ISSN 2384-9169
Fascicolo n. 3 - 2020
rivista.eurojus.it

Protection of privacy: the right to confidentiality in working relationships

DI ARMANDO IADEVAIA* E MARZIA DE LUCA**

Table of contents: 1. Introduction – 2. The right to privacy: historical evolution and American perspective - 3. Right to privacy and personal data protection in European legislation - 4. GDPR and protection of privacy in working relationship - 5. The balance between privacy and control at workplace - 6. The case of López Ribalda and Others versus Spain - 6.1 The decision of the Grand Chamber of European Court of human Right - 7. Conclusions.

1. Introduction

This article analyzes exiting legal protection for the confidentiality of information collect through telematics systems in workplaces. The contribution of the paper is to approach empirically the reasons that employers give for engaging in monitoring and how employees assess the practice.

There are variety of reasons that an employer might wish to monitor the activities of their staff: on security grounds; health and safety; performance management; protecting organizational resources and interests and compliance with legal requirements. Advances in computer technology have increased the employer's ability to monitor the electronic communications of employees in the workplace[1]. Workers are exposed to many types of privacy-invasive monitoring while earning a living. These include drug testing, closed-circuit video monitoring, Internet monitoring and filtering, E-mail monitoring, instant message monitoring, phone monitoring, location monitoring, personality and psychological testing, and keystroke logging. Employers do have an interest in monitoring in order to address security risks, sexual harassment, and to ensure the acceptable performance of employees.

*Italian lawyer, European planner, he is author of articles and comments in specialized press.
**Graduated in law, she took part, as delegate, in the international project National Model United Nation.
[1] N. J. KING, *Electronic Monitoring to Promote National Security Impacts Workplace Privacy*, in *Employee Responsibilities and Rights Journal*, 2003, p. 127.

However, these activities may diminish employee morale and dignity, and increase worker stress.

Technology has greatly increased employers' ability to monitor employees both at work and outside of work. At the same time, technologies like smart phones and social networking sites have blurred the lines between business and personal, public and private[2].

The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. The role of the law is to strike an appropriate balance between the legitimate interests of employers to protect business assets, against the need to protect the privacy of workers. Employers should be transparent about the nature and content of monitoring, and should have social media, Internet and email policies in place[3].

To understand the real extent and the scope of the right to privacy, in our context, is necessary an historical digression.

2. The right to privacy: historical evolution and American perspective

Privacy has historical roots in philosophical discussions, the most well-known being Aristotele's distinction between two spheres of life: the "public sphere" of the *polis*, associated with political life, and the "private sphere" of the *oikos*, associated with domestic life. However, it will take until the end of XIX century to witness an initial recognition of the concept of privacy as a human right in the United States. Nowadays, this right is counted among the rights of the personality. Personality rights are generally considered to consist of two types of rights:

- the "*Right of Publicity"*, or to keep one's image and likeness from being commercially exploited without permission or contractual compensation, wich is similar (but not identical) to the use of trademark;
- the "*Right to Privacy"*, or the right to be left alone and not have one's personality represented publicly with no permission.

In order to provide a full explanation of the right to privacy's modern concept, it is fundamental to make an excursus, starting from the fundamental rights.

The philosopher and jurist Norberto Bobbio stated that fundamental rights are an historical product, gradually generated by the fight for new freedoms against old powers[4].

According to his theory, human rights dimension is necessarily marked by political, social, economical and technological factors. However, as new rights arise from the society, they do not replace the old ones, but rather it is possible observe an accumulation[5]. This

[2] Employee Rights Law, Legal resource, https://www.hg.org/employee-rights-law.html

[3] G. PHILLIPS, K. SCOTT, *Employment Law*, College of Law Publishing, Legal Practice Guides, London, 2016. See also G. LOCKWOOD, *Workplace Monitoring and Surveillance: The British Context,* Athens Journal of Law, pp. 205-228.

[4] N. BOBBIO, *L'Età dei diritti*, Torino, 1992, XII-XIII.

[5] E. BRUGIOTTI, *La privacy attraverso le "generazioni dei diritti". Dalla tutela della riservatezza alla protezione dei dati personali fino alla tutela del corpo elettronico*, in *Dirittifondamentali.it*, 2, 2013, 1; R. KREIDE, *Politica globale e diritti umani, Potenza e impotenza di uno strumento politico*, Torino, 2010, 38; N. BOBBIO, *op. cit*., XVI.

dynamic allowed scholars to recognize different generations of fundamental rights[6]. The first generation consisted in civil and political rights, which emerged during the liberal revolution imposing significant restrictions on the State, consequently been called "*negative*" freedoms[7].

Subsequently, in XIX and XX centuries, a second generation arose from the working class struggled for social justice. Scholars refer to this new set of freedoms as "*positive*" and they refer to basic rights as healthcare, education, and the right to vote[8].

Finally, the social and scientific revolution led Constitutionalism to recognize two more generations of rights[9], related to bioethics and digital technologies. Afterwards, legal systems reacted by adopting new Charters (as the European Charter of Fundamental Rights also called Treaty of Nice) affirming both new rights and an extensive re-interpretation of previous ones. The technological revolution has certainly accelerated the transition to a global (digital) society; but when did start what we can define "the race" to privacy? Scholars commonly agree that privacy made its first appearance between the XVIII and XIX centuries, a period known as the private law golden age[10]. Due to the rapid urbanization, the diffusion of portable cameras and the changing newspapers-reading habits (yellow journalism), the western society was definitely more sensitive to the need of preserving its intimacy[11]. Soon arose the necessity to ask for the recognition of a new, yet undefined, right to protect one's private life. Despite having faced the same social issues, the Common lawyers related the new-born right to privacy to the fundamental right of Liberty and the Civil lawyers to the fundamental right of Dignity[12]. This divide continues nowadays as both sides of the Atlantic seems far from finding a common ground. However, not only the public

---

[6] A. SPADARO, *Dai diritti individuali ai doveri collettivi. La giustizia distributiva nell'età della globalizzazione*, Soveria Mannelli, p. 28 ff.; R. BIN G. PITRUZZELLA, *Diritto costituzionale*, Torino, 2015; A. BARBERA, C. FUSARO, *Corso di diritto costituzionale*, Bologna, 2016; C. TOMUSCHAFT, *Human Rights: Between idealism and Realism*, Oxford, 2008, p. 25 ff.; L. MEZZETTI, *Manuale breve. Diritto costituzionale*, Milano, 2013, p. 501 ff.

[7] R. R. PALMER, *The Age of Democratic Revolutions*, Princeton, 1959; G. GUSFORD, *Les révolutions de France et Amérique*, Paris, 1988; G. BOGNETTI, *Lo spirito del costituzionalismo americano*, Torino 1998; B. BAYLIN, *The Ideological Origins of the American Revolution*, Cambridge (U.S.), 1967.

[8] E. DENNINGER, *Stato di prevenzione e diritti dell'uomo*, in *Nomos*, 1996, p. 47 ff. G. MORBIDELLI, *La Costituzione*, in G. MORBIDELLI, L. PEGORARO, A. REPOSO, M. VOLPI (eds.), *Diritto pubblico comparato*, Torino, 2007, p. 42 ff.

[9] K. VASAK, *Pour une troisième génération des droits de l'homme*, in C. SWINARSKI (ed.), *Etudes et essais sur le droit international humanitaire et sur les principes de la Croix-Rouge en l'honneur de Jean Pictet*, The Hague, 1984; S.M. HELMONS, *La quatrième génération des droits de l'homme*, in M. VERDUSSEN (ed.), *Les droits de l'homme au seuil du troisième millénaire: mélanges en hommage à Pierre Lambert*, Brussels, 2000; A. ALESSANDRI, *Commento al draft di Protocollo sulla ricerca biomedica*, in *I diritti dell'uomo - cronache e battaglie*, 2003; *contra* P. DE STEFANI *I diritti umani di terza generazione*, in *Aggiornamenti sociali*, 2009. The Author Consider the fourth generation of rights a simple development of the previous ones.

[10] M. PERROT, *Modi di* abitare, in P. ARIES, G. DUBY (eds.), *La vita privata*, Roma-Bari, 2001, p. 10; L.M AUSTIN, D. KLIMCHUCK (eds.), *Private Law and the Rule of Law*, Oxford, 2014; W. LUCY, *The Rule of Law as the Rule of Private Law,* in *Private Law and the Rule of Law,* Oxford, 2014, 46 ff.; K.S. ZIEGLER, *Human Rights and Private Law: Privacy as Autonomy*, London, 2007.

[11] In particular, the mass-urbanization enabled the still local media to reach more users, hence compromising someone's reputation became increasingly easier. L. MIGLIETTI, *Profili storico-comparativi del diritto alla privacy*, in *DirittiComparati.it*, 4 December 2014; N. BOBBIO, *Liberalismo e democrazia*, Milano, 2011, 3 ff.; P. MALVESTITI, *Lo Stato e l'economia*, Roma, 1955, p. 21 ff.

[12] This situation is summarized by JAMES WHITMAN, *The Two Western Cultures of Privacy: Dignity v. Liberty*, in *Yale Law Journal*, 2004, p. 1151-1221; see also J.L. HALPERIN, *L'essor de la "*privacy*" et l'usage des concepts juridiques*, in *Droit et Société*, 2005, p. 765 ff.

opinion, but scholars believe that privacy, regardless of its name (privacy, vie privée, riservatezza, intimidad) still shares the same purpose. Many academics assumed this being the consequence of American privacy legal transplant all around the world[13]. A large number of scholars consider the famous 1890 article "*Right to Privacy*" , written by the Bostonian lawyers Samuel Warren and Louis Brandeis[14] on the *Harvard Law Review*, the milestone of modern privacy and it represents the first legal paper recognizing privacy protection as a separate right.

Neverthless, their work was the brilliant synthesis and development of both the English and French experiences, unfortunately often neglected. However, at the time of its publishing the "*Right to Privacy*" found a society still unprepared to dismiss completely any association with other rights as honour, reputation and, first of all, property[15].

As soon as new business practices started threatening the person in unexpected ways, the society strongly felt the necessity to secure what Judge Cooley defined as the right " *to be let alone*"[16]. Indeed, the Bostonian lawyers's aim was to explore right to privacy's roots and to focus on the existing common law torts inadequacy, rather than providing a comprehensive conception of it[17]. As a consequence, even though the "*right to be let alone*" was mentioned in several decisions, it was considered a vague concept.

As a matter of fact, privacy has a cross-cutting nature, considered as set of different ideas, rather than a unitary right[18]. Ruth Gavison, in an attempt to address the right of privacy to " limited access", defined "three irreducible elements: secrecy,anonimity,and solitude"[19]. Though, this definition could be too limited. Another theory argues that privacy consists of two elements: the interest in being left alone, on one hand, and the interest in concealing

---

[13] J.J. HALPERIN, *L'essor de la "*privacy*" et l'usage des concepts juridiques*, cit., p. 765-782. For an analysis in depth of the legal transplant process see A. WATSON, *Legal Transplants: An Approach to Comparative Law*, Athens (U.S.), 1974.

[14] S. D. WARREN, L.D. BRANDEIS, *The Right to Privacy*, in *Harvard Law Review*, 1890, p. 193 ff.

[15] A. WESTIN, *Privacy and Freedom*, New York, 1967, 337; A. BALDASSARRE, *op. cit.*, p. 1.

[16] T. M. COOLEY, *A Treatise on the Law of Torts, or the Wrongs which arise Independent of Contract*, Chicago, 1888, p. 29. Around the same time that Warren and Brandeis published their article, the Supreme Court referred to the right to be let alone in holding that a court could not require a plaintiff in a civil case to submit to a surgical examination: «As well said by Judge Cooley: 'The right to one's person may be said to be a right of complete immunity; to be let alone», in *Union Pac. Ry. Co. v. Botsford*, 141 U.S. 250 (1891). However, it must be noted that Cooley's right to be let alone was, in fact, a way of explaining that attempted physical touching was a tort injury; he was not defining a right to privacy see R.E. SMITH, *Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet*, Providence, 2004, 128.

[17] E. J. BLOUSTEIN, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, in *New York University Law Review*, 1964, p. 970 ff.

[18] Judith Thomson, claims that the right to privacy is not a distinct right, but it is «overlapped by other rights» J.J. THOMSON, *The Right to Privacy*, in F. SHOEMAN (ed.) *Philosophical Dimension of Privacy: an Anthology*, Cambridge, 1984, p. 284, whilst Jerry Kang defines privacy as the union of three overlapping clusters of ideas: physical space «the extent to which an individual's territorial solitude is shielded from invasión by unwanted objects or signals»; choice «an individual's ability to make certain significant decisions without interference»; flow of personal information «an individual's control over the processing-i.e., the acquisition, disclosure, and use-of personal information»; J. KANG, *Information Privacy in Cyberspace Transactions*, in *Stanford Law Review*, 1998, pp. 1202-03.

[19] «Our interest in privacy is related to our concern over our accessibility to others: the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others' attention. privacy as limited access to the self is valuable in furthering liberty, autonomy, and freedom»: see R. GAVISON, *Privacy and the Limits of Law*, in *Yale Law Journal*, 1980, p. 423.

information, rather than limiting its access, on the other hand[20]. The idea of concealment has clearly inspired American Information privacy, a fundamental right set in law-case by the Supreme Court of the United States and carved directly from the fourth Amendment[21].

Alan Westin stated "Privacy is the claim of indviduals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others"[22].

Richard Murphy tried to elaborate a neutral approach to privacy, considering protection worthy with respect to "any data about an individual that is identifiable to that individual"[23], which is very similar to the "personal data" definition made by Directive 95/46/EC regulating European data flows.

In *Roe v. Wade* the Supreme Court defined privacy as an "interest in independence in making certain kinds of important decisions"[24]. Yet, it was 1948 when the Universal Declaration of Human Rights (UDHR) mentioned privacy and private life at *Article 12*[25]. Subsequently, the UDHR inspired both *Article17* of International Covenant on Civil and Political Rights and *Article 8* of the 1950 European Court of Human Rights (ECHR) .

Only later, during the second half of XX century, right to privacy rooted in European Courts and the concept of privacy adopted was mirroring the American "*right to be let alone*". However, its constitutional foundation will be set not, as the US Fourth Amendment, in the value of freedom from the State, but in human dignity and self-determination[26].

3. Right to privacy and personal data protection in European legislation

Nowadays recognized as fundamental human right, it was only in the second half of XX century that the right to privacy began to take hold in the EU legislation. The first references to the right to privacy can be found in the 1950 *European Convention on Human Rights*[27], which stated that there can be no interferences by a public authority in the exercise of the right to one's own individual freedom, with the exception of legal interference such as necessary measures for national security, for public safety, for the defence of order and for the prevention

---

[20] R. A. POSNER, *The Economics of Justice*, Harvard University Press, Harvard, 1981, 272-273.

[21] *Whalen v. Roe,* 429 U.S. 599-600 (1977), see also *Griswold v. Connecticut,* 381 U.S. 479 (1965) and *Roe v. Wade,* 410 U.S. 113 (1973).

[22] A. WESTIN, *Privacy and Freedom*, New York, 1967, p. 7; see R. P. BENZANSON, *The Right to Privacy Revisited: Privacy, News, and Social Change*, in *California Law Review*, 1992, p. 1133, at p. 1135 («I will advance a concept of privacy based on the individual's control of information»); O. M. RUEBHAUSEN, O.G. BRIM, *Privacy and Behavioral Research*, in *Columbia Law Review*, 1965, p. 1184, at p. 1189 («The essence of privacy is no more, and certainly no less, than the freedom of the individual to pick and choose for himself the time and circumstances under which, and most importantly, the extent to which, his attitudes, beliefs, behavior and opinions are to be shared with or withheld from others»); see A. WELLS BRANSCOMB, *Who Owns Information? From Privacy Public Access*, New York, 1994; C. FRIED, *Privacy*, in *Yale Law Journal*, 1968, pp. 483 ff.

[23] R. S. MURPHY, *Property Rights in Personal Information. An Economic Defense of Privacy*, in *Georgia Law Journal*, 1996, p. 2381, at p. 2383.

[24] *Whalen v. Roe*, 429 U.S. 589 (1977) at 599-600.

[25] «No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks». The article has been written by a French and American joint committee led by R. CASSIN, J. HUMPHREY, J. L. HALPERIN, *Protection de la vie privée et privacy: deux traditions juridiques différentes?*, cit., pp. 59 ff.

[26] F. PETRUCCO , *The right to privacy and new technologies: between evolution and decay,* in *Media Laws*, 1/2019, p. 162.

[27] European Convention on Human Rights, Rome, 4.XI.1950

of crimes, for the protection of health or morality, or for the protection of rights and freedoms of others.

This primary concept has been brought back and expanded in subsequent other international agreements, such as the *Schengen Agreement*, and in the *Charter of Fundamental Rights of the European Union,* which *Article 8* takes inspiration from the 1948 *Universal Declaration of Human Rights ,* but looking further into the aspect of the protection of personal data. However, in Europe, unlike the United States, there has been a history of totalitarian states, which have acted as 'super-controllers' towards citizens: for this reason, a different sensitivity to privacy has developed in Europe from a historical point of view. The European experience of XX century consisted of a control of information about citizens, operated by the states. Therefore, it is correct to say that, today, to the traditional notion of confidentiality (right to privacy) is added the more modern notion of personal data protection. Emblematic is the case of *Stasi,* the State security Ministry, East Germany's main security and espionage organization, lasted until 1990: the purpose was to monitor the politically incorrect behaviour of all East German citizens. Once the person was identified, the aim was to force the same one to abandon his social, work or academic position; subsequently the victim was integrated as an informant. In 1989, it was estimated that the *Stasi* had 91,000 full-time employees and probably more than 100,000 informants, with the highest percentage of spies per capita of all Warsaw Pact states: one spy for every 59 inhabitants. After the fall of the Berlin Wall in 1989, the Stasi offices were invaded by citizens, not before a large amount of compromising material was destroyed by Secret Service officers. The remaining documents are now available to all people who were spied on. Today many things have changed and, especially in the field of personal data protection, Germany can be considered the cradle of European data protection. Since the 1970s, Germany has had extensive rules on privacy and the processing of personal data. However, it was not until 1990 and BDSG in 2001 that, with the implementation of Directive 95/46/EC[28], amended in July 2009, the need for consent in the processing of "free data" (name,last name, address and telephone number)[29] was expressly excluded. How was the impact of recognition of the right to privacy in the legislation of other European countries? In light of the fact that private law is always been the backbone of English legal and political life, it is clear that Common lawyers associated privacy with property, by defining it as *ius excludendi alios*[30].

Nevertheless, English society started a long process of property *"dematerialization"*, by adopting a copyright regulation meant to protect property from behaviors unrelated to its material retention[31]. Therefore, arose the necessity to regulate property's new *"inner dimension"* (the unborn privacy)[32], and the English Courts started affording protection to

[28] 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.
[29] E. ROSSI, *Il diritto alla privacy nel quadro giuridico europeo ed internazionale delle recenti vicende sulla sorveglianza di massa, il diritto comunitario e degli scambi internazionali*, 2014.
[30] Notably, property framed both the relationships among privates and the political affiliation, at least prior to the appearance of political parties, see A. BALDASSARRE, *Privacy e Costituzione. L'esperienza statunitense*, Roma, 1974, p..48.
[31] The very first copy regulation has been the 1710 *Statue of Anne*, later replaced by the 1988 Copyright, Design and Patents Act.
[32] A. BALDASSARRE, *op. cit.*

thoughts, sentiments and emotions, as long as they were expressed through arts or writings, by preventing their publication. For this reason, clearly, the copyright started being insufficient; the dissociation between the concepts of property and privacy was the necessary precondition for the resulting configuration of an autonomous individual right.

In the long run private law has proved not to protect fundamental rights sufficiently because of its arbitrary nature. The public law intervention became, therefore, necessary and it is partially responsible for the private law shift from property right to personal right[33]. Nowadays, it is not possible talk about privacy without referring to the processing of personal data; the United Kingdom has had its own data protection legislation since 1984. Since 1st March 2000, the protection of personal data in United Kingdom has been governed by the *Data Protection Act* 1998, implementation of Directive 95/46/EC. It is worth to remember that UK adopted the *opt-out system* mechanism. Thus, the relevant legislation only requires that those people concerned should be informed that personal data may be used for commercial purposes. On the other hand, there is no duty of the controller to inform people of their right to request the deletion of data from the archives.

The French cultural tradition followed a path similar to the English one, by alternating different privacy designs and mixing what Robert Post described as the "three Common law concepts of reputation", namely: *property, honour and dignity*. It is important to notice that while Warren and Brandeis were praising the protection accorded to privacy by French legislation, on the other side of the Ocean Laboulaye was criticizing it and condemning the American freedom of expression[34]. However, the legislator did not define the exact content of the "private life" concept. Only in 1874 the *Court de cassation*, tried to define private life content with a decree (*arrêt)*[35]. The decree extended the concept of private life outside the domestic walls. This change paved the way to a new *privacy* concept evolution during the sixties and seventies of XX century, in order to protect also celebrities private life, in line with the American example. With the regard to personal data processing, in France, on 6 January 1978, was approved the *Loi informatique et libertés* and an independent authority has been set up to ensure the effectiveness: the *Commission Nationale de l'informatique et des Libertés (CNIL).* However, France was the last country to implement Directive 95/46/EC, on 6 August 2004, amended the previous law of 6 January 1978.

Rich is the Spanish legal tradition that unites the three figures of *Article 18.1, Spanish Constitution* (The right to honour, personal and family intimacy and to one's own image is guaranteed; the domicile is inviolable; no entry or registration may be made in it without the consent of the holder or judicial decision, except in case of flagrant crime) in a *derecho general de la intimidad.* Other authors, on the other hand, believe that *Article 18* expresses a single legal good, *la intimidad*, protected by the different rights listed. In order to determine the extent of a *derecho a la intimidad* it is decisive the bond between *paragraph I and IV Article18,* related to " cyber freedom". In Spain since 14 January 2000, are in force the *Ley Orgánica no 15 de Protecciòn de Datos de Carácter Personal* (LOPD) of 13 December 1999, wich has also been implemented in Spain to the Directive 95/46EC, and Regulation

[33] F. PETRUCCO *The right to privacy and new technologies: between evolution and decay,*, *op. cit*., p. 155.
[34] R. LEFEBVRE (pseudonyme de Laboulaye), *Paris en Amérique*, Paris, 1887, 136.
[35] J. L. HALPERIN, *Protection de la vie privée et privacy: deux traditions juridiques différentes ?,* in *Les nouveaux cahiers du Conseil constitutionnel*, 2015; Id., *Diffamation, vie publique et vie privée en France de 1789 a 1944*.

n.994/1999 on minimum security measures. The legislature, subsequently, adopted additional measures: *Ley de Servicios de la Sociedad de Información y de Comercio Electronico* (LSSI) and *Ley General de Telecomunicaciones* (LGT), *Real Decreto* (RD) n. 424/2005[36], regulating traffic data and location data.

With regard to the *Italian Constitution*, there is no specific article that protects the right to privacy, but this can be obtained by interpretation from *Articles 2 and 3* that allow confidentiality to be incorporated into human rights. But also from *Articles 13, 14 and 15*, in wich privacy protection can be perceived in areas concerning personal freedom, domicile, freedom and secrecy of correspondence and all forms of communication. The first source of law was the case law of the *Supreme Court of Cassation*. This, with the judgment n. 4487 of 1956, initially denied the presence of a right to privacy. The reference to *Article 2 Constitution* did not arrive until 1975, with the judgment of *the Court of Cassation n. 2129* of 27 May 1975, by which the Court identified that right in the protection of those, strictly personal, family situations and events. The Court itself stated that even if those situations have occurred outside the home, they do not have a socially appreciable interest for third parties. This statement is fundamental to balance the right to report. The dividing line between the right to privacy and the right to third party information, therefore , seemed to be the popularity of the individual. Anyway, even very popular individuals retain that right, limited to facts that have nothing to do with the reasons for their own popularity. The already mentioned Law 675/1996[37], later replaced by D.Lgs n. 196/2003[38], played a key role in the processing and protection of personal data. Since 1st January 2004, *D. Lgs 196/2003* has also focused on important issues such as how confidential data should be processed in the context of publicly accessible electronic communications services and the obligation, by providers, to make the user more aware of how their confidential information will be processed and used. The EU Directives 95/46/EC and 97/66/EC were applied to the data processing on the internet. According to *95/46 EC*, the data processing is legitimate if it is permitted by the individual and he/she must be aware of it.

Applying these coordinates in workplaces, European employers are bound by comprehensive data protection acts that limit and regulate the collection of personal information on workers. These laws specifically call for purpose and collection limitations, accuracy of data, limits on retention of data, security, and protections against the transfer of data to countries with weaker protections. These protections place employees on a more equal footing while allowing employers to monitor for legitimate reasons.

4. GDPR and protection of privacy in working relationship

[36] Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, «BOE» núm. 102, de 29/04/2005.

[37] Legge n. 675 del 31 dicembre 1996 - Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali, testo consolidato con il d.lgs. 28 dicembre 2001, n. 467, pubblicata sulla Gazzetta Ufficiale n. 5 dell´8 gennaio 1997 - Supplemento Ordinario n. 3. Legge abrogata ai sensi dell´articolo 183, comma 1, lettera a), del Codice in materia dei dati personali.

[38] Decreto legislativo 30 giugno 2003, n.196 recante il "Codice in materia di protezione dei dati personali" in S.O n. 123 alla G.U. 29 luglio 2003, n. 174

The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. The development and application of the concept of privacy in European law encompasses three clusters of ideas. First, privacy embodies autonomy interests; it protects decisions about the exercise of fundamental constitutional liberties with respect to private behavior, such as decisions relating to marriage, procreation, contraception, family relationships, and child - rearing. Second, privacy protects against surveillance or intrusion when an individual has a "*reasonable expectation of privacy*" or right to confidentiality. Third, privacy encompasses informational interests; this notion is most frequently expressed as the interest of an individual in controlling the dissemination and use of information that relates to himself or herself or to have information about oneself be inaccessible to others.

The concept of *confidentiality* has suffered a significant evolution. Today, its protection no longer provides only for the prohibition of disclosing information concerning the privacy of the individual, but it also requires all those who carry out "treatment" operations on other people's personal data to take appropriate precautions, in order to minimize any damage to the data holders. In this, above all, there is the difference between the traditional notion of *"confidentiality/privacy"* and the more modern notion of *"personal data protection"*. Therefore, it must be stated that data processing is subject to three basic rules:

1. necessary consent of the person, who must be expressed in a free and conscious way;
2. indication, by the holder, of the purpose for which the data is collected;
3. obligation of the same holder to comply with all legal provisions on data collection and management.

Following the recognition of privacy as a fundamental human right in the *UN Declaration of Human Rights* and in other European and international treaties, privacy issues first appeared in some European countries in the 1970s. During these years, several countries started to process their citizens' data on a massive scale, which led to the first privacy laws. In the 1980s private companies started gathering data about their customers. For this reason a common protection system was implemented across Europe, followed by the EU Data Protection Directive in the 1990s (*Directive 95/46/EC*).

Every European country had to adapt this set of rules to their national regulations. But, as technology transformed society in the last twenty years, a review of the existing legislation on personal data processing was also required. In 2016, the EU adopted the *General Data Protection Regulation*, GDPR (*no 2016/679*), which replaces the 1995 Data Protection Directive, and came into force since 25 May 2018. Considered a milestone in the regulation of personal data protection in EU, the *Article 1 Sec. 2* of the GDPR states: "This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data". Additionally, it defined the legal meaning of "personal data", "processing of personal data", "personal data filing system", "controller", "processor", "third party", "recipient", and "the data subject's consent", which are now used worldwide[39]. The GDPR provides a high level of data protection and is directly applicable in all EU member states and in working relationship too. Despite the European common ground, each country

[39] Art. 2, Directive 95/46/EC.

still has its own different law system. Compliance rules differ depending on the local culture, for example there are huge differences between UK and Greece or Italy. Every form has, of course, to be filled in using the local languages. These rules will also apply to data processing as part of the work report. Companies (outside the EU) may also be subject to the GDPR if the establishment of a company is collecting personal data of an EU Member State or is addressing the EU market, even if this establishment is located outside the EU. Furthermore, the GDPR has established the concept of a Data Protection Officer (DPO) in Europe, ex art. 37 GDPR.

The GDPR introduces a duty for you to appoint a data protection officer (DPO) if you are a public authority or body, or if you carry out certain types of processing activities.

The European DPO gets his rights from law. DPOs assist you to monitor internal compliance, inform and advise on your data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority. The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level. A DPO can be an existing employee or externally appointed. In some cases several organisations can appoint a single DPO between them. DPOs can help you demonstrate compliance and are part of the enhanced focus on accountability[40].

However, before the GDPR came into force, the *WP29-Working Party 29* (a joint working group of the National Data Protection and Surveillance Authority), had issued guidelines to define the figure of the DPO. Since 25 May 2018 the WP29 has ceased its work and has been replaced by the *European Data Protection Board (EDPB).* The Board will not only issue guidelines on the interpretation of core concepts of the GDPR but also be called to rule by binding decisions on disputes regarding cross-border processing. According to *Chapter 6 of the GDPR*, each EU member state shall provide for one or more independent public authorities to be responsible for monitoring the application of the GDPR. Those data protection authorities (DPAs) supervise, through investigative and corrective powers, the application of the data protection law. Infringements of the GDPR may lead to fines up to 20 Million € or 4% of the total worldwide annual turnover of a company. The basic principles are also applied directly to treatments in the context of the working relationship.

In particular, employers must, under *art. 5 GDPR*: have legitimate requirements for personal information about their employees. They need to know who they're hiring. They need to address performance issues and ensure the physical security of their workplace. They may see electronic monitoring and other surveillance as necessary to ensure productivity, stop leaks of confidential information, and prevent workplace harassment. So sometimes employers have to delve into private matters. But they can keep those instances to a minimum, and limit the impact on personal privacy. The possibility that an individual employee might do something harmful doesn't justify treating all employees as suspects.

Please note that the processing of personal data in the workplace, after the GDPR came into force, is considered to be carried out by both private and public employers, unlike the broadening of the Privacy Code prior to the changes of the *D.lgs. 101/2018*. The treatment of personal data in employment relationships must be, like any other treatment, lawful and

[40] Information Commissioner's office. https://ico.org.uk/

therefore based on one of the legal basis of the treatment referred to in *Article 6, paragraph 1* GDPR, that impose the personal consent.

The *consent* is defined as any manifestation of free, specific and informed will with which the person agrees that the personal data concerning him is the subject of treatment. For consent to be valid, it must also be revoked. The purpose pursued by the employer must be legitimate. The chosen method or the specific technology with which the treatment will be carried out must be necessary, the treatment must be proportionate to the business needs and must be carried out in the least intrusive way possible. Therefore, it is essential that there are specific mitigation measures to ensure an adequate balance between the legitimate interest of the employer and the fundamental rights and freedoms of workers. These measures should include restrictions on monitoring to ensure that the worker's private life is not violated. These restrictions could be:

- geographical (e.g. monitoring only in specific places; monitoring should be prohibited from monitoring sensitive areas such as religious places and, for example, health and local areas for breaks);
- data-oriented files (e.g. personal communications and electronic files should not be monitored);
- defined in time terms (e.g. sample monitoring, rather than continuous monitoring).

The *treatment of particular categories of data* is governed by *Article 9, paragraph 1* GDPR, which provides a blanket ban on their treatment, excluding the cases mentioned in paragraph 2. National legislation (rule of law or collective agreement) can:

-authorize (under *Article 9.2.b*) GDPR treatment for fulfillment of obligations and the exercise of specific rights of the controller or person concerned in relation to labour law and social security and social protection;

The national legislature has therefore introduced special measures to be respected, added by *Article 2-septies* of the Privacy Code, newed by D.lgs. 101/2018. The treatment of genetic, biometric and health-related data must therefore be carried out in the presence of one of the conditions provided by Article 9 paragraph 2. The processing of particular categories of data in employment reports is carried out only to pursue specific purposes, established by the law

In addition to defining cases of legitimate treatment, the Guarantor has specific indications for the treatments carried out both before taking it, and in constancy of employment. Finally, the Guarantor prescribes specific methods of processing communications and documents containing particular categories of data:

-data collection must normally take place with the person concerned;

-the means used for communications containing particular categories of data must be used individually directly to the person concerned or to a delegate. In the case of paper communication, this must take place in closed;

- documents intended to circulate within the organization must contain only the information needed by the department or function recipients of the document; Measures must also be taken to ensure that the document is received only by the relevant offices and only authorized staff;
- absence notices and notices within the organization should not contain reasons from which you may become aware of the absent person's personal data.

At this point, a proper reference must be made to the *"right to be forgotten"*, found in *Article 17* GDPR. The right to be forgotten, made popular by Victor Mayer-Schönenberg's book "Delete", is the idea according to which an information should be delate, rather than persist eternally in some database[41]. In fact, internet has undermined the monopoly on information and with the up taking of digital economy, users, while longing for more privacy, feel the urge to share personal content and store data on the web, with the appropriate risks[42]. Therefore, should users be able to decide, whether or not, to permanently delate their data on the Internet? According to the European institution, yes, thus resulting in the inclusion of the right to be forgotten within the concept of privacy[43].

5. The balance between privacy and control at workplace

As previously anticipated, nowadays information and communication technologies (hereinafter ICT) acquired a significant role in workplace, with growing use of computers in all aspects of operations and increasing communication and dissemination of information through the internet.

ICT techniques are mainly used in the digital domain, typically grouped together under the term "surveillance capitalism"[44].

Information technology is used for all kinds of surveillance tasks. It can be used to augment and extend traditional surveillance systems such as CCTV and other camera systems, for example to identify specific individuals in crowds, using face recognition techniques, or to monitor specific places for unwanted behaviour. Such approaches become even more powerful when combined with other techniques, such as monitoring of Internet-of-Things devices[45]. Social media and other online systems are used to gather large amounts of data about individuals – either "voluntary", because users subscribe to a specific service such as Google, Facebook, Instagram or involuntary by gathering all kinds of user related data in a less transparent manner. Data analysis and machine learning techniques are then used to generate prediction models of individual users that can be used, for example, for targeted advertisement, but also for more malicious intents such as fraud or micro-targeting to influence elections[46] or referenda such as Brexit[47]. In addition to the private sector surveillance industry, governments form another traditional group that uses surveillance techniques at a large scale, either by intelligence services or law enforcement. These types of surveillance systems are typically justified with an appeal to the "greater good" and protecting

[41] N. L. RICHARDS, *ibid.*, 1511 and 1531.
[42] A. CAVOUKIAN, *7 Foundational Principles of Privacy by Design,* Office of the Information & Privacy Commissioner of Ontario, 2010.
[43] R. RAZZANTE, *I tanti dubbi sul diritto all'oblio*, in *AgendaDigitale.eu*, 7 November 2014; N. L. RICHARDS, *Why Data Privacy is (Mostly) Constitutional*, cit., 1531 ff.
[44] S. ZUBOFF, 2019, *The age of surveillance capitalism: the fight for the future at the new frontier of power*, London, Profile Books.
[45] N. H. MOTLAGH, M. BAGA, M. T. TALEB, *UAV-based Io T platform: A crowd surveillance use case*, in *IEEE Communications Magazine*, 2017, pp. 128–134.
[46] H. ABELSON, R. ANDERSON, S. M. BELLOVIN, J. BENALOH, M. BLAZE, W. DIFFIE, R. L. RIVEST, *Keys under doormats: mandating insecurity by requiring government access to all data and communications*, in *Journal of Cybersecurity*, 2015, pp. 69–79.
[47] C. CADWALLADR, E. GRAHAM-HARRISON, *The Cambridge analytica files*, The Guardian, 2018, pp. 6–7.

citizens, but their use is also controversial. For such systems, one would typically like to ensure that any negative effects on privacy are proportional to the benefits achieved by the technology. Especially since these systems are typically shrouded in secrecy, it is difficult for outsiders to see if such systems are used proportionally, or indeed useful for their tasks[48]. This is particularly pressing when governments use private sector data or services for surveillance purposes

The debates about privacy at workplace are revolving around new technology such us drones, wearable sensors and sensor networks, social media, smart phones, closed circuit television, to government cyber - security programs, surveillance, RFID tags, big data, head-mounted displays and search engines. The impact of some of these new technologies is worrisome.

We must outline how modern technologies may impact privacy, as well as how they contribute to mitigating undesirable effects. However, there are new and emerging technologies that may have an more profound impact in our life, for example "*brain-computer interfaces*". In this case computers are directly connected to the brain. In this way, not only behavioral characteristics are subject to privacy considerations, but even one's thoughts run the risk of becoming public, with decisions of others being based upon them. When brain processes could be influenced from the outside, autonomy would be a value to reconsider to ensure adequate protection.

Apart from evaluating ITC against current moral norms, we need to consider the possibility that technological changes influence the meaning of norms themselves [49]. Technology thus does not only influence privacy by changing the accessibility of information, but also by changing the privacy norms themselves. For example, social networking sites invite users to share more information than they otherwise might. The "*oversharing*" becomes accepted practice within certain groups. With future and emerging technologies, such influences can also be expected and therefore they ought to be taken into account when trying to mitigate effects[50].

Fundamental question is to found a way by which is feasible to protect privacy and try to hide information from parties who may use it in undesirable ways. Gutwirth & De Hert[51] argue that it may be more feasible to protect privacy by transparency – by requiring actors to justify decisions made about individuals, thus insisting that decisions are not based on illegitimate information. This approach comes with its own problems, as it might be hard to prove that the wrong information was used for a decision. Then, it may well happen that citizens, in turn, start data collection on those who gather data about them, governments. Such "*counter(sur)veillance*" may be used to collect information about the use of information,

[48] K. J. LAWNER, *Post-September 11th International Surveillance Activity – A Failure of Intelligence: The Echelon Interception System & (and) the Fundamental Right to Privacy in Europe*", Pace International Law Review, 2012, pp. 435–480.
[49] M. BOENINK, T. SWIERSTRA, D. STEMERDING, *Anticipating the interaction between technology and morality: a scenario study of experimenting with humans in bionanotechnology*, in *Studies in Ethics, Law, and Technology*, 2010.
[50] See also G. DANEZIS, S. GÜRSES, *A critical review of 10 years of Privacy Technology,* Department of Electrical Engineering, KU Leuven, 12 August 2010.
[51] S. GUTWIRTH, P. DE HERT, *Regulating profiling in a democratic constitutional state*", in *Hildebrandt and Gutwirth*, 2008, pp. 271–302.

thereby improving accountability[52]. The open source movement may also contribute to transparency of data processing. In this context, transparency can be seen as a pro-ethical condition contributing to privacy[53].

It has been argued that *the precautionary principle*, well known in environmental ethics, might have a role in dealing with emerging information technologies as well[54]. The principle would see to it that the burden of proof for absence of irreversible effects of information technology on society, would lie with those advocating the new technology.

Consequently, precaution can be used to impose restrictions at a regulatory level, in combination with or as an alternative to empowering users, contributing to the prevention of informational overload on the user side. It is appropriate to note that not all social effects of information technology concern privacy[55]. Examples include the effects of social network sites on friendship, and the verifiability of results of electronic elections. Therefore, sensitive approaches and impact assessments of information technology should not focus on privacy only, since information technology affects many other values as well, such as the right to work.

In particular, some employers use hidden cameras or other instrument of surveillance at the workplace to monitor the productivity and behavior of their employees, as well as identifying any signs of potential theft. However, these cameras may generate privacy implications and infringe on the rights of employees. European employment laws are generally silent on this issue, so the rights in this area depend on the laws of national State. Some countries have enacted very specific laws addressing surveillance in the workplace, such as California's ban on installing a surveillance mirror in a restroom, shower, or locker room at work. In Connecticut, employers may not operate surveillance equipment in areas designed for employee rest or comfort -- such as restrooms, locker rooms, or employee lounges.

Other states specifically prevent employers from installing cameras in employee lounges and union meetings, such as in many european states.

It is becoming easier to monitor employees as surveillance technology is becoming more affordable. Enterprises have an incentive in monitoring employees as it is more efficient to stop employees from surfing the internet or completing personal chores during work hours. Whether an employer needs to disclose their monitoring activities depends on where they are situated, where they do business, and in what area of business they operate; there are different regulations for different states, localities, countries, areas of business and the like.

In Europe, the GDPR requires that an employer not only disclose that they are monitoring their employees but also in what manner and for what purposes. The GDPR requires that an employee is given a considerable amount of information about their employer's monitoring practices and to what extent those practices are used.

---

[52] S. GÜRSES, A. KUNDNANI, J. VAN HOBOKEN, *Crypto and empire: the contradictions of counter-surveillance advocacy*", Media, Culture & Society, 2016, pp. 576–590.
[53] M. TURILLI, L. FLORIDI, *The ethics of information transparency*, in *Ethics and Information Technology*, 2009, pp. 105–112.
[54] W. PIETERS, A. VAN CLEEFF, *The precautionary principle in a world of digital dependencies*", in *Computer*, 2009, pp. 50–56.
[55] W. PIETERS, *Beyond individual-centric privacy: Information technology in social systems*, in *The Information Society*, 2017, pp. 271–281.

If a society is allowed to monitor, legally, their employees, they may not be out of the legal woods. Enterprise will need to ensure that they are collecting only the information that is necessary, the information that they are collecting is being used only for the purposes for which it was collected, the information is secured properly, and there is a plan in place in case there is a breach.

On the basis of the relevant statistics, the typical employee, usually, complete a personal errand on occasion during work hours. HR departments would benefit from updating their privacy policies and procedures to ensure that the fine line between monitoring employee activity and infringing on employee privacy is not crossed.

The GDPR has opened the way for a new take on privacy laws, and there will be more to come, as said the European commissioner Mariya Gabriel. It is only a matter of time before other countries follows suit of United State legislation. HR departments should come to know the EU General Data Protection Regulation as it not only might affect them directly, but it will soon become the blueprint for regulations of the future. At the very least, it is a good business model to ensure your employees' privacy rights are protected[56].

The Data Protection Act doesn't prevent employers from monitoring workers, but employers should remember workers are entitled to some privacy at work.

Monitoring in the workplace can occur for a variety of reasons: it can be used to safeguard employees, for example to ensure workers aren't at risk from unsafe working practices. In some sectors employers may have a legal or regulatory need to carry out some monitoring. The information gathered through monitoring should only be used for the purpose it was carried out for, unless it leads to the discovery of other things such as a breach of health and safety.

Employers may monitor staff at work in various ways, this can include:

1. CCTV Known as Capacitor coupled voltage transformer s a switchgear device used to convert high transmission class voltage into easily measurable values, which are used for metering, protection, and control of high voltage systems. It can be placed in the workplace for a number of reasons. However, if CCTV is installed the employer should make sure the employees are aware it, this is usually done by displaying signs to say where the locations of the cameras are. Workers should also be given the reason for the monitoring. Signs should be clear, visible and readable. They contain details of the purpose of the surveillance and who to contact about the scheme and include contact details such as website address, telephone number or e mail address. Under the Data Protection Act if the employer gives a reason for the cameras for example to prevent theft, the employer cannot then use the footage for another reason such as recording entry and exit of workers from the workplace[57].
2. looking at use of email or website visits. It's very rare that employers would need to carry out monitoring in secret without the staff being told they are being monitored. Employers must have a genuine reason to carry out covert monitoring such as criminal activities or malpractice. Monitoring must be obtained as quickly as possible, and only

[56] L. BERRY-TAYMAN, *Europe Leads the Way in Employee Privacy Law So It's Time to Embrace GDPR.*
[57] Information Commissioner's Office guidance, *In the picture: A data protection code of practice for surveillance cameras and personal information.*

as part of a specific investigation. The monitoring must stop when the investigation has finished.

3. listening in on telephone calls
4. bag searches. If employers intend to carry out bag searches a workplace policy must be in place that informs employees that bags and purses will be subject to searches. Employers must have a legitimate work-related reason for carrying out searches.
5. Satellite or Global Positioning System (GPS) Surveillance Technology is now incorporated into cell phones, and vehicle tracking technology. GPS is a global navigation tracking system deployed by the Department of Defense, later used extensively for air travel, and has now become available for personal communication devices and service features for personal ground transportation.

These procedures should be made clear and understood by all workers. If a worker does not comply with the policy and procedures they may be liable to disciplinary action.

6. The case of López Ribalda and Others versus Spain

The employment contract creates a particular relationship that is a legal situation between unequals. In this way becomes harder for the employee, to defend oneself and secure his fundamental rights. For the very reason, it is necessary to provide a more effective protection mechanism. Within this scope, many conflicts have been submitted to the European Court of Human Rights (ECHR), to asses the effects of new technologies on right to respect private and family life that enables the individual to protect his/her personal existence in society.

In this prospective can be explained the case of Lopez Ribalda and other versus Spain.

In 2009, the applicants were employed as cashiers or sales assistants by the Spanish supermarket chain M.

After noticing inconsistencies between the stock level and the sales figures as well as financial losses over a period of five months amounting to around 80.000 euros the supermarket manager installs a video surveillance system. The supermarket informed the Spanish Data Protection Agency of the fact of installation and was advised to put up signs saying that CCTV had been installed.

The employees, however, were only informed about the instalment of the visible cameras. The applicants, together with other staff members, were filmed, through the hidden cameras, taking part in the theft of goods. The footage was communicated to a union representative and after fourteen employees, including the applicants, were dismissed on disciplinary grounds, as they were caught on camera helping customers and other co-workers steal as well as stealing themselves.

After some days of recording, several thefts and employees involved are detected and as result of this management fired fourteen employees for disciplinary reasons.

During this process, three of the five applicants have signed an agreement with the employer, admitting their involvement in thefts and waiving their possible future claims for dismissal, in return for the company's promise not to make a denunciation. Following their dismissal, all applicants initiated proceedings for unfair dismissal before the Employment Tribunal questioning the use of covert recordings as evidence and opposing the use of such material as a breach of their privacy. They argued that the CCTV evidence should not be

admitted as it had been obtained in breach of their human rights and further the personal data collected on the CCTV was their data and they had not consented to that data being processed.

The Employment Tribunal found no violation of the right to respect for private life with regard to two applicants as it concluded that the recordings were valid evidence and that their dismissal had been lawful. However, the tribunal dismissed the other three applicants' cases, upholding the employer's objection that the action was invalid because they had signed settlement agreements. Subsequently, the High Court upheld the first-instance judgments on appeal, arguing that the supermarket's surveillance had met the criteria because it had been justified owing to suspicions of misconduct, had been appropriate for the aim pursued, and necessary[58].

The employees appealed and their appeal eventually ended up at the European Court of Human Rights.

About this thematic the Constitutional Court delivered a leading judgment on the lawfulness of video-surveillance in the workplace in the light of the protection provided by Article 18 § 1[59] of the Spanish Constitution[60].In that case the employer had installed a system of hidden CCTV cameras in the ceiling of the clothing and footwear department of a shop, directed towards three tills and the reception desk.

The Constitutional Court held that the measure at stake had to pass a threefold test to be considered acceptable: there had to be a legitimate aim "appropriateness test", and the measure had to be necessary "necessity test" and proportionate "strict proportionality test". In other words, the Court had to verify whether a fair balance had been struck between the interference with a fundamental right and the importance of the legitimate aim pursued. On the subject of the video-surveillance at issue in that case, it found as follows:

"*In the present case, the covert video-surveillance ... was a justified measure since there was a reasonable suspicion that the person investigated had committed some wrongdoing at work; it was suited to the purpose pursued by the company (to verify that the worker was in fact committing the suspected wrongdoing, in which case he would be subjected to an appropriate disciplinary sanction); it was necessary (the recordings were to be used as evidence of the wrongdoing); and it was proportionate (since the cameras were only zoomed in on the checkout counters and solely for a limited period of time) ... ; it follows that there has been no interference with the right to [respect for] privacy as enshrined in Article 18.1 of the Spanish Constitution.*"

---

[58] F. BREGIANNIS, *López Ribalda and Others v. Spain – covert surveillance in the workplace: attenuating the protection of privacy for employees,* in *Labour Law, Right to Private Life*.

[59] ARTICULO 18. "1.Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. 2.El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito. 3.Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial. 4.La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

1. "E' garantito il diritto all'onore, all'intimità personale e familiare e alla propria immagine. 2. Il domicilio è inviolabile. Nessun accesso o perquisizione saranno consentiti senza il consenso del titolare o decisione giudizaria, eccezion fatta nel caso di flagrante reato. 3. E' garantito il segreto delle comunicazioni e in specie di quelle postali, telegrafiche e telefoniche, salvo decisione giudiziale. 4. La legge porrà limiti all'uso dell'informatica per salvaguardare l'onore e l'intimità personale e familiare dei cittadini e il pieno esercizio dei loro diritti".

[60] judgment n. 186/2000.

In a previous judgment of 10 April 2000[61],applying a similar proportionality test, the Constitutional Court had taken the view that video and audio recording devices placed at the checkout and on a gaming table in a casino,had been a disproportionate measure in view of the resulting major interference with the right of employees and customers to respect for their private life. In this case,the court noted that the employer had failed to show how the sound recording, which was particularly intrusive for the right to privacy of those concerned, had been necessary for the protection of its legitimate rights and interests.

Subsequently, in judgment n. 29/2013 of 11 February 2013, which concerned events after the Personal Data Protection Act had entered into force, the Constitutional Court held that the permanent installation of a video-surveillance system, initially as a security measure for the purpose of monitoring employees' activity, required that the workers' representatives and employees be given prior notification and that a failure to do so would be in breach of Article 18 § 4 of the Constitution. In that case, an employee of Seville University had been suspended from his duties without pay for unjustified late arrivals and absences that had been established by means of video-surveillance installed with the approval of the administration. The Constitutional Court found as follows:

"*…it must not be overlooked that the [Constitutional Court has] established, in an invariable and continuing manner, that an employer's power is limited by fundamental rights among many other authorities, STC no. 98/2000, of 10 April, legal ground no. 7, or STC no. 308/2000, of 18 December, legal ground no. 4). Consequently, in the same way that the 'public interest' behind the punishment linked to an administrative offence is not enough to allow the State to deprive the citizen concerned of his or her rights derived from [sections 5(1) and (2) of the Personal Data Protection Act] (STC 292/2000, of 30 November, legal ground no. 18), the 'private interest' of an employer cannot justify using the worker's personal data to his or her detriment without previously informing him or her of the monitoring measures that have been implemented"*. There is no reason in the employment sphere to restrict the right to be informed, a fundamental right that is protected by Article 18.4 of the Constitution. Accordingly, it is not enough that the data processing itself is lawful, being prescribed by law (section 6(2) of the Personal Data Protection Act), or proves, in a given case, to be proportionate to the aim pursued; monitoring by the employer, while certainly possible, must also guarantee the requisite prior information.

In a judgment of 3 March 2016[62] the Constitutional Court consolidated its case-law concerning the use of hidden surveillance cameras. In this case the manager of a clothing shop had detected some thefts from the till and suspected one of its employees. He had temporarily installed hidden cameras zoomed in on the area where the till was located. The employer had placed a sign indicating in a general manner the presence of CCTV cameras, including the information provided for by section 5 of the Personal Data Protection Act, as required by Article 3 of Instruction no. 1/2006 issued by the Spanish Data Protection Agency. The Constitutional Court explained in the following terms the relevance of the fulfilment of the obligation to provide information under section 5 of that Act:

[61] Costitutional Court of Spain, judgment of 10 april 2000, no. 98/2000
[62] Costitutional Court of Spain judgment of 03 march 2016, no. 39/2016.

"*as has been emphasized, even though the express consent of the employee is not required to implement a monitoring measure which involves the processing of [personal data], the obligation to provide information under section 5 of the Personal Data Protection Act remains. Without prejudice to any legal sanctions which may be entailed by an employer's failure to comply with the obligation, for it to constitute a violation of Article 18.4 of the Constitution it is necessary to ascertain whether the proportionality principle has been upheld. The right to data protection should be weighed in the balance against any limitations that may be justified by the employee's work obligations and the corresponding power of monitoring and supervision granted to the employer by Article 20.3 of the Labour Regulations, in relation to Articles 33 and 38 of the Constitution. The assessment of the constitutional relevance of a total or partial lack of information in cases of video-surveillance in the workplace requires the balancing in each case of the competing constitutional rights and values: on the one hand the employees' right to the protection of personal data and, on the other, the employer's management power, which, essential as it is to the proper running of a productive organization, reflects the constitutional rights recognized in Articles 33 and 38 of the Constitution and ... is enshrined in Article 20.3 of the Labour Regulations, which expressly empower the employer to adopt monitoring and supervision measures in order to verify that the workers comply with their employment duties ... This general monitoring power provided for by law legitimize the supervision carried out by the employer of the employees' performance of their professional tasks (see ... the judgment of the European Court of Human Rights Bărbulescu v. Romania of 6 [sic] January 2016), without prejudging the particular circumstances of each case, which will determine whether or not the monitoring implemented by the employer has entailed a violation of the fundamental right at stake".*

In that case the Constitutional Court found that there had been no violation of Article 18 § 4 of the Constitution, in particular on the ground that the employer had placed a board indicating that video-surveillance was in place, in accordance with the regulations. It considered that the board contained sufficient information as to the existence of monitoring and the purpose of the data processing. After examining the proportionality of the interference with the employee's private life, using the criteria laid down in the case-law, it further found that there had not been any breach of the right to personal privacy protected by Article 18 § 1 of the Constitution.

The case was referred to the European Court of human right.

6.1 The decision of the Grand Chamber of European Court of human Right

Under Article 8 "*right to respect for private life*" and Article 6 § 1 "*right to a fair trial*" of the ECHR, the applicants complained about the covert video-surveillance and the courts' use of the data obtained to find that their dismissals had been fair. In particular, the three applicants who signed settlement agreements also argued that the agreements had been forced upon them due to the video material and should not have been used as evidence during the dismissal procedure.

According to the Chamber: "*while the video-surveillance had been set up on account of legitimate suspicions of theft, it had been broad in scope – not being limited in time, affecting all the employees working at the tills and covering all working hours – and had breached the obligation under domestic law to give prior information, to those persons who were concerned*

by the collection and processing of their personal data, of the existence, purpose and implementation of the measures".

For this reason, the case was referred to the Grand Chamber on 28 May 2018.

The Grand Chamber disagreed with its junior and allowed the appeal by a majority ruling. It held that the employer's failure to inform the workers that they were being covertly monitored did not infringe their right to privacy. In reaching its conclusion that the surveillance was proportionate, the Grand Chamber evaluated a number of factors.

It was significant that duration of surveillance had lasted for a short period of time. As the filming had been limited to only ten days, the intrusion it presented was minimal.

The court also examined how levels of privacy could differentiate depending on location. Here, as the employees worked on a supermarket floor which was accessible to the public, a lower standard of privacy should be expected, as opposed to private spaces such as toilets or changing rooms, where video surveillance should be entirely prohibited.

The scale of misconduct involved could potentially justify the installation of hidden CCTV. Here, due to the extent of the losses incurred sometimes up to €20,000 per month and the fact that the employer had reasonable cause to suspect the employees were guilty of theft, surveillance had not exceeded what was necessary. The court also gave weight to the fact that only a limited number of people had viewed the footage. In particular, the employer had attempted to prevent the recordings being accessed and circulated throughout the organisation.

The three dissenting judges disagreed with these findings, contending that its colleagues had failed to strike a balance between the employer's and the employees' respective rights. The minority also voiced concern in regards to technological advances, stating that such developments pose additional challenges when protecting Article 8 rights and advocated the need an enhanced protection of privacy in our modern day world[63].

Later, the Court ruled on the applicability of Article 8[64]. The applicants argued that their employer's decision to dismiss them had been based on recordings obtained by means of video-surveillance in their workplace, in breach of their right to respect for their private life, and that, by refusing to declare their dismissal null and void, the domestic courts had failed in their duty to protect that right. They relied on Article 8 of the Convention. To that end, it reviewed the concept of 'private life', as defined by the Court's case law, and acknowledged ones reasonable expectation not to be recorded in his private social life.

In order to invoke Article 8, an applicant must show that his or her complaint falls within at least one of the four interests identified in the Article, namely: private life, family life, home and correspondence. Some matters, of course, span more than one interest. First, the Court

---

[63] J. SHELSTON, *Employer's secret recording of employees did not breach privacy rights*, in *Brabners Foundation*.
[64] ARTICOLO 8 – Right to respect for private and family life "1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others." Diritto al rispetto della vita privata e familiare. "1. Ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza. 2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria per la sicurezza nazionale, per la pubblica sicurezza, per il benessere economico del paese, per la difesa dell'ordine e per la prevenzione dei reati, per la protezione della salute o della morale, o per la protezione dei diritti e delle libertà altrui".

determines whether the applicant's claim falls within the scope of Article 8. Next, the Court examines whether there has been an interference with that right or whether the State's positive obligations to protect the right have been engaged. Conditions upon which a State may interfere with the enjoyment of a protected right are set out in paragraph 2 of Article 8, namely in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. Limitations are allowed if they are "in accordance with the law" or "prescribed by law" and are "necessary in a democratic society" for the protection of one of the objectives set out above. In the assessment of the test of necessity in a democratic society, the Court often needs to balance the applicant's interests protected by Article 8 and a third party's interests protected by other provisions of the Convention and its Protocols.

The primary purpose of Article 8 is to protect against arbitrary interferences with private and family life, home, and correspondence by a public authority[65]. This obligation is of the classic negative kind, described by the Court as the essential object of Article 8[66]. However, member States also have positive obligations to ensure that Article 8 rights are respected even as between private parties[67]. In particular, although the object of Article 8 is essentially that of protecting the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private life[68]. These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves[69].

As pointed out, this expectation might be higher in relation to certain areas of the supermarket, such as toilets and private rooms, yet still exists in open public spaces, such as the entrance/exit or the area of the checkout counters. As video-surveillance was in place in the applicants' workplace for a period of ten days, the hidden cameras being directed towards the supermarket checkout area and its surroundings and potentially recording the employees during their whole workday, the Court concluded that the employer's measure interferes with Article 8.

In this context the Court first observed that the Spanish Government had argued that the State was not responsible in this case as the disputed acts had been carried out by a private company. However, the Court reiterated that countries had a positive obligation under the European Convention to take measures to ensure respect for private life and it therefore had to examine whether the State had struck a fair balance between the applicants' rights and the employer's. Under Spanish law individuals were to be clearly told about the storage and processing of personal data, but the applicants had had no such warning. The domestic courts

[65] European Court of Human Rights judgment of 22 february ,n. 588/2013, Libert v. France, para. 40-42.
[66] European Court of Human Rights judgment of 27 october 1994, n. 18535/1991, Kroon and Others v. the Netherlands, para. 31.
[67] European Court of Human Rights judgment of 5 september 2017, n. 61496/2008, Bărbulescu v. Romania [GC], para.108-111 as to the actions of a private employer
[68] European Court of Human Rights judgment of 24 april 2018, n. 4587/2019, Lozovyye v. Russia, para.36.
[69] See, for example, European Court of Human Right judgment of 10 april 2007, n. 6339/2005, Evans v. the United Kingdom [GC], para. 75, although the principle was first set out in , European Court of Human Right judgment of 13 june 1979, n. 6833/1974, Marckx v. Belgium.

had found that justifiable given the reasonable suspicions of theft and because there had been no other way to provide sufficient protection for the employer's rights and interfere less with those of the applicants. The Court observed that it had not found a violation in the case of Köpke v. Germany, which had also concerned covert video surveillance of an employee. However, in that case there had been no clear domestic law on the issue and the surveillance had been limited. The monitoring in this case had involved all employees over several weeks, during all working hours. The Court disagreed with the domestic courts about the proportionality of the measure. The surveillance had not complied with Spanish law, in particular when it came to notification, and the employer's rights could have been given at least some protection by other means. For instance, the 3 company could have provided the applicants with general information about the surveillance and given the notification required under the Personal Data Protection Act. The Court found that the domestic courts had failed to strike a fair balance between the rights involved and there had been a violation of Article 8 in respect of the applicants.

The Court examined whether the use of the video material obtained in violation of the European Convention, Article 6[70], had made the domestic proceedings as a whole unfair. It noted that the applicants had been able to challenge the authenticity of the recordings in adversarial proceedings and that the films had not been the sole evidence for the courts' decisions, which had also been based on witness statements. The Court also saw no reason to

[70] ARTICLE 6. Right to a fair trial 1. "*In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly but the press and public may be excluded from all or part of the trial in the interests of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice. 2. Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law. 3. Everyone charged with a criminal offence has the following minimum rights: a) to be informed promptly, in a language which he understands and in detail, of the nature and cause of the accusation against him; (b) to have adequate time and facilities for the preparation of his defence; (c) to defend himself in person or through legal assistance of his own choosing or, if he has not sufficient means to pay for legal assistance, to be given it free when the interests of justice so require; (d) to examine or have examined witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him; (e) to have the free assistance of an interpreter if he cannot understand or speak the language used in court*".
Diritto a un equo processo 1. "Ogni persona ha diritto a che la sua causa sia esaminata equamente, pubblicamente ed entro un termine ragionevole da un tribunale indipendente e imparziale, costituito per legge, il quale sia chiamato a pronunciarsi sulle controversie sui suoi diritti e doveri di carattere civile o sulla fondatezza di ogni accusa penale formulata nei suoi confronti. La sentenza deve essere resa pubblicamente, ma l'accesso alla sala d'udienza può essere vietato alla stampa e al pubblico durante tutto o parte del processo nell'interesse della morale, dell'ordine pubblico o della sicurezza nazionale in una società democratica, quando lo esigono gli interessi dei minori o la protezione della vita privata delle parti in causa, o, nella misura giudicata strettamente necessaria dal tribunale, quando in circostanze speciali la pubblicità possa portare pregiudizio agli interessi della giustizia. 2. Ogni persona accusata di un reato è presunta innocente fino a quando la sua colpevolezza non sia stata legalmente accertata. 3. In particolare, ogni accusato ha diritto di: (a) essere informato, nel più breve tempo possibile, in una lingua a lui comprensibile e in modo dettagliato, della natura e dei motivi dell'accusa formulata a suo carico; (b) disporre del tempo e delle facilitazioni necessarie a preparare la sua difesa; (c) difendersi personalmente o avere l'assistenza di un difensore di sua scelta e, se non ha i mezzi per retribuire un difensore, poter essere assistito gratuitamente da un avvocato d'ufficio, quando lo esigono gli interessi della giustizia; (d) esaminare o far esaminare i testimoni a carico e ottenere la convocazione e l'esame dei testimoni a discarico nelle stesse condizioni dei testimoni a carico; (e) farsi assistere gratuitamente da un interprete se non comprende o non parla la lingua usata in udienza".

challenge the domestic courts' findings that it had been possible to use the third, fourth and fifth applicants' settlement agreements as evidence, even if they had been obtained after the video recordings had been shown to them. The domestic courts had weighed up the validity of the documents and the applicants had had ample opportunity to object to them. Overall, it found no breach of the fair trial provision. It also rejected as manifestly ill-founded the first applicant's complaint about a lack of reasoning or consideration of specific circumstances by the courts. Additionally, it is underlined that the footage was not the only evidence for proving the thefts and its use did not undermine the fairness of the trial. As mentioned in the judgment, the applicants' statements, the testimony of the supermarket manager, the company's legal representative and the staff representative, and the expert's report comparing the images recorded by the video-surveillance and the till receipts were also taken into account. In assessing the settlement agreements signed between the employer and three of the applicants, the Court confirmed that no trace of intimidation or duress could be identified.

The Court found in particular that under Spanish data protection legislation the applicants should have been informed that they were under surveillance, but they had not been. The employer's rights could have been safeguarded by other means and it could have provided the applicants at the least with general information about the surveillance. The domestic courts had failed to strike a fair balance between the applicants' right to privacy and the employer's property rights. However, the Court found that the proceedings as whole had been fair because the video material was not the only evidence the domestic courts had relied on when upholding the dismissal decisions and the applicants had been able to challenge the recordings in court[71].

The Chamber noted that "*while the video-surveillance had been set up on account of legitimate suspicions of theft, it had been broad in scope – not being limited in time, affecting all the employees working at the tills and covering all working hours – and had breached the obligation under domestic law to give prior information, to those persons who were concerned by the collection and processing of their personal data, of the existence, purpose and implementation of the measures. Having regard to those factors, the Chamber did not share the opinion of the domestic courts as to the proportionality of the video-surveillance measure taken by the employer. It was of the view, in particular, that the employer's rights could have been secured by informing the applicants, even in a general manner, of the installation of a video-surveillance system"*.

In this way, the Chamber found that the domestic courts had failed to strike a fair balance between the applicants' right to respect for their private life and the other interests at stake, and that there had thus been a violation of Article 8 of the Convention.

However, there were dissenting opinion of judges De Gaetano, Yudkivska and Grozev.

They showed that this case demonstrates the growing influence and control that technology has in our world, and more particularly, the collection and use of our personal data in our everyday activities. As a living instrument, the Convention, and therefore the Court, not only needs to recognise the influence of modern technologies, but also has to develop more adequate legal safeguards to secure respect for the private life of individuals.

[71] Press contacts echrpress@echr.coe.int.

In particular, new technologies have dramatically changed the ease with which video-surveillance can both be carried out and transmitted, thus multiplying significantly the potential infringement of privacy rights under Article 8 of the Convention. It is precisely for this reason that there is a need, at national level, for the legislative framework to be clear and foreseeable in relation to cases concerning electronic surveillance. This becomes crucial in cases such as the present one, where an employer uses covert video-surveillance in the workpalace. Therefore a clear and foreseeable legal framework, with appropriate and effective safeguards, becomes of paramount importance. Moreover, the legal framework is of particular importance in the context of employment relationships, where the employer has significant powers with regard to employees and any abuse of those powers should be avoided. Information on the implementation of surveillance measures is essential for the persons concerned to be able to assert the totality of the rights that they are guaranteed, such as the rights of access, of rectification.

The majority agree that Spanish law requires that *"it is necessary to inform the individuals concerned, clearly and prior to implementation, of the existence and conditions of such data collection"*, thus limiting the invasion of privacy and giving employees the opportunity to regulate their conduct. This requirement was clearly not met in the present case. However, the majority went on to hold that this was "*just one of the criteria to be taken into account in order to assess the proportionality of a measure*"[72]. The Employment Tribunal, when judging the proportionality of the measure, did not expressly address the applicants' argument that they had not been informed of the monitoring specifically and prior to its implementation, as required by domestic law.

They also find unsatisfactory the assessment made by the domestic courts when determining whether the covert video-surveillance had been necessary. The Tribunal confirmed that it was a necessary measure for the legitimate aim pursued, to discover who had committed thefts in the supermarket. However, the Tribunal failed to consider whether a less restrictive measure could have been used by the employer to pursue the same aim. This failure takes on particular importance in the light of the majority's finding that the question whether it would have been possible "*to set up a monitoring system based on less intrusive methods and measures*"[73] is an important factor to be assessed in order to ensure the proportionality of covert video-surveillance measures in the workplace.

The employer had two legitimate aims: firstly, it wanted to stop further theft, for which purpose a warning about the installed video-surveillance system would have been sufficient. Secondly, it wanted to find out who was responsible for the losses it had sustained over the past months; here, prior notice of the visible and covert video-surveillance would not have proven useful. Nevertheless, since the theft committed was a criminal offence, the employer could have, and should have, gone to the police prior to taking such measures on its own initiative. The need to elucidate an offence does not justify private investigation, including in the form of covert video-surveillance, which amounts to an excessively intrusive measure and an abuse of power.

---

[72] European Court of Human Rights judgment of 17 october 2019, nos. *1874/13 and 8567/13*, Lopez - Ribalda and al. v. Spain, para. 131.
[73] European Court of Human Rights judgment of 17 october 2019, nos. *1874/13 and 8567/13*, Lopez – Ribalda and al. V. Spain, para. 116.

For all these reasons, according to the view of above judge the Court had to confirm, extend, and transpose the *Bărbulescu*[74] principles, as set out in paragraph 121, in respect of covert video-surveillance cases such as the present one. It established an important principle regarding the extent of control that can be exercised by an employer upon its employees, as well as a multitude of factors that the national courts have to consider in order to strike a fair balance between the competing interests of the parties.

In addition to exclude violation of Article 8 of the Convention, the Court has decided to allow the unlimited use of covert video-surveillance in the workplace without affording sufficient legal safeguards to those whose personal data will be collected and used for purposes unknown to them. With the growing influence that technology has on our society, the dissenting judges said that ITC cannot afford to let individuals take justice into their own hands and allow the right to a private life under Article 8 of the Convention to remain insufficiently protected when faced with such new challenges.

In the age of digital surveillance, the modern technologies establish new relationships between employer and employee. At the same time, they undermine the privacy of individuals in spaces such as workplaces open to the public, where the protection threshold is already set low.

7. Conclusions

Undoubtedly, technology developments and the advent of social networks have constantly renewed the world we live in. This has been definitely true for privacy. Nowadays, in fact, internet has undermined the monopoly on information and users, while longing for more privacy, feel the urge to share personal content and store data on the web, with the due risks. Indeed, details about our personality and private life are, more than before, no longer ours. Therefore, the recognition of a protection regarding the processing of personal data is fundamental, especially in employment relationships.

Many employers use cameras and video surveillance in the workplace, often to prevent theft or to monitor what employees are actually doing while on the clock. As long as the company has a legitimate need to film, the areas under surveillance are public, and employees know about the filming, these practices are likely to be upheld by a court. Because filming can implicate privacy rights, however, employers must be very careful not to cross the line.

In order for an employer to legally register employees at the workplace, there must be a legitimate business reason for the recording. Such purposes can include security reasons, time and motion studies, or other investigative processes. Camera recordings in areas where employees have a reasonable expectation of privacy, like locker rooms or bathrooms, is almost always prohibited.

If the recording is done by visible cameras, law seems to allow videotaping of individuals in the workplace, even without their consent or knowledge, as long as it is not done to commit a crime.

Otherwise, if the recording is done by hidden cameras, courts place a higher burden of proof for the employer to demonstrate that the surveillance is for a legitimate business reason.

[74] European Court of Human Rights judgment of 12 januray 2016, no. *61496/08* , Lopez - Ribalda and al. v. Spain, para. 131.

This means that employers cannot simply say the recording is for security reasons, and must provide a reason beyond that in order to justify their use of hidden cameras. In places where employees are unaware of video surveillance, their reasonable expectation of privacy may be heightened. As a result, employers are generally well-advised to provide notice of hidden cameras in the workplace.

By the way, we must create a prospective by which is possible to balance human right and defeat the offences generated at work.