HUNGARIAN LABOUR LAW
E - J O U R N A L

# Distant employees' control technologies: legal issues

**Elena Sychenko***

The right to supervise the employees' activities at work is an inherent right of an employer acknowledged by any national labour law. The fast digitalization of work processes and the spread of distant work in and after – the Covid era were the reasons for the development of a number of programs to control the working time and activities of employees. Some of these technologies permit video recording of the working place through the webcam installed in the computer, some –provide a "live view of screens of all remote computers like a surveillance camera"[1], others - check the movements of the mouse, make screenshots, monitor the emails and the use of the internet[2]. According to Eurofound, the COVID-19 crisis has expanded the market for surveillance technologies and accelerated their uptake: employee monitoring software companies such as Sneek and Teramind reportedly increased their sales during the pandemic.[3] Eurofound also noted the facts of using a facial recognition tool that logs when employees are away from their computer screens.[4] Leading multinationals such as IBM, Unilever, Microsoft, and Softbank, as scholars found out, were using emotional analytics to monitor employees for engagement, productivity and compliance.[5]

An employee has to accept the use of those programs otherwise the contract will not be concluded. In some jurisdictions, it is enough to notify an employee, in others - such software is often installed without informing an employee. Some digital surveillance tools are publicized by the producers as

* PhD, associate professor, Saint Petersburg State University; visiting professor, University of Trento.

1 https://www.softactivity.com/get/employee-monitoring/?gclid=Cj0KCQiA_bieBhDSARIsADU4zLf4Su4GHEYihQOgo2aL4VAaoUPAhdpVVu0yCKvzPj23aziMkVL2ayEaAtyIEALw_wcB

2 See, for example, Time Doctor, Toggl, RescueTime, Hours, Timely, Harvest, Everhour, Timeneye, ClickTime and TopTracker. Available at: https://www.timedoctor.com/blog/remote-employee-software/

3 Monitoring and surveillance of workers in the digital age. Eurofound, 15 December 2021. https://www.eurofound.europa.eu/data/digitalisation/research-digests/monitoring-and-surveillance-of-workers-in-the-digital-age

4 Ibid.

5 Franci Suni Lopez – Nelly Condori-Fernandez –, Alejandro Catala: Towards real-time automatic stress detection for office workplaces. In: Juan Antonio Lossio-Ventura – Denisse Muñante – Hugo Alatrista-Salas (eds.): *Information Management and Big Data. SIMBig 2018.* Cham, Springer, 2019. 273–288.; cited from Peter Mantello – Manh-Tung Ho: Emotional AI and the future of wellbeing in the post-pandemic workplace. *AI & society,* 2023. 1–7.

"secret" or "spy" programs, which permit to record all the employee's activities without being noticed.[6] The mere existence of such programs means that employees may never be sure that an employer is not using this software. It's needless to say that this fact creates additional stress at the workplace. It has been also demonstrated in a number researches that open digital monitoring has a detrimental impact on the psychological health of employees.[7] As was noted by Shelley Wallach already in 2002, by our very human nature, we are not psychologically equipped to deal with such an invasion of our privacy.[8]

At the same time, digital surveillance might have a positive impact on the organization of work, on discipline, on detection of legally non-compliant or dangerous employee behaviours. For example, sentiment analysis tools have been used to detect sexual harassment in employee communications and insider threat; smart digital cameras and semantic analysis have been used to manage construction safety by identifying a wide range of unsafe behaviours, including health and safety violations or failure to follow operational procedures.[9] It is evident that with the digitalization of more and more facets of our life and of human interaction, the use of digital tools for surveillance is inevitable. The market for such software will be growing as digital tools are becoming the key ones for controlling the work performance of all employees, especially distant ones. Therefore, there is a need to understand if there is a legal mechanism that ensures the due balance between the employer's rights and the right of employees to privacy. In this paper I will attempt to establish the limits of normal employer's supervision, distinguishing it from human rights abuses, and formulating the criteria to which any remote-control program should correspond.

The paper will first consider a number of national cases where employers used special technologies to control employees and reveal the legal problems which might arise in this field. Provided the fact that the surveillance is a huge challenge for the right to privacy, which is recognized in the European Convention of Human Rights (art. 8 of the ECHR), the approach of the European Court of Human Rights (ECtHR) to workplace surveillance might be considered a benchmark for all the countries of the Council of Europe. Its approach will be analyzed in part 2. From the case law of the ECtHR, the

---

6 For example, Russian soft "Bitcop" positions itself as a spy one and might be installed and used without being noticed by an employee. See https://bitcop.ru/monitoring/obzor-luchshih-besplatnyh-programm-dlja-slezhenija-za-kompjuterom

7 Walter Malti: The Changing Work Landscape as a Result of the COVID-19 Pandemic: Insights from Remote Workers Life Situations in South Africa. *International Journal of Sociology and Social Policy,* Vol. 40, No. 9/10. (2020) 12 46.; Ella Hafermalz – – Kai Riemer: Productive and Connected while Working from Home: What Client-facing Remote Workers can Learn from Telenurses about 'Belonging Through Technology'. *European Journal of Information Systems,* 2020. DOI: 10.1080/0960085X.2020.1841572, cited from Kirstie Ball: *Electronic Monitoring and Surveillance in the Workplace. Literature review and policy recommendations.* Luxembourg, Publications Office of the European Union, 2021.

8 Shelley Wallach: The Medusa Stare: surveillance and monitoring of employees and the right to privacy. *International Journal of Comparative Labour Law and Industrial Relations*, Vol. 27, Iss. 2, 2011.

9 See Jonathan Bishop:(2017) Detecting Sexual Harassment in Workplace Electronic Communications Networks: The Role of PROTEGER for Augmentive Behaviour Monitoring. In: *Social Issues Surrounding Harassment and Assault: Breakthroughs in Research and Practice*. IGI Global, 2018. 44–79.;I. Elifoglu – Ivan Abel – Özlem Tasseven: (2018) Minimizing Insider Threat Risk with Behavioral Monitoring. *Review of Business,* Vol. 38, Iss. 2, 2018. 61–73.; S. Y. Guo – L. Y. Ding – H. B. Luo – X. Y. Jiang: (2016) A Big-Data-based platform of workers' behavior: Observations from the field. *Accident Analysis and Prevention,* Vol. 93, 2016. 299–309.; all papers cited from Ball op. cit.

factors which might determine the legitimacy of digital surveillance will be derived and considered in the conclusions of the paper.

## 1. National cases

In this part the national cases are presented as illustrations of possible approaches and possible problems arising in the field of employee privacy protection, looking also outside the Council of Europe to have a broader view of privacy problems.

### *1.1. Canadian case*

We will start with the consideration of the recent judgment of a Canadian court, which was reported by media in different countries.[10] The private employer has proved through the special time-tracking program "TimeCamp" that an employee was watching Disney channel during working time and dismissed her.[11] The employee appealed against dismissal, but the court not only found in favour of the employer but also awarded the employer the compensation for the "time theft" in the sum of $1,506.34 for 50.76 unaccounted hours. It should be stated that the judgment is very brief and neither the applicant nor the court refer to the issue of privacy and do not consider the legitimacy of the proof received through the use of the "TimeCamp". It is said that the employer installed a time-tracking program on the employee's work laptop, the employee's consent or notification is not mentioned. The employee stated that "she found TimeCamp difficult to use and she could not get the program to differentiate between time spent working and time spent on the laptop for personal use (which was allowed).[12] The employer provided the Court with the video explaining how this program works:

"where an employee opens a document or accesses a client file, TimeCamp records when and for how long they had the document open or were in the file. The videos show TimeCamp captured the detail of each of Miss Besse's activities which Reach could then use to distinguish between work and non-work activities. For example, if Miss Besse had a streaming service like Disney Plus open, TimeCamp recorded its electronic pathway and how long the service was accessed. As this was not activity associated with client work, Reach would classify it as personal. Similarly, if she accessed a client file, used software associated with client work, or printed client documents, TimeCamp

10 See media publications in English: https://tinyurl.com/336j7sx3 ; in Italian: https://tinyurl.com/4ev3s3dc

11 Civil Resolution Tribunal. Besse v. Reach CPA Inc., 2023 BCCRT 27. January 11, 2023. https://decisions.civilresolutionbc.ca/crt/crtd/en/item/523029/index.do

12 Ibid.

recorded those electronic pathways and the time spent on each task, and Reach classified this as work activity".[13]

The judge relied on the fact that TimeCamp automatically recorded activities in such a way that the employer could identify and classify them as work or non-work related. On this basis it was established that the employee did not work on files she recorded time for in her timesheets, leading to the unaccounted hours. It constituted a "time theft", a very serious form of misconduct that might lead to an irreparable breakdown in the employment relationship and justify the dismissal.

In this judgment, the court takes for granted that digital surveillance was a necessary measure and does not consider if there might have been any other less detrimental tools used to achieve the same objective. There is no balancing between workplace privacy and the employer's right to control as if the use of such programs recording everything that is happening on the laptop has nothing to do with private life. Even though, as it was stated in the judgment, the employee was permitted to use it for personal purposes. Also, neither the question about the use of the information gathered by this software was considered, nor about the employee's consent or notification. The court ignored the statement of the applicant that she did not understand how this program worked and how it differentiated working and non-working time. All these questions, as will be demonstrated further should constitute the core of the analysis of similar cases in the countries of the Council of Europe.

The lack of arguments about the unlawfulness of monitoring through this digital tool, in this case, might be due to the impossibility of exclusion of the evidence if it was collected with the violation of national norms. The Canadian rules on this point are very restrictive: under section 24(2) of the Canadian Charter of Rights and Freedoms, if a court concludes that evidence was obtained in a manner that infringed or denied any rights or freedoms guaranteed by this Charter, the evidence shall be excluded if it is established that, having regard to all the circumstances, the admission of it in the proceedings would bring the administration of justice into disrepute. Section 8 of the Charter protects the privacy of people against unreasonable searches and seizures, ensuring a very limited scope of protection. Also, it is highly unlikely that the admission of the illegally made record of employees' monitoring "would bring the administration of justice into disrepute" as these words are also narrowly interpreted in the jurisprudence of the Supreme Court of Canada.[14]

It is interesting to note that in 2023 new rules came into force in Ontario, requiring employers with 25 or more employees to adopt a written policy on electronic monitoring of employees. This policy must contain the following information: 1. Whether the employer electronically monitors employees and if so, i. a description of how and in what circumstances the employer may electronically monitor employees, and ii. the purposes for which information obtained through electronic monitoring may

13 Ibid.

14 R v Collins, 1987 CanLII 84 (SCC), [1987] 1 SCR 265, per Lamer CJ, cited from Exclusion of Evidence Under Section 24(2) of the Charter. https://www.criminalnotebook.ca/index.php/Exclusion_of_Evidence_Under_Section_24(2)_of_the_Charter

be used by the employer. 2. The date the policy was prepared and the date any changes were made to the policy. 3. Such other information as may be prescribed.[15] The new norms also include the following lines: "For greater certainty, nothing in this section affects or limits an employer's ability to use information obtained through electronic monitoring of its employees". Thus, it is made very clear that even the record of electronic monitoring obtained with the violation of these norms might still be used as proof of misconduct.

### *1.2. Italian case*

The Italian case is brought as an example of an opposite approach compared to the Canadian case. This case is different because it was considered by a special data protection body under the norms of the EU General Data Protection Regulation and also norms providing a human right to privacy.

The case was considered by the Italian Guarantor for the protection of personal data (Guarantor), which already in 2007 adopted guidelines[16] on the monitoring of Internet use and email and formulated the obligation of employers to inform employees in a clear and detailed manner about the permitted methods of use of company tools and the possible implementation of controls also on an individual basis.[17]

The circumstances of the case are the following: the municipal servant was subject to disciplinary measures on account of his having allegedly visited websites that had no connection with his work assignments. The Guarantor found that it was not possible to monitor workers' internet browsing indiscriminately as any control activities must always be carried out in compliance with the Workers' Statute and privacy legislation.

The investigation in this case revealed that the Municipality had been using, for about ten years, a control and filtering system for employees' internet browsing, with data retention for one month and the creation of specific reports, for network security purposes. Although the employer had entered into an agreement with the trade union organizations, as required by sector regulations, the Guarantor highlighted that this data processing must in any case also comply with the data protection principles envisaged by the GDPR. The system, implemented by the Municipality, without having adequately informed the employees, allowed *unnecessary and disproportionate processing operations* with respect to the purpose of protection and security of the internal network, carrying out a preventive and generalized collection of data relating to the connections to the websites visited by the individual

15 Working for Workers Act, 2022, S.O. 2022, c. 7 - Bill 88 https://www.ontario.ca/laws/statute/s22007

16 Lavoro: le linee guida del Garante per posta elettronica e internet. *Gazzetta Ufficiale* n. 58 del 10 marzo 2007. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1387522

17 See, among others, Accesso alla posta elettronica dei dipendenti – 22 dicembre 2016, prov. No. 5958296; Prov. no. 139 of 7 April 2011, web doc. no. 1812154; Prov. no. 308 of 21 July 2011, web doc. no. 1829641; Prov. 23 December 2010, web doc. no. 1786116. https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/5958296

employees. The system also collected information unrelated to the professional activity and in any case attributable to the private life of the interested party. It was noted that the need to reduce the risk of improper use of Internet browsing cannot lead to the complete cancellation of any expectation of confidentiality of the data subject in the workplace, even in cases where the employee uses network services made available by the employer. The employer was fined in a sum of 84,000 euros for the unlawful processing of personnel data.[18]

It is particularly valuable that the Guarantor did not limit itself to the norms of GDPR (which might have been sufficient) but expressed a broader view, integrating into the judgment the norm of the European Convention on Human Rights (article 8 – right for respect to private life) and referring to a number of cases considered by the ECtHR. In particular, it was stated: "Considering that the dividing line between the working and professional sphere and the strictly private one cannot always be drawn clearly, the annulment of any expectation of confidentiality of the data subject in the workplace cannot be prefigured, even in cases where which the employee is connected to the network services made available by the employer or uses a corporate resource even through personal devices, which is why the European Court of Human Rights has confirmed over time that the protection of privacy ( art. 8 European Convention on Human Rights) also extends to the workplace, where the personality and relationships of the person who works are expressed (see Judgments of the European Court of Human Rights Niemietz v. Allemagne, 16.12. 1992 (rec. n. 13710/88), spec. para. 29; Copland v. UK, 04.03.2007 (rec. n. 62617/00), spec. par. 41; Bărbulescu v. Romania [GC], 5.9 .2017 (request n. 61496/08), specific paragraphs 70-73 and 80; Antovic and Mirkovic v. Montenegro, 11.28. 2017 (rec. n. 70838/13), spec. par. 41-42). Therefore, the processing of data carried out using information technology, in the context of the employment relationship, must comply with respect for fundamental rights and freedoms as well as the dignity of the person concerned, for the protection of workers and third parties (see Recommendation CM/Rec( 2015)5 of the Committee of Ministers to the Member States on the processing of personal data in the employment context, spec. point 3)".

The body considering the case attached attention to the factors of necessity and proportionality of the surveillance measure and found that these criteria were not met.[19] This case provides a very interesting example of the broad vision of the right to privacy, where the State authority relies both on norms on data protection and privacy protection. Also, it should be noted that under Italian law (article 4 of the Workers' statute) the information collected through remote checks can be used by the employer if it was collected in line with privacy rules. Therefore, if the use of digital surveillance violated the norms of GDPR, the ECHR, or national law, the records cannot be used as proof of misconduct.

---

18 Ordinanza ingiunzione nei confronti di Comune di Bolzano - 13 maggio 2021 [9669974] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9670319

19 Text of the judgment is available here: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9669974

### *1.3. French case*

The French case is about the geolocation of employees. The employer equipped the vehicles used by its traveling employees, responsible for putting up posters and maintaining urban equipment, with a geolocation device that had not been activated. The company provided the staff representatives with an information document about the use of this device, but the coordinating body of the health, safety, and working conditions committees and the works council issued an unfavorable opinion on the geolocation project, requesting its withdrawal. The employer made a declaration to the National Commission for Information Technology and Freedoms (Commission Nationale de l'Informatique et des Libertés) and implemented the tracking device in the summer of 2016. The trade unions brought an action before the court seeking to prohibit the company from continuing to set up and operate the geolocation system. The judgment ordered the withdrawal of the geolocation system that had been put in place, whereas "the implementation of a geolocation system is lawful when the employee has only limited autonomy in the organization of his or her work; that the company […] had argued that itinerant employees have limited capacity to organize their movements, as they are assigned a tour perimeter, with time slots and a precise schedule, the autonomy of these employees being relative and controlled". The Court of Appeal noted that there were devices in place within the company to monitor the working time of the itinerant operating staff, which were less intrusive than geolocation, with the result that the use of this device was not justified. The Court of Cassation supported this view.

The proportionality test in this case one of the key reasons for prohibiting the use of geolocation. The court considered the legitimacy of such a geolocation device, answering the following questions: if it is necessary and in particular if another device does not already meet these purposes; if it is not disproportionate to the purpose sought, and finally if the data retention period is not excessive with regard to the purpose sought. Even though the Court did not refer to any jurisprudence of the ECtHR, it was following the same logic and formulated the same set of questions to answer.

### *1.4. Russian cases*

The case law of Russian courts is an example of absolutizing employers' managerial rights and sacrificing the privacy rights of employees. Any installment of monitoring facilities is found to be in line with the law without any research on its necessity and proportionality, there were cases when the employee was disciplined for putting balloons in order to close the video camera which was filming only her workplace place all day long, including breaks and before – after-working time.[20]

[20] Decision of the Judicial Board on civil cases of the Orenburg Regional Court of December 3, 2014 in case No. 33-7039 / 2014. See also: Appeal decision of the Krasnoyarsk Regional Court of November 14, 2012 in case No. 33-9899, Appeal decision of the Altai Regional Court of 15 October 2013 in the case of N 33-8403 / 2013.

Even the lack of employee notification about video monitoring is not considered by national courts as a factor evidencing the infringement of privacy rights.[21] In one case, the redundancy procedure was justified by the employer by providing data on the use of the working computer for social network communications. This data made the employer think that this employee did not have enough work and can be dismissed for redundancy reasons. The court considered this evidence admissible without any research of the employee's notification or the limits of surveillance.[22]

An analysis of case law of the period when Russia was still part of the CoE, shows that video recording and other monitoring of an employee's performance with digital means (for example, shadow copying of all files on an employee's computer)[23] is interpreted by the courts as a manifestation of the employer's right to manage labor (Article 22 of the Labor Code of the Russian Federation). As a rule, the existence of general consent to the processing of personal data or fixing the possibility of video recording in the internal labor regulations of the organization is sufficient to recognize such control as legal.[24] Although, such an approach is contrary to the requirements of Art. 9 of the Federal Law of the Russian Federation of 27 July 2006 No. 152-FZ on personal data (further – Law).

In many decisions, the plaintiffs, when appealing against the introduced video surveillance, refer to the norm of Art. 23 of the Constitution of the Russian Federation on the right to privacy. My study showed that the courts tend to ignore such arguments,[25] only in one case the reference to the constitutional right to privacy became the basis for the satisfaction of the worker's claim and the recognition of the illegality of the video.[26] In some decisions, the court, refuses to recognize video surveillance as illegal, pointing out, for example, that "video surveillance was carried out at the workplace, as a result of which the employees of the company and the plaintiff were not infringed in private life" or that "the use of video surveillance equipment by[27] the employer does not violate the employee's constitutional rights to privacy […] because it is carried out for purposes related to the protection of the building, and not in order to establish the circumstances of his private life".[28] It is interesting to note that in the latter case the video recorded by the cameras set up for "security" was used to prove the absence of the worker from the workplace.

---

21 The decision of the Leningrad district court of the city of Kaliningrad on 05/25/2017 in case No. 2-2243 / 2017.

22 Appeal decision of the Novgorod Regional Court of June 6, 2012 in case No. 2-1935 / 12-33-823.

23 Decision in case No. 2-1688/2018 dated March 27, 2019 Leninsky District Court of Yaroslavl (Yaroslavl Region).

24 Decision in case No. 2-502/2017 dated June 26, 2017. Privokzalny District Court of Tula (Tula Region); Decision in case No. 2-1609/2017 dated May 19, 2017, Leninsky District Court of Voronezh (Voronezh Region); Appeal ruling of the Altai Regional Court dated October 15, 2013 in case N 33-8403/2013; Appeal ruling of the Krasnoyarsk Regional Court dated November 14, 2012 in case No. 33-9899; Decision of the Michurinsky City Court of the Tambov Region dated July 15, 2016 in case No. 2-947/2016.

25 The case of installing a "shadow copy" program for all files on a work computer: Decision dated March 27, 2019 in case No. 2-1688/2018 Leninsky District Court of Yaroslavl (Yaroslavl Region).

26 Decision in case No. 2-81/2020 dated February 19, 2020, Berezovsky District Court of Yugra (KhMAO).

27 Decision No. 2-3212/12 dated July 20, 2012 in case No. 2-3212/12 Volzhsky District Court of Saratov (Saratov Region).

28 Case of video surveillance of employees and dismissal based on data from video cameras installed in the building: Decision dated April 29, 2019 in case No. 2-2607/2018 of the Moscow District Court of Ryazan (Ryazan Region). A similar approach in relation to cameras installed to ensure security in the organization: Ruling of the Krasnoyarsk Regional Court dated November 14, 2012 in case No. 33-989920; Decision of the Michurinsky city court of the Tambov region dated July 15, 2016 No. 2-947 / 201621.

This approach is contrary to the principles on the processing of personal data established by Art. 5 of the Law. In particular, the principle of limiting processing to the achievement of specific, predetermined, and legitimate purposes (clause 2, article 5 of the Law). In addition, paragraph 7 of this article establishes the need to destroy or depersonalize the processed personal data upon reaching the goals of processing. I suppose that the application of these principles to the situation described in the decision of the court of the Tambov region should have led the court to conclude that the video recording was illegal since the personal data obtained in order to protect the building were used for other purposes – to determine the employee's failure to fulfill his duties.

Geolocation of employees, according to the judges, also derives from the employer's right to manage labour and does not require the employee's written consent or special procedures. In the opinion of experts of the State Labour Inspectorate, the introduction of geolocation is possible by changing the terms of the employment contract (parts 1 and 2 of Article 74 of the Russian Labour Code).[29] In practice, this type of control is introduced by a local legal act and changes in the job description of the employee.[30] In one decision, the court considered it sufficient to introduce geolocation without any formalization of the employer's right to control the performance of work duties and to conclude an agreement with MTS, the largest mobile network in Russia, on the connection to the Mobile Employees option, which allows tracking the location of all employees who use the relevant equipment.[31] This approach is in sharp contrast with the norms of the Law on private data but still is widespread.

The recorded data (through tracking computer files, video, geolocation and etc.) is normally used to prove an employee's misconduct. According to Article 55 of the Civil Procedure Code of the Russian Federation, evidence in a case shall be information *obtained in accordance with the procedure prescribed by law*. Therefore, to establish violations of the requirements of the Labor Code of the Russian Federation or the Law, the court must decide on the illegality of monitoring/video surveillance/geolocation if it was obtained with the violation of the norms on personal data. However, in the vast majority of decisions, the courts do not consider compliance with data protection norms a condition for the lawfulness of surveillance and the resulting recordings.[32] It is striking that none of the courts referred to the ECtHR's case law.

Finishing the part about the national cases the following should be pointed out: the review of these cases demonstrated the differences in the national approaches to the issue of employee monitoring through different digital tools. The examples of France and Italy have much in common as the judgments are built upon the proportionality exercise, balancing the rights of employers to control

[29] Question: How do you prepare and keep track of the working time of mobile employees on the basis of GPS tracker readings? (Expert Consultation, State Labour Inspectorate of the Nizhny Novgorod Region, 2021) ConsultantPlus.

[30] Decision No. 2-1064/2019 2-1064/2019~M-279/2019 M-279/2019 dated 15 August 2019 in case No. 2-1064/2019 Industrial District Court of Khabarovsk (Khabarovsk Territory).

[31] Decision No. 2-3688/2016 of 29 November 2016 in case No. 2-3688/2016 Domodedovo City Court (Moscow Region).

[32] As one example: Decision in case No. 2-248 / 2020 dated February 11, 2020 Rudnichny District Court of Kemerovo.

work and employees' privacy. This legal reasoning, as it will be explained below, is characteristic of the ECtHR, which, as it is proposed in the paper, might serve as a benchmark for formulating legal restrictions on the use of digital surveillance tools.

## 2. Approach of the ECtHR to workplace privacy

The introduction of a framework for considering cases on employees' privacy and the proposal of a "checklist" of questions to be responded to by national courts[33] in similar cases are the key achievements of the ECtHR. This framework is deduced from the second paragraph of article 8 and complimented with the "reasonableness of the expectations of privacy" test applied in the majority of workplace privacy cases. Thus, considering such cases the Court first (but not always) establishes if the employee had a reasonable expectation of privacy[34], then the ECtHR considers if there had been an interference with the right to privacy and evaluates its lawfulness and necessity.[35] The proportionality assessment of the interference with the legitimate aim pursued by the employer is the most important part of the last step.[36]

This framework is applicable both in case of the violation of the states' negative obligation not to interfere with the right to privacy when the case is brought, for example, by a public servant.[37] Also, it is used in the cases on positive obligations of the states to secure the right to privacy in relations between private parties, involving also the obligations of national courts to correctly considered the case in line with article 8.[38] While Article 8 contains no explicit procedural requirements, the decision-making process involved in measures of interference with this right must be fair and ensure due respect for the interests safeguarded by Article 8.[39]

The proportionality test is one of the most controversial issues in privacy cases in particular as far as private employees are concerned.[40] In cases concerning the positive obligations of the State under Article 8, the Court verifies if the right to privacy is effectively protected and correctly balanced with the employer's rights by national courts. These are cases of dismissal of employees for non-

33 See, in partuclar, such a list in ECtHR, Bărbulescu v. Romania (61496/08)GC 05/09/2017, para. 121.

34 See, for example, ECtHR, Halford v. United Kingdom (20605/92) 25/07/1997, para. 44 and Copland v. the United Kingdom (62617/00) 03/04/2007, para. 42.

35 ECtHR, Halford v. United Kingdom (20605/92) 25/07/1997; Copland v. the United Kingdom (62617/00) 03/04/2007; ECtHR, Peev v. Bulgary, para. 43.

36 Ibid.

37 ECtHR, Pay v. UK (32792/05) inadmissible 16 September 2008, or Peev v. Bulgaria (64209/01) 26 July 2007, Radu v. Moldova(50073/07) 15 April 2014.

38 ECtHR, Köpke v. Germany (420/07) inadmissible 05/10/2010; Bărbulescu v. Romania (61496/08)12/01/2016.

39 ECtHR, Guide on Article 8 of the Convention – Right to respect for private and family life. Updated on 31 August 2022.

40 See controversial judgments delivered by the Chambers and the Grand Chamber of the ECtHR in cases Bărbulescu v. Romania and López Ribalda v. Spain, and dissenting opinions of judges to each of these 4 judgments.

compliance with their duties revealed by the means of video surveillance (in Köpke v. Germany[41], Lopez Ribalda and others v. Spain[42]) and by monitoring of private messages sent from corporate Yahoo messenger account (Bărbulescu v. Romania[43]) and the access of employer to employee's files on the computer (Libert v. France[44]).

It is noteworthy that the two leading cases on employee privacy were reconsidered by the Grand Chamber of the ECtHR because of the different approaches of the judges to the proportionality of the interference. Thus, in 2016 the Chamber did not find a violation of article 8 in the case of an engineer, who was dismissed for the use of the company's Internet for personal purposes after his personal messages were read by the employer (Barbulescu v. Romania). The ECtHR concluded that the measure was proportionate as the employer did not have another method to verify whether the applicant infringed internal policy. It found that the employer acted within its disciplinary powers and pointed out that the monitoring was limited in scope and proportionate.[45] The Grand Chamber reconsidered the case and delivered the judgment in 2017. By 11 votes to 6, it decided that the State has violated its positive obligations under article 8 and included new factors which should be taken into account by national courts in such cases thus extending the proportionality exercise.[46]

In the case Lopez Ribalda and others v. Spain, the Chamber did not share the domestic courts' view on the proportionality of the measures adopted by the employer because these acts did not comply with the requirements stipulated in the Spanish Personal Data Protection Act. This led the Court to conclude that the domestic courts failed to strike a fair balance between the applicants' right to respect for their private life under Article 8 of the Convention and their employer's interest in the protection of his property rights.[47] It was a good point for excluding covert video surveillance at the workplace as such. Indeed, the employer always has other ways and less intrusive methods to establish the employees' misbehavior. The Grand Chamber, on the contrary, approved the approach of the national courts in October 2019. It expressed a light criticism of Spanish courts for attaching little attention to the fact of employees' notification about the recording but still concluded that there had been no violation of the ECHR.

It should be noted that some national high courts of the Council of Europe are aware of this line of ECtHR's case law. The Bărbulescu case is a champion, being referred to by Constitutional court[48]

41 ECtHR, Köpke v. Germany (420/07) inadmissible 05/10/2010.

42 ECtHR, López Ribalda v. Spain (application no. 1874/13) 09.01.2018

43 ECtHR, Bărbulescu v. Romania (61496/08)12/01/2016.

44 ECtHR, Libert v. France (application no. 588/13)22.02.2018

45 ECtHR, Bărbulescu v. Romania (61496/08)12/01/2016, para. 60.

46 ECtHR, Bărbulescu v. Romania (61496/08)GC 05/09/2017, para. 121.

47 ECtHR, López Ribalda and Others V. Spain (1874/13 8567/13) 09/01/2018, para. 69.

48 Spanish Constitutional Court, judgment of 3 March 2016 (no. 39/2016). See López Ribalda and Others v. Spain, para. 56, see also Tribunal Constitucional TC (Pleno) Sentencia num. 119/2022 de 20 septiembre RTC\2022\119.

and the Supreme Court in Spain[49]. In the same time lower courts do not refer often to Strasburg jurisprudence. In the French database of national judgments only one reference to Barbulescu judgment was found – in the case about the use of an employee's IP to obtain proof of misconduct,[50] no references were found in the jurisprudence of the Commission Nationale de l'Informatique et des Libertés (French Data Protection Authority)[51] At the same time, Italian courts and Guarantors do cite this ECtHR case much more often.[52]

## 3. Conclusions

The recent report "Data subjects, digital surveillance, AI and the future of work" demonstrates that the use of digital surveillance in widespread in all European countries and is likely to grow. In this paper, the different cases on digital surveillance were considered to demonstrate a number of legal and practical issues. Among these issues, it is worth to point the following:

1. Impossibility to exclude the record of surveillance as evidence of misconduct even if it was obtained in violation of laws in cases of Canada and Russia. It comes from a narrow formulation of the grounds for excluding evidence in Canadian law, and from the court's reluctance to apply relevant norms on processing of private data by Russian courts.
2. The lack of balancing employer's rights to control against employee's privacy rights in Russian case law;
3. Broad perception of employers' right to control (Canada and Russia).
4. Integration of the proportionality tests in the consideration of national cases on workplace privacy by national courts and by guarantors for the protection of personal data in France and Italy.
5. The limited reference to the case law of the ECtHR by national courts considering cases on workplace privacy (Italy and France).
6. No references to the case law of the ECtHR by French Data Protection Authority while some references might be found in the practice of an Italian one.

---

49 See Spanish Supreme Court: Tribunal Supremo. Sala de lo Penal, Sentencia núm. 56/2022,24/01/2022. https://www.poderjudicial.es/

50 Cour de Cassation, civile, Chambre sociale, 25 novembre 2020, 17-19.523.

51 https://www.legifrance.gouv.fr/ (accessed 15.04.2023).

52 Corte suprema di cassazione, Sez. Lavoro Civile: Sentenza N.34092 Del 12/11/2021; Sentenza N.33380 Del 11/11/2021; Ordinanza N.13266 Del 28/05/2018, see the jurisprudence of the Italian Garante Per La Protezione Dei Dati Personali: Ordinanza ingiunzione nei confronti di Azienda ospedaliera di Perugia – 7 aprile 2022 [9768363]; Provvedimento del 17 settembre 2020 [9461168]; Ordinanza di ingiunzione nei confronti di Regione Lazio – 1 dicembre 2022 [9833530]; null Ordinanza ingiunzione nei confronti di Comune di Bolzano – 13 maggio 2021 [9669974].

I suppose that the use of the set of questions elaborated by the ECtHR in the Grand Chamber Barbulescu judgment might ensure a more harmonious approach to the evaluation of the legality of digital surveillance throughout the countries of the Council of Europe.[53]

In para. 120 the Court formulated the following criteria which might be applicable for the evaluation of digital tools installed or used by an employer for the control of employees:

(i) Clear notification of an employee about the monitoring activities, which should be given in advance

(ii) The extent of the monitoring by the employer and the degree of intrusion into the employee's privacy (a distinction should be made between monitoring of the flow of communications and of their content, whether all communications or only part of them have been monitored, was monitoring limited in time and the number of people who had access to the results, were their spatial limits to the monitoring);

(iii) Presence of legitimate reasons to justify monitoring the communications and accessing their actual content;

(iv) The possibility to establish a monitoring system based on less intrusive methods and measures than directly accessing the content of the employee's communications;

Under these criteria, neither screenshotting nor keylogging might not be justified as this software constitutes a deep intrusion into an employee's privacy enabling an employer to access the content of any private information being viewed or sent through the employer's device.

53 ECtHR, Bărbulescu v. Romania (61496/08)GC 05/09/2017, para. 120.