplemented by the newly introduced right to restriction of processing (Article 18 GDPR)[211]. Moreover, I believe that the transparency requirements would act as an effective deterrent on employers seeking to implement overly intrusive monitoring activities. Knowing that employees must be notified in detail of the existance of monitoring activities, employers will be more reluctant to introduce measures which are highly intrusive.

4.2 The Extent and Degree of Intrusion of the Monitoring, the Principle of Proportionality and Privacy Impact Assessments

Second, the ECtHR requires an assessment of the "*the extent of the monitoring by the employer and the degree of intrusion into the employee's privacy*"[212] as well as an examination of the possibility for the implementation of less invasive monitoring techniques.[213] This criterion corresponds to the second step of the balancing test under Article 7 (f) of the Data Protection Directive and Article 6 (1) (f) from the General Data Protection Regulation, namely evaluating the impact that the anticipated monitoring activities on the employees – including identifying possible privacy risks and their likelihood and severity.

---

[204] GDPR, Article 13 (1) (b) and Article 14 (1) (b)
[205] GDPR, Article 13 (1) (e) and Article 14 (1) (e)
[206] GDPR, Article 13 (1) (f) and Article 14 (1) (f)
[207] GDPR, Article 13 (2) (a) and Article 14 (2) (a)
[208] GDPR, Article 13 (2) (d) and Article 14 (2) (d)
[209] GDPR, Article 13 (2) (f) and Article 14 (2) (f)
[210] Wayland, K., Armengol, R., Johnson, D.G., p. 239
[211] Ibid
[212] ECtHR, *Bărbulescu v Romania, §121 (ii)*
[213] ECtHR, *Bărbulescu v Romania, §121 (iv)*

The objective is to ensure that the degree of intrusion in the employee's privacy is proportionate to the goals pursued by the employers. For instance, in its Working document on the surveillance of electronic communications in the workplace, the Article 29 Working Party advises to always choose prevention over detection[214]. If the employees are banned from streaming music at work, it will be proportionate to bock the access to websites like YouTube and Spotify other than accessing and reviewing the browsing histories of the employees on a recurring basis.

Another example is a decision of the Federal Labour Court of Germany, which concluded that installing a keylogging software on the company's devices to record every key stroke is illegitimate as it is too intrusive on the employee's right to privacy[215]. However, the court pointed out that the use of such employee monitoring techniques could be justified in order to prevent alleged criminal offences or severe negligence of work responsibilities.[216] This serves as an excellent example of the application of the proportionality principle.

An interesting question arises with regards to the enforcement of the principle of proportionality under the GDPR. According to Article 83 infringements of "*the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9*"[217]will result to fines up to 20 000 000 EUR, or to 4 % of the global annual turnover of an undertaking. However, the principle of proportionality is not explicitly listed in any of the above articles. In my opinion data controller can still be implicitly subject to an administrative fine for introducing disproportionate processing, for example for failing to appropriately establish the balance between the employer's legitimate interests and the employees' interest, rights and freedoms. In that case the legal basis for the fine will be breach of Article 6 (1) (f).

The GDPR provides a tool ensuring that "*the extent of the monitoring by the employer and the degree of intrusion into the employee's privacy*"[218] would be assessed before the launch of the monitoring activity. Article 35 of the Regulation provides that a privacy impact assessment is required "*[w]here a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons*"[219]. The assessment must be carried out prior

---

[214] Article 29 Working Party (2002), Working document on the surveillance of electronic communications in the workplace

[215] The Local (27 July 2017), *German court rules bosses can't use keyboard-tracking software to spy on workers*, Retrieved from https://www.thelocal.de

[216] Ibid

[217] GDPR, Article 83 (5) (a)

[218] ECtHR, *Bărbulescu v Romania, §121 (ii)*

[219] GDPR, Article 35 (1)

the processing. Article 29 Working Party has issued Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "*likely to result in a high risk*" for the purposes of Regulation 2016/679. Employee monitoring falls under at least two of the high-risk criteria – systematic monitoring and data concerning vulnerable data subjects. Hence it will require a privacy impact assessment to be carried out prior to its implementation[220].

Assessing the impact of the anticipated monitoring activities will and the provision of appropriate safeguard to mitigate the identified risk will guarantee the implantation of the least intrusive measures ensuring compliance with the principle of proportionality

4.3 The Legitimate Reasons Justifying the Monitoring and the Employer's Legitimate Interests

The next relevant factor is "*whether the employer has provided legitimate reasons to justify monitoring the communications and accessing their actual content*"[221]. The overlap with the sixth ground for lawfulness of processing under Article 7 (f) DPD and Article 6 (1) (f) GDPR – necessity for the purposes of the legitimate interests pursued by the controller is evident.

The employee may have different reasons justifying the monitoring: (i) exercising of fundamental rights[222] such the property rights, guaranteed by Article 1 of Protocol no. 1 to the ECHR; (ii) prevention of fraud and financial crime[223]; (iii) or compiling with regulations that require "*reasonable steps*" to achieve compliance with creating a legal obligation for employee monitoring , such as Article 16 (7) of the Directive 2014/65/EU of the European Parliament and of the council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (MiFID II)[224].

The ECtHR provides several examples of legislative instruments that may provide justification for employee monitoring. The International Labour Office's Code of Practice on the Protection of Workers' Personal Data allows secret monitoring if "*it is in conformity with national legislation*"[225] or "*if there is suspicion on reasonable grounds of criminal activity or other*

---

[220] Article 29 Working Party Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.

[221] ECtHR, *Bărbulescu v Romania, §121 (iii)*

[222] Article 29 Working Party in its *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC,* p. 34

[223] Ibid, p. 35

[224] Article 16 (7) of MiFID requires investment firms to "take all reasonable steps to prevent an employee or contractor from making, sending or receiving relevant telephone conversations and electronic communications on privately-owned equipment which the investment firm is unable to record or copy".

[225] See ECtHR, *Bărbulescu v Romania, §38 and* The International Labour Office, *Code of Practice on the Protection of Workers' Personal Data (1997),* §6.14, (2) (a)

serious wrongdoing"[226] and continuous "*if required for health and safety or the protection of property*."[227]Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment lists security as a legitimate reason for the surveillance of professional electronic communications[228].

An example of legislation which justifies the monitoring of employees' communications is the Regulation of Investigatory Powers Act (RIPA)[229]. Although the Act forbids the interception of electronic communications without the consent of all parties it provides an exception benefiting the employers[230]. The RIPA grants the employers the possibility to lawfully monitor their employee's communications under the following exhaustive situations: (i) to determine the existence of business relevant information; (ii) to ensure adherence to internal compliance procedures and regulatory requirements; (iii) to enforce employee performance standards; (iv) for the purpose of crime detection and prevention; (v) to ensure information technology system integrity.[231] It should be noted that the provisions of RIPA permitting employee monitoring are permissive[232], meaning that the processing will not qualify as necessary for compliance with a legal obligation (DPA, Article 7 (c) and GDPR, Article 6 (c)). However, the above provisions provide the employer with a solid justification of the employer's legitimate interest.

4.4 The Consequences for the Monitoring and the Purpose Limitation Principle

Further, "*the consequences of the monitoring for the employee subjected to it*"[233] in particular whether the results of the monitoring we used "to *achieve the declared aim of the measure*"[234] need to be taken into consideration. The rationale behind this prescription can be traced back to the purpose limitation principle. The employee monitoring should pursue only "*specified, explicit and legitimate purposes"*[235]. In compliance with the principle of transparency the employees need to be provided with precise information about the purposes of the monitoring,

---

[226] Ibid, §6.14, (2) (b)

[227] Ibid, §6.14, (3)

[228] See ECtHR, *Bărbulescu v Romania, §43 and* Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment § 14.3

[229] See Carey, P., & Treacy, B. (2015). *Data protection: a practical guide to UK and EU law*. Oxford: Oxford University Press., p.226

[230] Ibid.

[231] Ibid.

[232] Ibid.

[233] ECtHR, *Bărbulescu v Romania, §121 (v)*

[234] Ibid.

[235] GDPR, Article 5 (1) (b)

in clear and concise form to avoid any ambiguity.[236] Further, if the employer wishes to use the information gathered as part of the monitoring initiatives for a new purpose the new form of processing needs to compatible with what has been already communicated to the employees. When carrying out a compatibility assessment account should be taken of the "*relationship between the purposes for which the personal data have been collected and the purposes of further processing; the context in which the personal data have been collected and the reasonable expectations of the data subjects as to their further use; the nature of the personal data and the impact of the further processing on the data subjects; the safeguards adopted by the controller to ensure fair processing and to prevent any undue impact on the data subjects.*"[237] As a result if the consequences of the monitoring are not reasonably expected by the employees, they would most likely be in breach of the principle of purpose limitation.

Let's examine the following scenario. The company X provides its employees with a privacy notice that as of the following week all internet activities are going to be monitored to ensure malware protection and network integrity. John Smith, one of those employees, listens to music on YouTube regularly during working hours. One month later John Smith is dismissed for violating of the work discipline by utilising the company resources for personal use. In this case the use of Internet activity monitoring for enforcing the labour discipline or enhancing productivity will be in contradiction to the principle of purpose limitation as the consequences of the monitoring go way beyond the declared purpose of the measure.

4.5 Appropriate Safeguards and The Principle of Integrity and Confidentiality

Finally, the ECtHR establishes a requirement for the introduction of "*adequate safeguards, especially when the employer's monitoring operations were of an intrusive nature*"[238]This provision overlaps with several data protection aspects.

First, the General Data Protection Regulation includes data security as a one of the principles relating to processing of personal data. The employer will be obligated to introduce "*appropriate technical or organisational measures*"[239] in order to prevent "*unauthorised or unlawful processing and against accidental loss, destruction or damage*" of personal data.[240]

---

[236] Article 29 Working Party, Opinion 03/2013 on purpose limitation, p. 39

[237] Ibid, p. 40

[238] ECtHR, *Bărbulescu v Romania, §121 (iv)*

[239] GDPR, Article 5 (1) (f)

[240] Ibid.

In the second place, the use Article 7 (f) of the DPD and Article 6 (1) (f) from the GDPR as a lawful ground for the employee monitoring require the balancing the interest of the employer with interests and fundamental rights of employees.[241] As part on the balancing exercise the employer must introduce appropriate safeguards in order to mitigate the risks imposed by such an intrusive measure.[242]

Further, as the employee monitoring falls under the category of high risk processing activities, under Article 35 of the GDPR, a privacy impact assessment will be required, and special measures need to be introduced in order to mitigate those risks[243].

A safeguard of particular importance for employee monitoring is limiting the access to the information gathered through the measure to a need-to-know basis[244].

5 Conclusion

The principles for ensuring respect for private life and correspondence in an employment context defined by the European Court of Human Rights applied in conjunction with the data protection principles of lawful and fair processing, transparency, purpose limitation, necessity, proportionality frame the right to employee privacy by affording it with protection proportionate to the legitimate interests of the employer. The framework for safeguarding employee privacy through data protection is composed of the following key elements:

(i) **Transparency** to define the employees' reasonable expectations to privacy;
(ii) **Proportionality** ensuring that the degree of intrusion into the employee's private life is taken into account and the less intrusive measures are chosen;
(iii) **Legitimacy,** providing that the monitoring will be justified only by the employer's legitimate interests;
(iv) **Purpose limitation,** requiring that the consequences of the monitoring for the employees subjected to always be in line with the pursued goals and with the employee's reasonable expectations; and
(v) **Integrity and Confidentiality** to ensure the introduction of appropriate safeguards guaranteeing the security of the data gather through the monitoring operations.

The ECtHR and this thesis leave the question about the correlation between these principles and their relative weight in the balancing of the employee's rights to privacy and the employer legitimate interests to further academic research and debate.

---

[241] Article 29 Working Party in its *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC.* p.1

[242] Ibid.

[243] See further, Article 29 Working Party Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, p. 9

[244] Article 29 Working Party in its *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC.* p.32

Table of reference

Legislation

European Union

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

Directive 2014/65/EU of the European Parliament and of the council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (MiFID II)

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

The International Labour Office, *Code of Practice on the Protection of Workers' Personal Data (1997)*

United Kingdom

Regulation of Investigatory Powers Act (RIPA)

United States of America

The United States Constitution, The Bill of Rights & All Amendments

List of cases

European Court of Human Rights

Judgment on the merits and just satisfaction, delivered by a Chamber, MARCKX v. BELGIUM, no. 6833/74, ECHR, 1979

Judgment on the merits and just satisfaction, delivered by a Chamber, *Niemietz v Germany*, no. 13710/88, ECHR, 1992

Judgment on the merits and just satisfaction, delivered by a Chamber, *Halford v. The United Kingdom*, no. 20605/92, ECHR, 1997

Judgment on the merits and just satisfaction, delivered by Court (Fourth Section), *Copland vs. the United Kingdom*, no. 62617/00, ECHR, 2007

Judgment on the merits and just satisfaction, delivered by the Court (Fifth Section), Peev v. Bulgaria, no. 64209/01, ECHR, 2007

Decision on admissibility delivered by a Chamber, *Köpke v. Germany*, no.420/07, ECHR, 2010

European Court of Justice

Judgment of the Court of 21 September 1989. Hoechst AG v Commission of the European Communities, Joint Cases 46/87 and 227/88

United States Supreme Court

Katz v. United States, 389 U.S. 347, 360-61 (1967) (Harlan, J., concurring)

Authoritative Guidance

Article 29 Working Party, Opinion 8/2001 on the processing of personal data in the employment context

Article 29 Working Party, working document on the surveillance of electronic communications in the workplace (Adopted May 2002)

Article 29 Working Party in its *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*

Article 29 Working Party, Opinion 03/2013 on purpose limitation

Article 29 Working Party Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679

Article 29 Working Party, Opinion 2/2017 on data processing at work

European Court of Human Rights, *Guide on Article 8 of the Convention – Right to respect for private and family life*

Information Commissioner's Office (UK), *Consultation: GDPR consent guidance*

Information Commissioner's Office (UK), Guide to Data Protection

Information Commissioner's Office (UK), The Employment Practices Code

Information Commissioner's Office (UK), What is personal data? – A quick reference guide

Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment

Scholar Literature

Books

Brems, E., & Gerards, J. H. (2015). Shaping rights in the ECHR: the role of the European Court of Human Rights in determining the scope of human rights. Cambridge: Cambridge University Press

Bogg, A. L., & Novitz, T. (2014). Voices at work: continuity and change in the common law world. Oxford: Oxford University Press

Bygrave, L. A. (2014). *Data privacy law: an international perspective*. Oxford: Oxford University Press

Carey, P., & Treacy, B. (2015). *Data protection: a practical guide to UK and EU law*. Oxford: Oxford University Press

Kuner, C. (2007). European data protection law: Corporate compliance and regulation. Oxford: Oxford University Press, p. 269-270

Morriss, A. P. (2010). *Global labor and employment law for the practicing lawyer: proceedings of the New York University 61st annual Conference on labor*. Austin: Wolters Kluwer

Otto, M. (2016). The right to privacy in employment: a comparative analysis. Oxford, UK: Hart Publishing

Roagna, I.(2012), *Protecting the right to respect for private and family life under the European Convention on Human Rights*, Council of Europe human rights handbooks, p.9

Kilkelly, U.(2003), *The right to respect for private and family life. A guide to the implementation of Article 8 of the European Convention on Human Rights*, Human rights handbooks, No.1

Articles

Aynes, R.L. (1974) *Katz and the Fourth Amendment: A Reasonable Expectation of Privacy or, a Man 's Home Is His Fort*, p. 66

Bygrave, L.A. (1998), *Data Protection Pursuant to the Right to Privacy in Human Rights Treaties,* International Journal of Law and Information Technology, volume 6

Bygrave, L. A. (2001). *The Place of Privacy in Data Protection Law*., (UNSW Press, Volume 2, No 1, 2001)

Chatzinikolaou, A. (2017) *Bărbulescu v Romania and workplace privacy: is the Grand Chamber's judgment a reason to celebrate?*, Strasbourg Observers, available at https://strasbourgobservers.com

Gómez-Arostegui, H. Tomás (2005) "Defining Private Life Under the European Convention on Human Rights by Referring to Reasonable Expectations," California Western International Law Journal: Vol. 35 : No. 2 , Article 2

Plourde-Cole, H. (2010). *Back to Katz: Reasonable Expectation of Privacy in The Facebook Age*, 38 Fordham Urb. L.J. 571

Rolland, S.E., Sirleaf, M., Telesetsky, A., Scimeca, N. & Behles, C. (2007), European Court of Human Rights Expands Privacy Protections: Copland v. United Kingdom, InSights, Volume:11, Issue: 21, available at https://www.asil.orgd

Wayland, K., Armengol, R., Johnson, D.G., *When Transparency Isn't Transparent. Campaign Finance Disclosure and Internet Surveillance* in Fuchs, C., Boersma, K., Albrechtslund, A., & Sandoval, M. (2013). *Internet and Surveillance The Challenges of Web 2.0 and Social Media*. Florence: Taylor and Francis.

Winn, Peter A. (2008), *Katz and the Origins of the 'Reasonable Expectation of Privacy' Test*, McGeorge Law Review, Forthcoming. Available at SSRN: https://ssrn.com/abstract=1291870

Media Articles

Associated Press (2017), *Would YOU let your employer implant an ID chip in your arm?*, retrieved from http://www.dailymail.co.uk

Deutsche Welle (2017), *European court sides with worker in landmark privacy ruling*, retrieved from http://www.dw.com

Gogan, M. (2016), *How do Companies Monitor Employee Internet Usage*, TG Daily, available at http://www.tgdaily.com

Herman, L. *How Much Time Do We Waste at Work? (Hint: It's Scary)*, The Muse, available at https://www.themuse.com

The Local (27 July 2017), *German court rules bosses can't use keyboard-tracking software to spy on workers, Retrieved from* https://www.thelocal.de

Wilhelm, E.-O., (2017), *Bărbulescu ruling: Workplace privacy is alive and kicking*, IAPP Privacy Tracker, retrieved from https://iapp.org

Zhang, E. (2017), How GDPR Will Reshape Your Data Protection Strategy, Digital Guardian, retrieved from https://digitalguardian.com

Other

Bloomberg Finance L.P., A Bloomberg Professional Services Offering, retrieved from

https://data.bloomberglp.com/professional/sites/10/Surveillance-Fact-Sheet-1.pdf

Erns & Young, Considerations for your e-communications surveillance program, p.2

European Court of Human Rights, Factsheet – Surveillance at workplace

European Court of Human Rights, Information Note on the Court's case-law 210

European Data Protection Supervisor, Transparency available at https://edps.europa.eu/data-protection/our-work/subjects/transparency_en

Human Rights Education Project, What is private life?, retrieved from http://www.human-rights.is

Information Commissioner's Office (UK) (2017), Data security incident trends by sector and type 2017/18

International Organization for Standardization, ISO/IEC 27000 family - Information security management systems, available at https://www.iso.org/isoiec-27001-information-security.html