VOLUME 5 ISSUE 2 ARTICLES & ESSAYS

UNIVERSITY OF BOLOGNA LAW REVIEW

https://doi.org/10.6092/issn.2531-6133/10514

Video Surveillance of the Employees Between the Right to Privacy and Right to Property After López Ribalda and Others v. Spain

VELJKO TURANJANIN †

ABSTRACT

The tension between safety and privacy has become an important issue in the modern world. Video surveillance systems are indeed powerful tools for fighting crime on the one hand, and for the protection of property from theft on the other. The European Court of Human Rights (ECtHR) has examined the issue of video surveillance in many of its decisions. In this work, the author analyses the issue of video surveillance over employees and its influence on fundamental human rights and freedoms. He elaborates upon the ECtHR's case of López Ribalda and Others v. Spain in order to identify the balance between the right to privacy and the right to property. This is a case from the civil law, but with elements that could may be used in the criminal proceedings. Furthermore, it is important to determine when exactly the video footage of employees may be used as evidence in criminal proceedings. After the introductory remarks, the author briefly deals with the facts of the above case and explains the basic applicable international legal acts. He then observes the issue of video surveillance from two points of view – those of Article 8 and Article 6 of the European Convention on Human Rights and Fundamental Freedoms (ECHR). Finally, he concludes that the ECHR took the right direction in establishing the balance between the protection of property and the right to privacy.

KEYWORDS

Video-Surveillance; Employee; Illegally Obtained Evidence; Human Rights

TABLE OF CONTENTS

† Dr. Veljko Turanjanin, Assistant Professor of Law, University of Kragujevac (Republic of Serbia); Ph.D., University of Kragujevac (Republic of Serbia). Dr. Turanjanin focuses on criminal procedure law, juvenile criminal law, organized crime and human rights. The latest scientific projects he has been dealing with cover the topics of human rights and the relationship between Serbian and E.U. law.

INTRODUCTION

As a child, I read two books that influenced me deeply: George Orwell's *1984* and Aldous Huxley's *Brave New World*. At the time, it seemed to me that those works told stories of an unimaginable future; yet, that future is now here. In recent times, the use of video surveillance by both the public authorities and the private sector is becoming increasingly common, and so are fear and distrust, as demonstrated by specific problems and public outrage aroused by Edward Snowden's recent disclosures.[1] Video surveillance, without a doubt, represents a valuable tool to protect people and property from damage and theft. Further, prosecuting authorities around the world have increasingly come to rely on the notion of seriousness to loosen the safeguards built into the criminal justice system, most notably around the protection that is usually granted to suspects, shifting towards a risk–security–seriousness paradigm, while simultaneously increasing the use of surveillance and closed-circuit television [hereinafter C.C.T.V.]; in turn, these are often at odds with the notion of respect for private life, as exemplified in Article 8 of the European Convention on Human Rights and Fundamental Freedoms [hereinafter Eur.Ct.H.R.].[2] As Mahmood Rajpoot and Jensen point out,

> . . . law enforcement agencies worldwide rely on closed circuit TV (C.C.T.V.) systems to help prevent, detect and investigate attacks against public safety. It is also used to detect and investigate attacks against property, e.g. vandalism. The private sector also uses C.C.T.V. to protect public safety in the private sphere mostly to protect against intrusions, theft and vandalism.[3]

The first video surveillance systems appeared in the 1950s and their development was then boosted by the invention of the video cassette in 1956; used by private individuals, these quickly became widespread in the following three decades.[4] However, the practice of visual surveillance is much older, originating in the late nineteenth century as a method to assist prison officials in the discovery of escape techniques.[5]

Today, video surveillance is most often used in public places and by institutions or companies, who operate C.C.T.V. systems composed of a set of cameras monitoring a

[1] Rachel C. Taylor, *Intelligence-Sharing Agreements & International Data Protection: Avoiding a Global Surveillance State*, 17 Wash. Univ. Glob. Stud. L. Rev. 731, 739 (2018).
[2] Anthony Amatrudo & Leslie William Blake, Human Rights and the Criminal Justice System 105 (2014).
[3] Qasim Mahmood Rajpoot & Christian Jensen, *Video Surveillance: Privacy Issues and Legal Compliance*, *in* Promoting Social Change and Democracy through Information Technology 69 (Vikas Kumar & Jakob Svensson eds., 2015).
[4] *See* Council of Europe, *Video Surveillance of Public Areas* (PACE, Working Paper No. 115, 2008).
[5] Anthony C. Caputo, Digital Video Surveillance and Security 1 (2010).

specific protected area, with additional equipment used for transferring, viewing and / or storing and further processing the C.C.T.V. footage.[6] As technological innovations invade all facets of life, and particularly as unobtrusive monitoring devices become more easily available, the tension between safety and privacy is becoming an important issue in the modern world.[7]

The right to privacy is a constitutionally well–recognized human right.[8] As stated above, the European Court of Human Rights [hereinafter Eur.Ct.H.R.] has examined the issue of video surveillance (in both public and private areas) in many of its decisions. On the one hand, the pervasive use of video cameras in public places captures the activities of people and allows officials to observe the daily activities of a target individual; such pervasive surveillance may have a negative impact on the people's democratic rights to freely express their thoughts and to associate freely in order to share those thoughts.[9] On the other hand, the video surveillance of employees in private companies raises numerous questions. Video surveillance technologies are inordinately intrusive into an individual's privacy, to an extent that they jeopardize personal autonomy.[10]

As judges De Gaetano, Yudkivska and Grozev pointed out in their joint dissenting opinion in the case of Lopez Ribalda and Others v. Spain which in itself demonstrates the growing influence and control that technology has in our world which in particular pertains to the collection and use of our personal data in everyday activities; in such circumstances, the Eur.Ct.H.R. needs to interpret the Convention as a living instrument, which means not only recognising the influence of modern technologies but also developing more adequate legal safeguards to secure respect for the private life of individuals.

The key judgment examined in this work is *López Ribalda and Others v. Spain*. In this judgment, the Eur.Ct.H.R. further elaborated on the proportionality of video surveillance measures in the workplace. This judgment is essentially a matter of labour law; at the same time, it raises the question of the use of video footage of employees as evidence in criminal procedures. The factors that have to be taken into consideration should be applied regardless of whether the case falls within the sphere of civil or criminal law. For the purpose of such considerations, we must first elaborate on the right to privacy and

[6] Dana Volosevici, *Some Considerations on Video-Surveillance and Data Protection*, 5 Jus et Civitas: J. Soc. & Legal Stud. 7, 9 (2018).
[7] Elizabeth G. Adelman, *Video Surveillance in Nursing Homes*, 2 Alb. L. J. Sci. & Tech. 821, 821 (2002); Quentin Burrows, *Scowl because you're on Candid Camera: Privacy and Video Surveillance*, 31 Val. U. L. Rev. 1079 (1997).
[8] David Banisar & Simon Davies, *Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments*, 18 J. Marshall J. Comput. Info. L. 1, 3 (1999).
[9] Mahmood Rajpoot & Jensen, *supra* note 3, at 70.
[10] Christopher S. Milligan, *Facial Recognition Technology, Video Surveillance, and Privacy*, 9 S. Cal. Interdisc. L. J. 295, 299 (1999).

the right to a fair trial. First, the issue of the processing of personal data is integrated into Article 8 of the Eur.Ct.H.R., while the issue of evidence is integrated into Article 6 of the Eur.Ct.H.R.. The author believes that the court in Strasbourg will and should apply the same criteria regarding video surveillance of employees in matters of criminal law and of labour law.

Therefore, this work starts by examining the compliance of video surveillance with Article 8 of the Eur.Ct.H.R. and continues with analysing the issue of admissibility of such evidence under Article 6 of the Eur.Ct.H.R.. Before that, the author will briefly lay out the facts of the case. Next, this work shall deal with the basic international acts relevant to the subject.

1. FACTS OF THE CASE *LÓPEZ RIBALDA AND OTHERS V. SPAIN*

Here, the applicants were all working in a supermarket of the M. chain situated in Sant Celoni (Barcelona province); the first three applicants were cashiers, while the fourth and fifth applicants were sales assistants behind a counter. Starting from March 2009, the supermarket's manager noticed inconsistencies between the stock level and the sales figures, and in the following months, he identified losses of approximately 80,000 Euros. The manager started an internal investigation to shed light on the losses, and in that context, on June 15th, 2009, he installed C.C.T.V. cameras. Some cameras were visible, but others were hidden. It is important to note that the visible cameras were directed towards the entrances and exits of the supermarket, while the hidden cameras were placed at a certain height and directed towards the checkout counters. Three tills were covered by the range of each camera, including the areas in front of and behind the counters, and the exact number of tills being monitored was not stated by the parties. The documents in the file show that at least four tills were filmed. The manager called a meeting to inform the supermarket's staff of the installation of the visible cameras on account of the management's suspicions about thefts. However, the problem arose because of the hidden cameras. In this case, neither the staff nor the staff committee was informed of the existence of these cameras. The important fact for the management is that in 2007, the company had notified the Spanish Data Protection Agency that it intended to install C.C.T.V. cameras in its shops. Accordingly, the Agency emphasized the obligations to provide information under the legislation on personal data protection, while a sign indicating the presence of C.C.T.V. cameras had been installed in the shop

where the applicants worked. However, the parties did not indicate the location of the cameras.

Hidden cameras recorded footage and revealed thefts of goods at the tills by a number of employees. The management of the supermarket informed the union representative about that fact on June 25th, 2009. The representative watched the recordings and after that, on June 25th and 29th, 2009, all the workers suspected of theft were called for individual interviews. Fourteen employees were dismissed as a consequence, including the five applicants. Before the interviews, all suspected workers, including the applicants, had a meeting with the union representative. The union representative told them she had watched the video recordings. That was enough for some workers because during the meeting, a number of employees admitted that they had been involved in the thefts with other colleagues. In addition, the employees concerned were notified of their dismissal on disciplinary grounds with immediate effect and the dismissal letters indicated that the hidden C.C.T.V. cameras had filmed them. Cameras showed that on several occasions between June 15th and 18th, 2009, the workers helped customers or other supermarket employees to steal goods and stole goods themselves. Among the other facts, the letters clearly stated that the first three applicants worked at the tills. They had allowed customers and colleagues to go to the cash till and leave the shop with goods they had not paid for. Furthermore, they added that those applicants had scanned items presented at the checkout by customers or colleagues and had then cancelled the purchases, with the result that the goods had not been paid for. A comparison between the goods actually taken away by customers and the sales receipts had made it possible to prove everything. Finally, the cameras had reportedly caught the fourth and fifth applicants stealing goods with the help of their colleagues at the tills. According to the employer, and the law, these acts constituted a serious breach of obligations of good faith and loyalty required in the employment relationship, and justified the termination of the contract with immediate effect. For this work, it is particularly important that the applicants and other employees had appealed against their dismissals before the Employment Tribunal in Spain, the employer filed a criminal complaint against fourteen employees, including the five applicants on July 31st, 2009. Consequently, criminal proceedings were opened against them. However, the investigating judge decided to reclassify the charges as a minor offence (*falta*) on July 15th, 2011, finding that the investigation had not established that there had been any concerted action between the defendants in committing the offences and that the value of the goods stolen by each defendant had not exceeded 400 euros. In a decision of September 27th, 2011, the judge declared that the prosecution was time-barred on account of the statutory limitation of proceedings for that type of offence.

2. RELEVANT INTERNATIONAL ACTS IN THIS FIELD

The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8, and as the Eur.Ct.H.R. stated in *S. and Marper v. The United Kingdom* and recently, in *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*.[11] Therefore, in this matter, the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [hereinafter the Personal Data Convention] plays a crucial role. This is the first legally binding international instrument that recognises the protection of individuals regarding the automatic processing of their personal data.[12] Under Article 2, personal data means any information relating to an identified or identifiable individual, while automatic processing includes storage of data, carrying out logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination. Then, as Article 5 prescribes,

> personal data undergoing automatic processing shall be (a) obtained and processed fairly and lawfully; (b) stored for specified and legitimate purposes and not used in a way incompatible with those purposes; (c) adequate, relevant and not excessive in relation to the purposes for which they are stored; (d) accurate and, where necessary, kept up to date; (e) preserved in a form which permits identification of the data subjects for no longer than is required for he purpose for which those data are stored.

Regarding the Personal Data Convention, Article 8 is particularly important. It prescribes that:

> [A]ny person shall be enabled to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file; to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form; to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles; to have a remedy if a request for confirmation or, as the

[11] S. and Marper v. The United Kingdom, App. Ns. 30562/04 and 30566/04, Eur.Ct.H.R. (2008); Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, App. No. 931/13, Eur.Ct.H.R. (2017).

[12] Dolores-Fuensanta Martínez-Martínez, *Unification of Personal Data Protection in the European Union: Challenges and Implications*, 27 El Profesional de la Información 185, 187 (2018).

> case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.

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, in its relevant parts, provides numerous rights and obligations.[13] This Directive was repealed by the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. The Regulation (EU) 2016/679 has been applicable since 25 May 2018.[14] This

[13] The Council Directive 95/46, art. 7, 1195 O.J. (L 281) 1, 2 (EC) provided that personal data had to be

> (a) processed fairly and lawfully; (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards; (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed; (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified; (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.

Further, the same article provides that

> . . . personal data could be processed only if: (a) the data subject has unambiguously given his consent; or (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or (c) processing is necessary for compliance with a legal obligation to which the controller is subject; or (d) processing is necessary in order to protect the vital interests of the data subject; or (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.

Among others, Article 10 of this Directive provided that

> . . . the controller or his representative had to provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it: (a) the identity of the controller and of his representative, if any; (b) the purposes of the processing for which the data are intended; (c) any further information such as the recipients or categories of recipients of the data or the existence of the right of access to and the right to rectify the data concerning him.

In the end, what is particularly important for these considerations is that legislative measures could be adopted to restrict the scope of the obligations and rights when such a restriction constitutes a necessary measure to safeguard national security; defence; public scrutiny; the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for regulated professions; an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters; a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e) and the protection of the data subject to the rights and freedoms of others.

[14] As Julia Hörnle pointed out, the comparison with the now superseded Directive 95/46/EC is important as it sketches the background and development of current data protection law, which is important for the wider context and in particular for showing how difficult coordination of national competences in this field has

Regulation was finally adopted more than four years after the European Commission proposed it.[15] It incorporates most of the provisions of Directive 95/46/EC and reinforces some of the safeguards contained therein. This Regulation has direct applicability in all EU member states, and is automatically integrated into the national legislation once it enters into force.[16]

According to Article 4, Point 1 of the Regulation (EU) 2016/679 personal data means

> any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Video-surveillance footage often contains images of people and the information can be used to identify these people either directly or indirectly, while recognizable facial images always constitute personal data.[17] According to Point 2, processing means

> any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
>
> Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another

been. Julia Hörnle, *Juggling More than Three Balls at Once: Multilevel Jurisdictional Challenges in EU Data Protection Regulation*, 27 Int'l J. L. & Info. Tech. 142, 143 (2019). In the development of data protection, it is important to draw attention to the Directive 2016/680, of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, 2016 O.J. (L 116/89).

[15] W. Gregory Voss, *European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting*, 72 Bus. Law. 221, 221-22 (2016).

[16] For example, Simona Chirica, *The Main Novelties and Implications of the New General Data Protection Regulation*, 6 Persp. Bus. L.J. 159 (2017).

[17] *See* Volosevici, *supra* note 6, at 8.

> natural person; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child" (Article 6 Paragraph 1 of the Regulation (EU) 2016/679).[18]

[18]Furthermore, Point (f) of Regulation 2016/679, art. 6, 2016 J.O (L 119) 2-4 (EU) provides that

> . . . shall not apply to processing carried out by public authorities in the performance of their tasks. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations . . . . The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by Union law or Member State law to which the controller is subject. The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations . . . The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia: (a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing; (b) the context in which the personal data have been collected, in particular regarding the relationship between data subject and the controller; (c) the nature of the personal data, in particular whether special categories of personal data are processed or whether personal data related to criminal convictions and offences are processed; (d) the possible consequences of the intended further processing for data subjects and (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Just to clarify, this Regulation under the pseudonymisation understands the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person, while - as provided by Regulation 2016/679, art. 4, 2016 J.O (L 119) 7,8 (EU) - controller is

> . . . the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Restrictions are provided under Article 23 in a case of

> (a) national security; (b) defence; (c) public security; (d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; (e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security; (f) the protection of judicial independence and judicial proceedings; (g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions; (h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g); (i) the protection of the data subject or the rights and freedoms of others; (j) the enforcement of civil law claims.

The next important international document is the opinion of the Venice Commission on "video surveillance by private operators in the public and private spheres and by public authorities in the private sphere and human rights protection", adopted at its 71st Plenary Session in 2007. According to it, the private sphere in a physical meaning is a place where those who own this private sphere can restrict access. Private spheres are not, in principle, open freely to the public and are not accessible indiscriminately. Rules governing the private sphere are mainly those related to private law and more specifically to the rights to privacy. The powers of the public authorities over these areas are more restricted than over public areas (point 15). The private sphere will also include workplaces and the use of video surveillance in workplace premises, which raises legal issues concerning the employees' privacy rights (point 18). As regards workplaces, the introduction of video monitoring requires respecting the privacy rights of the employees (point 52). Video surveillance would, in general, be allowed to prevent or detect fraud or theft by employees in case of a well-founded suspicion. However, except in very specific circumstances, videotaping would not be allowed at places such as toilets, showers, restrooms, changing rooms, or smoking areas and employee lounges where a person may trust to have full privacy (point 53). Moreover, and which is really important for these considerations, secret surveillance should only be allowed, and then only on a temporary basis, if proven necessary because of lack of adequate alternatives (point 54). As regards shops, camera surveillance may be justified to protect the property, if such a measure has proven to be necessary and proportional. It may also be justified at certain locations

in the shop to prevent and prosecute robberies under threat but, again, only if proven necessary, and no longer than necessary, and national legislation will have to clearly define the legal basis of the surveillance and the necessity of the infringement in view of the interests protected (points 57-58). In the concluding remarks, the Venice Commission emphasized that video surveillance has to respect the requirements laid down by Article 8 of the Eur.Ct.H.R. and at least follow the requirements laid down by Directive 95/46/EC. Finally, people have to be notified of being surveyed unless the surveillance system is obvious. This means that the situation has to be such that the person observed may be assumed to be aware of the surveillance, or has unambiguously given his /her consent.

At the 1224th meeting of the Ministers' Deputies, the Committee of Ministers of the Council of Europe adopted Recommendation CM/Rec(2015)5 on the processing of personal data in the context of employment. In Article 10, this Recommendation provides:

> 10.1. Information concerning personal data held by employers should be made available either to the employee concerned directly or through the intermediary of his or her representatives, or brought to his or her notice through other appropriate means. 10.2. Employers should provide employees with the following information: the categories of personal data to be processed and a description of the purposes of the processing; the recipients, or categories of recipients of the personal data; the means employees have of exercising the rights set out in principle 11 of the present recommendation, without prejudice to more favourable ones provided by domestic law or in their legal system and any other information necessary to ensure fair and lawful processing.

It also provides that

> 15.1. the introduction and use of information systems and technologies for the direct and principal purpose of monitoring employees' activity and behaviour should not be permitted and where their introduction and use for other legitimate purposes, such as to protect production, health and safety or to ensure the efficient running of an organisation has for indirect consequence the possibility of monitoring employees' activity, it should be subject to the additional safeguards. 15.2. Information systems and technologies that indirectly monitor employees' activities and behaviour should be specifically designed and located so as not to undermine their

> fundamental rights. The use of video surveillance for monitoring locations that are part of the most personal area of life of employees is not permitted in any situation.

Further, employers should "inform employees before the introduction of information systems and technologies enabling the monitoring of their activities"; "take appropriate internal measures relating to the processing of that data and notify employees in advance"; "consult employees' representatives in accordance with domestic law or practice, before any monitoring system can be introduced or in circumstances where such monitoring may change" and "consult, in accordance with domestic law, the national supervisory authority on the processing of personal data" (Article 21 of the Recommendation).

As an independent EU advisory body, the Data Protection Working Party was established under Article 29 of Directive 95/46/EC in order to contribute to the uniform implementation of its provisions. According to its Opinion 8/2001, on the processing of personal data in an employment context, any monitoring must be a proportionate response by an employer to the risks it faces, taking into account the legitimate privacy and other interests of workers. Further, any monitoring must be carried out in the least intrusive way possible and workers must be informed of the existence of the surveillance, the purposes for which personal data are to be processed and other information necessary to guarantee fair processing. In Opinion no. 4/2004, the Data Protection Working Party pointed out that surveillance should not include premises that either are reserved for employees' private use or are not intended for the discharge of employment tasks – such as toilets, shower rooms, lockers and recreation areas; that the images collected exclusively to safeguard property and/or detect, prevent and control serious offences should not be used to charge an employee with minor disciplinary breaches; and that employees should always be allowed to lodge their counterclaims by using the contents of the images collected. The information must be given to employees and every other person working on the premises. This should include the identity of the controller and the purpose of the surveillance and other information necessary to guarantee fair processing in respect of the data subject.

3. VIDEO-SURVEILLANCE OF THE EMPLOYEE AND THE RIGHT TO PRIVACY

According to Article 8 of the Eur.Ct.H.R., every person "has the right to respect for his private and family life, his home and his correspondence". Additionally,

> 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.

Article 8 of the Eur.Ct.H.R. is therefore divided into four protected categories: private life, family life, home and correspondence. The concept of *private life* is a broad term, not suitable for exhaustive definitions, and essentially covering the physical and psychological integrity of a person. It can, therefore, encompass multiple aspects of the person's physical and social identity, as the Eur.Ct.H.R. stated in *Denisov v. Ukraine*.[19] In multiple judgments, the Eur.Ct.H.R. has dealt with the notion of private life, including issues related to personal identity, such as a person's name or image.[20] It should be noted that since 1992, the Eur.Ct.H.R. has gradually expanded the scope of coverage of Article 8 to other forms of interception of communications occurring in the workplace.[21] As Elena Sychenko emphasizes, cases on employee's privacy as adjudicated by the Eur.Ct.H.R. can be divided into two main groups - data protection, in which the Court deals with the legality of it being collected, used and disclosed; and the protection from interference with private life by activities such as workplace monitoring using video surveillance, searches of offices and equipment, and the interception of workplace telephone calls.[22] Video surveillance of the employees falls under the notion of Article 8 of the Eur.Ct.H.R. and under the right to privacy.[23] For these considerations, we will

[19] Denisov v. Ukraine, App. No. 76639/11, Eur.Ct.H.R. (2018).
[20] Schüssel v. Austria, App. No. 42409/98, Eur.Ct.H.R. (2002); Von Hannover v. Germany, App. No. 40660/08 and 60641/08, Eur.Ct.H.R. (2012).
[21] *See* Marta Otto, The Right to Privacy in Employment: A Comparative Analysis 76 (2016).
[22] Elena Sychenko, *International Protection of Employee's Privacy under the European Convention on Human Rights*, 67 Zbornik PFZ 757, 760 (2017).
[23] Some authors emphasize that many people feel that the negative effects of surveillance can be adequately countered by invoking the right to privacy, which has become one of the primary means of protection against surveillance and control. *See* Bart Willem Schermer, Software Agents, Surveillance, and the Right to Privacy: A Legislative Framework for Agent-Enabled Surveillance 71 (2007).

elaborate on three main judgments in this sphere: *Köpke v. Germany*,[24] *Bărbulescu v. Romania*[25] and *Antovic and Mirkovic v. Montenegro*.[26]

However, in the first place, we have to analyse the difference between positive and negative obligations in this sphere. It is very hard to draw clear boundaries around them and in contrast to negative obligations, positive obligations are not clear-cut.[27] The Eur.Ct.H.R. reiterated in *Palomo Sánchez and Others v. Spain*[28] that while the boundaries between the State's positive and negative obligations under the Eur.Ct.H.R. do not lend themselves to precise definition, the applicable principles are nonetheless similar, and in both contexts, regard must be had in particular to the fair balance that has to be struck between the competing private and public interests, subjected, in any event, to the margin of appreciation enjoyed by the State.[29] The video-surveillance measure in mentioned cases was imposed by the employers and cannot, therefore, be analysed as "interference", by State authority, with the exercise of Eur.Ct.H.R. rights. The applicants, nevertheless, took the view that the domestic courts had not effectively protected their right to respect for their private life. Although an object of Article 8 is essentially that of protecting the individual against arbitrary interference by 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 effective respect for private or family life.[30]

Positive obligations have been asserted by applicants in a wide range of contexts under the terms of this Article, and many of them have been upheld by the Eur.Ct.H.R..[31] The Eur.Ct.H.R. has held that in certain circumstances, the State's positive obligations under Article 8 of the Eur.Ct.H.R. are not adequately fulfilled unless it secures respect for private life in the relations between individuals by setting up a legislative framework taking into consideration the various interests to be protected in a particular context.

[24] Köpke v. Germany, App. No. 420/07, Eur.Ct.H.R. (2006).
[25] Bărbulescu v. Romania, App. No. 61496/08, Eur.Ct.H.R. (2017).
[26] Antović and Mirković v. Montenegro, App. No. 70838/13, Eur.Ct.H.R. (2017).
[27] *See* Marie-Bénédicte Dembour, Who Believes in Human Rights? Reflections on the European Convention 87 (2006).
[28] *See also* Sánchez v. Spain, App. No. 28955/06, 28957/06, 28959/06 and 28964/06, Eur.Ct.H.R. (2011). Similarly, *see* Nunez v. Norway, App. No. 55597/09, Eur.Ct.H.R. (2011); Dickson v. The United Kingdom, App. No. 44362/04, Eur.Ct.H.R. (2007).
[29] Sánchez v. Spain, App. No. 28955/06, 28957/06, 28959/06 and 28964/06, Eur.Ct.H.R. (2011). The fair balance test originates from Rees v. The United Kingdom, App. No. 9532/81, Eur.Ct.H.R. (1986) and it is followed in numerous judgments. *See* Dimitris Xenos, The Positive Obligations of the State under the European Convention of Human Rights 59 (2012); Steven Greer, The European Convention on Human Rights: Achievements, Problems and Prospects 264 (2006).
[30] Ribalda v. Spain, App. No. 1874/13 and 8567/13, Eur.Ct.H.R. (2019).
[31] Alastair Mowbray, The Development of Positive Obligations Under the European Convention on Human Rights by the European Court of Human Rights 127 (2004).

The similar approach was displayed by the Eur.Ct.H.R. in *X and Y v. the Netherlands*[32], *M.C. v. Bulgaria*,[33], *K.U. v. Finland*[34] *Söderman v. Sweden*,[35] and *Codarcea v. Romania*.[36] Those protective measures are not only to be found in labour law, but also in civil and criminal law. As far as labour law is concerned, it must ascertain whether the respondent State was required to set up a legislative framework to protect the applicant's right to respect for his private life and correspondence in the context of his professional relationship with a private employer.[37]

In *Köpke v. Germany*[38], Eur.Ct.H.R. elaborated on the compliance of the video surveillance of the employee with Article 8. In *Köpke*, a video recording of the applicant's conduct at her workplace was made without prior notice on the instruction of her employer. The picture material obtained thereby was processed and examined by several persons working for her employer and was used in the public proceedings before the labour courts. Through this decision, the Eur.Ct.H.R. developed a balance between the human right to respect for the applicant's private life and both her employer's interest in the protection of his property rights, guaranteed by Article 1 of Protocol no. 1 to the Eur.Ct.H.R., and the public interest in the proper administration of justice. It is not disputable that the employee has a right to private life. However, the employer, on the other hand, had a considerable interest in the protection of his property rights under Article 1 of Protocol no. 1.[39] In the end, we have to emphasize that video surveillance by an employer in order to detect theft by employees was held to infringe Article 8(1),

[32] X and Y v. the Netherlands, App. No. 8978/80, Eur.Ct.H.R. (1985).
[33] M.C. v. Bulgaria, App. No. 39272/98, Eur.Ct.H.R. (2003).
[34] K.U. v. Finland, App. No. 2872/02, Eur.Ct.H.R. (2008).
[35] Söderman v. Sweden, App. No. 5786/08, Eur.Ct.H.R. (2013).
[36] Codarcea v. Romania, App. No. 31675/04, Eur.Ct.H.R. (2009).
[37] Bărbulescu v. Romania, App. No. 61496/08, Eur.Ct.H.R. (2017).
[38] In Köpke v. Germany, App. No. 420/07, Eur.Ct.H.R. (2006), the applicant's employer noted in September 2002 that

> there were irregularities concerning the accounts in the drinks department of that supermarket, in that the sum of the till receipts for empty deposit bottles, which had been printed out, exceeded the total value of empty deposit bottles received by the supermarket. It suspected the applicant and another employee of having manipulated the accounts. Between 7 October 2002 and 19 October 2002 the applicant's employer, with the help of a detective agency, carried out covert video surveillance of the supermarket's drinks department. The camera covered the area behind the cash desk including the till, the cashier and the area immediately surrounding the cash desk. The detective agency made a video and examined the data obtained. It drew up a written report and produced several photos from the recording, which it sent to the applicant's employer together with two copies of the video (one concerning the applicant and one concerning the other employee monitored). On 5 November 2002, the applicant's employer dismissed the applicant without notice for theft. The applicant was accused of having manipulated the accounts in the drinks department of the supermarket and of having taken money (some 100 Euros during the period in which she had been filmed) from the tills for herself, which she had hidden in her clothes.

[39] *See* Köpke v. Germany, App. No. 420/07, Eur.Ct.H.R. (2006).

although the Eur.Ct.H.R. considered that it struck an appropriate balance, bearing in mind the rights of the employer and the probability of success in catching a dishonest worker. However, in rejecting the application, the Eur.Ct.H.R. said that this "might well be given a different weight in the future, having regard to the extent to which intrusions into private life are made possible by new, more and more sophisticated technologies".[40]

Bărbulescu judgment is directed towards the monitoring of the employees' communications.[41] In this case, the Eur.Ct.H.R. narrowed[42] its inquiry to the question "how the domestic courts to which the applicant applied dealt with his complaint of infringement by the employer of his right to respect for private life and correspondence in an employment context". In this case, the applicant was not informed in advance of the extent and nature of his employer's monitoring activities, or of the possibility that the employer might have access to the actual content of his messages. The warning from the employer must be given before the monitoring activities are initiated, especially where they also entail accessing the contents of employees' communications, and international and European standards point in this direction, requiring the data subject to be informed before any monitoring activities are carried out.[43] Therefore, there was a violation of Article 8.[44]

In *Antovic and Mirkovic v. Montenegro*, the Eur.Ct.H.R. dealt with a very specific issue nowadays[45] and in the first place, emphasized that video surveillance of an employee in

[40] Id.; William A. Schabas, The European Convention on Human Rights: A Commentary 377 (2015).

[41] The applicant in this case was employed in the Bucharest office of a Romanian private company, as a sales engineer. At his employer's request, for the purpose of responding to customers' enquiries, he created an instant messaging account using *Yahoo Messenger*, an online chat service offering real-time text transmission over the internet. It is important to note that he already had another personal *Yahoo Messenger* account. The applicant was summoned by his employer to give an explanation about the fact that he had used the internet for personal purposes, in breach of the internal regulations. The employer submitted a transcript of the messages, which the applicant had exchanged with his brother and his fiancée during the period when he had been monitored; the messages related to personal matters and some were of an intimate nature. The transcript also included five messages that the applicant had exchanged with his fiancée using his personal *Yahoo Messenger* account; these messages did not contain any intimate information (*see* Bărbulescu v. Romania, App. No. 61496/08, Eur.Ct.H.R. (2017).). *See* further: Veronika Szeghalmi, *Private Messages at Work - Strasbourg Court of Human Right's Judgement in Barbulescu v. Romania Case,* 2016 Hungarian Y.B. Int'l L. & Eur. L. 293; Johannes Eichenhofer, *Internet Privacy at Work - the Eur.Ct.H.R. Bărbulescu Judgment*, 2 Eur. Data Prot. L. Rev. 266 (2016). This is a very important judgment, because the Eur.Ct.H.R. set out clear requirements for how domestic legal systems should protect the right to private life in the context of workplace monitoring. See Joe Atkinson, *Workplace Monitoring and the Right to Private Life at Work*, 81 Mod. L. Rev. 688, 693 (2018).

[42] It is unjustifiably, according to the Joint dissenting opinion of judges Raimondi, Dedov, Kjølbro, Mits, Mourou-Vikström and Eicke.

[43] Bărbulescu v. Romania, App. No. 61496/08, Eur.Ct.H.R. (2017).

[44] Case *Libert v. France* is similar, but in the same time different, because the interference was by a public authority and consequently, the complaint was analysed from the angle not of the State's positive obligations, as in the case of *Bărbulescu v. Romania*, but of its negative obligations. Libert v. France, App. no. 588/13, Eur.Ct.H.R. (2018). *See* more in Sebastian Klein, *Libert v. France: Eur.Ct.H.R. on the Protection of an Employee's Privacy Concerning Files on a Work Computer*, 4 Eur. Data Prot. L. Rev. 250 (2018).

[45] In this case, the Dean of the School of Mathematics of the University of Montenegro, at a session of the School's council, informed the professors teaching there, including the applicants, that video surveillance

the workplace, be it covert or not, must be considered as a considerable intrusion into the employee's private life and constitutes an interference within the meaning of Article 8.[46] Video surveillance was introduced in the present case to ensure the safety of property and people, including students, and for the surveillance of teaching. It was noted that the law at all as a ground for video surveillance did not provide for one of those aims, notably the surveillance of teaching. Furthermore, there was no evidence that either property or people had been in jeopardy, one of the reasons to justify the introduction of video surveillance.[47] Accordingly, there was a violation of Article 8 of the Eur.Ct.H.R..[48] Because of the sensitive nature of this problem, there were opposing arguments.[49] We consider, however, that the opinion of the majority was more persuasive.[50]

---

has been introduced and that it was in the auditoriums where classes were held. He issued a decision introducing video surveillance in seven amphitheatres and in front of the Dean's Office that specified that the aim of the measure was to ensure the safety of property and people, including students, and the surveillance of teaching. The decision stated that access to the data that was collected was protected by codes, which were known only to the Dean. The data were to be stored for a year.

[46] Antović and Mirković v. Montenegro, App. No. 70838/13, Eur.Ct.H.R. (2017).

[47] *Id.* at § 59.

[48] *See e.g.,* Judges Vučinić and Lemmens in their Concurring opinion in a different way describe a relationship in classroom between professor and students:

> These interactions are of course not of a purely social nature. The setting is a very specific one. The teacher teaches students who are enrolled in his or her class. The relationship between teacher and students takes shape during the whole period of teaching (a year or a semester). In the auditorium the teacher can allow him- or herself to act ("perform") in a way he or she would perhaps never do outside the classroom. It seems to us that in such an interaction the teacher may have an expectation of privacy, in the sense that he or she may normally expect that what is going on in the classroom can be followed only by those who are entitled to attend the class and who actually attend it. No "unwanted attention" from others, who have nothing to do with the class. There may be exceptions, for instance when a lecture is taped for educational purposes, including for use by students who were unable to physically attend the class. However, in the applicants' case there was no such purpose. It seems to us that at least in an academic environment, where both the teaching and the learning activities are covered by academic freedom, the said expectation of privacy can be considered a "reasonable" one. Surveillance as a measure of control by the dean is, in our opinion, not something a teacher should normally expect.

However, they believe that video surveillance in an auditorium is possible, but, this means, among other things, that there must be a proper legal basis, that the scope of the surveillance must be limited, and that there are guarantees against abuse.

[49] In the view of the judges Spano, Bianku and Kjølbro, the university's video monitoring in the auditorium where the applicants were teaching as professors did not raise an issue as regards the applicants' private life. They believe it conclusive that the video monitoring took place at the university auditoriums, that the applicants had been notified of the video surveillance, that what was monitored was the applicants' professional activity, that the surveillance was remote, that there was no audio recording and thus no recording of the teaching or discussions, that the pictures were blurred and the persons could not easily be recognised, that the video recordings were only accessible to the dean and were automatically deleted after 30 days, and that the data or information was not subsequently used (Joint dissenting opinion of Judges Spano, Bianku and Kjølbro in Antović and Mirković v. Montenegro, App. No. 70838/13 (Nov. 28, 2017), http://hudoc.echr.coe.int/eng?i=001-178904).

[50] See more in Milica Kovač-Orlandić, *Video Surveillance in the Employer's Premises: The Eur.Ct.H.R. Judgment in Antović and Mirković v. Montenegro*, Collection Papers Fac. L. Niš, no. 82, at 165 (2019).

From the above, we can conclude that Article 8 leaves it to the discretion of the States to decide whether or not to enact a specific legislation on video surveillance or the monitoring of the non–professional correspondence and other communications of employees. Nevertheless, as the Eur.Ct.H.R. pointed out, regardless of the discretion enjoyed by States in choosing the most appropriate means for the protection of the rights in question, the domestic authorities should ensure that the introduction, by an employer, of monitoring measures affecting the right to respect for private life or correspondence of employees, is proportionate and is accompanied by adequate and sufficient safeguards against abuse.[51]

Since *Köpke* through *Bărbulescu*, the Eur.Ct.H.R. developed key principles in this sphere. These criteria must be applied while taking into account the specificity of the employment relations and the development of new technologies, which may enable measures to be taken that are increasingly intrusive in the private life of employees.[52] In that context, in order to ensure the proportionality of video-surveillance measures in the workplace, the domestic courts should take account of the following factors when they weigh up various competing interests:

> (i) Whether the employee has been notified of the possibility of video-surveillance measures being adopted by the employer and of the implementation of such measures. While in practice employees may be notified in various ways, depending on the particular factual circumstances of each case, the notification should normally be clear about the nature of the monitoring and be given prior to implementation.
>
> (ii) The extent of the monitoring by the employer and the degree of intrusion into the employee's privacy. In this connection, the level of privacy in the area being monitored should be taken into account, together with any limitations in time and space and the number of people who have access to the results.
>
> (iii) Whether the employer has provided legitimate reasons to justify monitoring and the extent thereof. The more intrusive the monitoring, the weightier the justification that will be required.
>
> (iv) Whether it would have been possible to set up a monitoring system based on less intrusive methods and measures. In this connection, there should be an assessment in the light of the particular circumstances of each case as to whether the aim pursued by the employer could have been achieved through a lesser degree of interference with the employee's privacy.

[51] *See* Köpke v. Germany, App. No. 420/07, Eur.Ct.H.R. (2006); Bărbulescu v. Romania, App. No. 61496/08, Eur.Ct.H.R. (2017).
[52] *See* Ribalda v. Spain, App. No. 1874/13 and 8567/13, Eur.Ct.H.R. (2019).

> (v) The consequences of the monitoring for the employee subjected to it. Account should be taken, in particular, of the use made by the employer of the results of the monitoring and whether such results have been used to achieve the stated aim of the measure.
>
> (vi) Whether the employee has been provided with appropriate safeguards, especially where the employer's monitoring operations are of an intrusive nature. Such safeguards may take the form, among others, of the provision of information to the employees concerned or the staff representatives as to the installation and extent of the monitoring, a declaration of such a measure to an independent body or the possibility of making a complaint.[53]

Following the above principles, national courts should conclude whether video surveillance over the employees is in accordance with the Eur.Ct.H.R. or not. More precisely, the positive obligations imposed on the State by Article 8 of the Eur.Ct.H.R. required the national authorities to strike a fair balance between two competing interests, on the one hand, the applicants' right to respect for their private life and, on the other, the possibility for their employer to ensure the protection of his property and the smooth operation of his company, particularly by exercising his disciplinary authority.[54]

Therefore, in *López Ribalda and Others v. Spain*, the domestic courts first found that the installation of the video-surveillance had been justified by legitimate reasons, namely the suspicion put forward by the supermarket manager because of the significant losses recorded over several months, suggesting that thefts had been committed. They also took into account the employer's legitimate interest in taking measures in order to discover and punish those responsible for the losses, with the aim of ensuring the protection of his property and the smooth functioning of the company. The domestic courts then examined the extent of the monitoring and the degree of intrusion into the applicants' privacy, finding that the measure was limited as regards the areas and staff being monitored – since the cameras only covered the checkout area, which was likely to be where the losses occurred – and that its duration had not exceeded what was necessary in order to confirm the suspicions of theft. Further, as regards the extent of the measure over time, video-surveillance lasted for ten days and ceased as soon as the responsible employees had been identified. The length of the

[53] *Id.*; Bărbulescu v. Romania, App. No. 61496/08, Eur.Ct.H.R. (2017), http://hudoc.echr.coe.int/eng?i=001-177082. *See* Caroline Calomme, *Monitoring of Employees' Communications: Eur.Ct.H.R. Spells Out Positive Obligations to Protect Employees' Privacy*, 3 Eur. Data Prot. L. Rev. 545, 547 (2017); Monica Gheorghe, *Considerations on the Conditions under Which the Employer May Monitor their Employees at the Workplace*, 7 Jurid. Trib., no. 2, at 62, 67 (2017).

[54] *See e.g.,* Ribalda v. Spain, App. No. 1874/13 and 8567/13, Eur.Ct.H.R. (2019).

monitoring does not, therefore, appear excessive in itself.[55] The employer did not use the video-surveillance and recordings for any purposes other than to trace those responsible for the recorded losses of goods and to take disciplinary measures against them. Then, the Eur.Ct.H.R. noted that the extent of the losses identified by the employer suggested that thefts had been committed by a number of individuals and the provision of information to any staff member might well have defeated the purpose of the video surveillance, which was to discover those responsible for the thefts but also to obtain evidence for use in disciplinary proceedings against them.[56]

We can therefore conclude that the disclosure of information regarding video surveillance is of great importance. In this case, the applicants had been informed of the installation of video surveillance. It was not disputed that two types of cameras had been installed in the supermarket where they worked: the visible cameras directed towards the shop's entrances and exits, of which the employer had informed the staff, and the hidden cameras directed towards the checkout area, of which neither the applicants nor the other staff members had been informed. The Eur.Ct.H.R. emphasized that while both the Spanish law and the relevant international and European standards do not seem to require prior consent of individuals who are placed under video surveillance, or more generally, of individuals who have their personal data collected, those rules still establish that it is, in principle, necessary to inform the individuals concerned, clearly and before the implementation of such systems, of the existence and conditions of such data collection, even if only in a general manner. The disclosure of information to the individual being monitored constitutes just one of the criteria to be taken into account in assessing the proportionality of such measures.[57] Therefore, under those circumstances, with regard to the weight of considerations justifying video surveillance, the Eur.Ct.H.R. concluded that the national authorities did not fail to fulfil their positive obligations under Article 8 of the Eur.Ct.H.R. such as to overstep their margin of appreciation. Accordingly, there has been no violation of that provision.

[55] *See* In *Köpke*, the duration of fourteen days was not found to be disproportionate. *See* Köpke v. Germany, App. No. 420/07, Eur.Ct.H.R. (2006).
[56] *See e.g.,* Ribalda v. Spain, App. No. 1874/13 and 8567/13, Eur.Ct.H.R. (2019).
[57] *Id.* at § 131.

4. WHETHER THE VIDEO-SURVEILLANCE OF THE EMPLOYEE IS ILLEGALLY OBTAINED EVIDENCE?

In *López Ribalda and Others*, the applicants further complained that recordings obtained in breach of their right to respect for their private life had been admitted and used as evidence by employment courts. Although this was a labour case, it opened an issue of illegally obtained evidence significant for criminal legal theory and practice. Academic workers around the world have long debated the normative and empirical arguments related to the admissibility of improperly obtained evidence.[58] Ölçer states that, while many national models for evidence exclusion can be clearly qualified as transplants from United States law[59], the same cannot be said of the Eur.Ct.H.R. model. Usually, the judge conducting a criminal trial has the power to exclude evidence obtained by unlawful or otherwise wrongful means, while legal systems have adopted different rationales for exclusion, resulting in variations in the scope of exclusionary power.[60] According to Article 6 of the Eur.Ct.H.R., everyone is entitled to a fair trial by an impartial tribunal in the determination of his civil rights and obligations or any criminal charge against him. As is well known, Article 6 guarantees the right to a fair trial[61], which is a recognisable feature of every significant international normative instrument charged with protecting human rights.[62] One of the areas of criminal procedure in which the Eur.Ct.H.R. has become quite active is rules regarding the admission and / or exclusion of illegally obtained evidence.[63] However, in numerous judgments, the Eur.Ct.H.R. repeated that this article does not lay down any rules on the admissibility of evidence as such, since this is primarily a matter of regulation under national law.[64]

---

[58] *See* Andrew Ashworth, *The Exclusion of Evidence Obtained by Violating a Fundamental Right: Pragmatism Before Principle in the Strasbourg Jurisprudence, in* Criminal Evidence and Human Rights: Reimagining Common Law Procedural Traditions 145 (Paul Roberts & Jill Hunter eds., 2012).

[59] *See* Stephen C. Thaman, *'Fruits of the Poisonous Tree' in Comparative Law*, 16 Sw. J. Int'l L. 333 (2010). For example, Thaman points out that the notion that evidence obtained as a result of police violation of the constitution could not be used in a criminal trial was finally established nationwide and made applicable to the states during the years that Earl Warren was Chief Justice of the US Supreme Court. *See* Stephen C. Thaman, *Balancing Truth Against Human Rights: A Theory of Modern Exclusionary Rules*, in Exclusionary Rules in Comparative Law 407 (Stephen C. Thaman ed., 2013).

[60] *See generally* Hock Lai Ho, *The Fair Trial Rationale for Excluding Wrongfully Obtained Evidence*, in Do Exclusionary Rules Ensure a Fair Trial? A Comparative Perspective on Evidentiary Rules 283 (Sabine Gless & Thomas Richter eds., 2019).

[61] In numerous judgments the Eur.Ct.H.R. often uses a standard phrase to stress the importance of the right to a fair trial: 'The right to a fair trial holds so prominently a place in a democratic society that there can be no justification for interpreting the guarantees of Article 6 of the Convention restrictively' (see more in Stefan Trechsel, Human Rights in Criminal Proceedings 82 (2005).

[62] *See e.g.,* Sarah Summers, Fair Trials: The European Criminal Procedural Tradition and the European Court of Human Rights 97 (2007).

[63] *See* Pinar Ölçer, *The European Court of Human Rights: The Fair Trial Analysis under Article 6 of the European Convention of Human Rights*, *in* Exclusionary Rules in Comparative Law 372 (Stephen C. Thaman ed., 2013).

[64] *See e.g.*, Schenk v. Switzerland, App. No. 00010862/84, Eur.Ct.H.R. (1988) *See also* Ruiz v. Spain, App. No. 30544/96, Eur.Ct.H.R. (1999).

Accordingly, in *Bochan v. Ukraine (N.2)*[65] the Eur.Ct.H.R. emphasized that issues such as the weight attached by the national courts to given items of evidence or findings or assessments in an issue before them for consideration are not for it to review, and that the Eur.Ct.H.R. should not act as a court of the fourth instance, and will not, therefore, question the judgment of national courts under Article 6, unless their findings can be regarded as arbitrary or manifestly unreasonable. In other words, we can see that the admissibility of evidence is primarily governed by the rules of the domestic law, so it often remains difficult to conclude from the Eur.Ct.H.R.'s decisions whether the use of illegally obtained evidence constitutes a violation.[66]

However, it is not the role of the Eur.Ct.H.R. to determine whether particular types of evidence may be admissible. The Eur.Ct.H.R. has to answer the question whether the proceedings as a whole, including the way in which the evidence was obtained, were fair, and this involves an examination of the unlawfulness in question and, where the violation of another Eur.Ct.H.R. right is concerned, the nature of the violation found. In other words, as Ho pointed out, under Strasbourg jurisprudence, the question raised by unlawfully obtained evidence is not whether the domestic court should have excluded it as such; it is whether, in the light of all relevant factors, the use or admission of the evidence in the domestic proceedings rendered it unfair as a whole and hence in contravention of Article 6.[67] A domestic court must always make a thorough assessment as to whether or not the means by which particular evidence has been obtained would render unfair its use in the trial which it is conducting. After *Khan v. The United Kingdom*[68], there is a consideration that so long as the defendant has the possibility of challenging the authenticity of the evidence, and so long as the trial court has the discretion to exclude unfair evidence, the requirements of Article 6 may be considered satisfied.[69] This is a very disputable understanding of the concept of fair trial.[70] This

[65] Bochan v. Ukraine, App. No. 22251/08, Eur.Ct.H.R. (2015).

[66] *See generally* Laurens van Puyenbroeck & Gert Vermeulen, *Towards Minimum Procedural Guarantees for the Defence in Criminal Proceedings in the EU*, 60 Int'l & Compar. L. Q. 1017, 1019 (2011).

[67] *See* Ho, *supra* note 61, at 287.

[68] *See generally* Khan v. The United Kingdom, App. No. 35394/97, Eur.Ct.H.R. (2000).

[69] *See* Ashworth, *supra* note 58, at 156.

[70] Here, we can agree with the judge Loucaides, who argued in his dissent opinion that such reasoning defies the structure of the Eur.Ct.H.R.: " I cannot accept that a trial can be fair, as required by Article 6 if a person's guilt for any offence is established through evidence obtained in breach of the human rights guaranteed by the Convention ". Judge Tulkens confirmed such understanding in his dissenting opinion in P.G. and J.H. v. The United Kingdom (no. 44787/98), Eur.Ct.H.R. § 76 (2001), where he stated:

> I do not think that a trial can be described as "fair " where evidence obtained in breach of a fundamental right guaranteed by the Convention has been admitted during that trial. As the Court has already had occasion to stress, the Convention must be interpreted as a coherent whole . . . . In concluding that there has not been a violation of Article 6, the Court renders Article 8 completely ineffective.

attitude is already grounded in *P.G. and J.H. v. The United Kingdom* and *Gäfgen v. Germany*.[71] While the use of evidence secured as a result of a measure found to be in breach of Article 3 always raises serious issues as to the fairness of the proceedings, it is important to answer the question of whether the use as evidence of information obtained in violation of Article 8 or domestic law rendered the trial unfair as a whole, contrary to Article 6; this has to be determined with regard to all the circumstances of the case, including respect for the applicant's defence rights and the quality and importance of the evidence in question. In particular, it must be examined whether the applicant was given an opportunity to challenge the authenticity of the evidence and to oppose its use. At this point, it is important to emphasize that Article 6(1), in conjunction with Article 3, requires all member states to adopt the categorical rule that evidence obtained by torture is inadmissible and cannot be used as proof of guilt in legal proceedings, but the Eur.Ct.H.R. has not adopted a similar categorical rule of exclusion for other types of unlawfully obtained evidence, such as evidence obtained by means that contravene the right of privacy in Article 8. It's also important to note that the Eur.Ct.H.R. has adopted the position that the use of illegally obtained evidence, particularly evidence obtained in violation of Article 8, which guarantees the right to respect for private life, does not necessarily lead to unfair proceedings.[72]

The quality of the evidence must be taken into consideration, as must the question of whether the circumstances in which it was obtained cast doubt on its reliability or accuracy.[73] The fact that is important for this consideration is that the principles concerning the admissibility of evidence were developed in the context of criminal law, although the Eur.Ct.H.R. applied them in a case concerning the fairness of civil proceedings.[74] The Eur.Ct.H.R. observed that, while the *fair trial* guarantees are not necessarily the same in criminal law and civil law proceedings, the States having greater latitude when dealing with civil cases, it may nevertheless draw inspiration, when examining the fairness of civil law proceedings, from the principles developed under the criminal limb of Article 6.[75] Thus, in *López Ribalda and Others v. Spain*, the Eur.Ct.H.R. took the view that the principles in question are applicable to its examination of the fairness of civil proceedings in the matter at hand.

[71] *See* P.G. and J.H. v. The United Kingdom, App. No. 44787/98, Eur.Ct.H.R. (2001); *see also* Gäfgen v. Germany, App. No. 22978/05, Eur.Ct.H.R. (2010).
[72] *See* Opinion of the EU Network of Independent Experts on Fundamental Rights on the "*Status of Illegally Obtained Evidence in Criminal Procedures in the Member States of the European Union*", 2003 6.
[73] *E.g.*, Ribalda v. Spain, App. No.1874/13 and 8567/13, Eur.Ct.H.R. (2019); Schenk v. Switzerland, App. No. 00010862/84, Eur.Ct.H.R. (1988); P.G. and J.H. v. The United Kingdom, App. No. 44787/98, Eur.Ct.H.R. (2001); Gafgen v. Germanya, App. No. 22978/05, Eur.Ct.H.R. (2010).
[74] *See* Vukota-Bojić v. Switzerland, App. No. 61838/10, Eur.Ct.H.R. (2016).
[75] *See* Saliba v. Malta, App. No. 24221/13, Eur.Ct.H.R. (2016).

Essentially, the Eur.Ct.H.R. had to examine whether the use as evidence of the images obtained through video surveillance undermined the fairness of the proceedings as a whole.[76] The applicants did indeed have access to the recordings obtained using video surveillance and were able to contest their authenticity and oppose their use as evidence, but they did not at any time dispute the authenticity or accuracy of the footage recorded by means of video surveillance. Their main complaint was based on the lack of prior information about the installation of the cameras. Furthermore, the images obtained from the video surveillance system were not the only items of evidence in their case. Consequently, the Eur.Ct.H.R. took the view that the use as evidence of the images obtained by video surveillance did not undermine the fairness of the proceedings in the present case.[77]

The Eur.Ct.H.R.'s approach to the use of evidence obtained by a violation of Article 8 of the Eur.Ct.H.R. has been much criticized.[78] For the purpose of these examinations, we can conclude that, from a certain point of view, the admissibility of video surveillance evidence depends on the existence of a violation of Article 8. In this case, the applicants realistically had very low odds to succeed in their demand. At the very moment when the Eur.Ct.H.R. finds that video surveillance did not violate the right to privacy, the footage obtained by it becomes admissible as evidence. This is even more true when we analyse the issue of the fairness of the proceedings as a whole. The problem arises in situations where the Eur.Ct.H.R. determines that there has been a violation of Article 8, but not of Article 6 related to evidence obtained in violation of Article 8. Therefore, the Eur.Ct.H.R.

[76] We should note that the Court in Beuze v. Belgium, App. no. 71409/10, Eur.Ct.H.R. (2018) enumerated the non-exhaustive list of factors that should, when it is appropriate, be taken into account:

> (a) [W]hether the applicant was particularly vulnerable, for example by reason of age or mental capacity; (b) the legal framework governing the pre-trial proceedings and the admissibility of evidence at trial, and whether it was complied with – where an exclusionary rule applied, it is particularly unlikely that the proceedings as a whole would be considered unfair; (c) whether the applicant had the opportunity to challenge the authenticity of the evidence and oppose its use; (d) the quality of the evidence and whether the circumstances in which it was obtained cast doubt on its reliability or accuracy, taking into account the degree and nature of any compulsion; (e) where evidence was obtained unlawfully, the unlawfulness in question and, where it stems from a violation of another Convention Article, the nature of the violation found; (f) in the case of a statement, the nature of the statement and whether it was promptly retracted or modified; (g) the use to which the evidence was put, and in particular whether the evidence formed an integral or significant part of the probative evidence upon which the conviction was based, and the strength of the other evidence in the case; (h) whether the assessment of guilt was performed by professional judges or lay magistrates, or by lay jurors, and the content of any directions or guidance given to the latter; (i) the weight of the public interest in the investigation and punishment of the particular offence in issue; and (j) other relevant procedural safeguards afforded by domestic law and practice.

[77] *See* Ribalda v. Spain, App. No. 1874/13 and 8567/13, Eur.Ct.H.R. (2019).

[78] *See* KellyPitcher, Judicial Responses to Pre-Trial Procedural Violations in International Criminal Proceedings 444 (2018).

has to establish a stronger connection between these two articles, as it did between Article 3 and Article 6. Essentially, the author agrees with the judges Loucaides and Tulkens in their opinion that a trial cannot be fair if a person's guilt for any offence is established through evidence obtained in breach of the human rights guaranteed by the Eur.Ct.H.R..[79]

CONCLUSION

The video surveillance system is rightfully considered a powerful tool for fighting crime and for protection of property from theft. However, this is still a sensitive matter. From the perspective of human rights, this kind of surveillance does violate them to a certain degree. A balance must be established between the loss of privacy and the seriousness of threats that the system is installed to mitigate. This is the balance between the right to private life and the right to property. As stated above, it is indisputable that video surveillance of employees is a very sensitive matter. In this sense, the author agrees with the judges De Gaetano, Yudkivska and Grozev, who believe that the question of which alternative measures could have been used by the employer to pursue their legitimate aim – measures which would simultaneously have had a less invasive impact on the employees' right to respect for their private life – had to be taken into consideration. Accordingly, there is a danger of encouraging individuals to take legal matters into their own hands. Therefore, since *Köpke*, through *Bărbulescu*, to *López Ribalda and Others*, the judgments of the Eur.Ct.H.R. continue to develop key principles in this sphere, which must be applied with regard to the specific nature of employment relations and the development of new technologies. In the matter of evidence obtained by violations of the right to privacy, the author believes that, in the future, the decisions of the Eur.Ct.H.R. will have to establish the same criteria for the relationship between Article 8 and Article 6 as they did for the conjunction between Article 3 and Article 6. This judgment could be a step forward in that direction, but this does indeed depend on the interpretation. Nevertheless, we still have to take into consideration the interests of

[79] When we speak on inadmissible evidence, it is important to give the Ashworts's explanation:

> [T]he Court's prevailing view seems to be that violations of Article 8 and the requirements of Article 6 are two entirely separate matters. The appropriate way to deal with Article 8 breaches is to provide a remedy to the person whose right was infringed, a remedy that might be found in an award of damages or perhaps a reduction in sentence. But the criminal trial is something separate, with its own fairness criteria, and the questionable provenance of the prosecution's evidence will not compromise trial fairness just because other substantive human rights have been breached.

See generally Ashworth, *supra* note 58, at 157.

employers towards the protection of their property. While the balance between the protection of property and the right to privacy is not easily achieved, the author believes that the Eur.Ct.H.R. took the right attitude in this case.