LEGAL ASPECTS REGARDING THE MONITORING OF EMPLOYEES IN THE WORKPLACE

Roxana Maria ROBA[*]

ABSTRACT: *The evolution of technology offers employers the possibility to permanently monitor the employees' activity. The legal provisions concerning the employer's right to use monitoring systems consisting of electronic communications means and/or video surveillance in the workplace is a topic of great interest. The present study aims to analyze the legal framework allowing employers to monitor employees in the workplace but also highlight the consequences of violating legal provisions concerning this topic.*

KEYWORDS: *employer, monitoring , employee, workplace, activity.*
JEL CODE: *K 31.*

Currently, technology allows employers to monitor their employees' activity in order to see to what extent they are correctly and efficiently fulfilling their obligations that they committed to through individual labor contracts, not only to improve the quality of work but also for security reasons. Employee supervision is often conducted through surveillance cameras, but it is also possible to use different means with less exposure.

One means of monitoring consists of supervising employees' internet usage. This is how the employer will be able to see what websites the employee is visiting and decide whether these websites are related or not to their work attributions.

Most of us have certainly been contacted by a company via phone call, or have attempted to contact a service or business, and were communicated the message that in order to improve services, the call would be recorded and continuing the conversation represents the agreement to be recorded.

Recording employees' phone calls can help employers evaluate their work but also to improve their strategies of attracting customers and represents a different means of monitoring the workforce.

Another employees might rather be interested in knowing how much time employees spend talking on the phone and whether these conversations are relevant for their activity in the workplace or not.

[*] Lecturer, PhD - Faculty of Law and Economics, University of Medicine, Pharmacy, Science and Technology, Tg. Mureș, ROMANIA.

Technology made it possible that through a device worn by employees, their body language be monitored in order to assess how much time is spent talking and participating in meetings, and also how many times they leave their desks[1]. In 2015, a Japanese company announced launching a sensor collecting and analyzing data about human behavior and using this information to evaluate the level of activity of the organization, which is closely connected to productivity at work[2].

There are multiple advantages to monitoring employees: transparency, security in the workplace, a better division of tasks, evaluating employee performance, increasing work efficiency etc.

However, employers taking such measures can also result in increasing stress levels of their employees, as they might perceive the monitoring measures as a sign of distrust, and thus resulting in decreased productivity at the workplace, or eventually even changing workplace.

At European Union level, regulations concerning private life and the protection of personal information are contained in articles 7 and 8 of the „Charter of Fundamental Rights of the European Union".

„The Court of Justice of the European Union"[3] had the opportunity to decide in a series of cases regarding the interpretation and application of articles 7 and 8 of the „Charter of Fundamental Rights of the European Union". Evaluating the CJEU caselaw we can conclude that there is a preference among judges for an extended protection of rights concerning personal data (Șandru, 2017).

A normative act of reference was also the „Directive 95/46/CE of the European Parliament and of the Council, of 24 October 1995[4] on the protection of individuals with regard to the processing of personal data and on the free movement of such data"[5]. The Directive 95/46/CE formulated the principles that govern the monitoring of the usage of internet and electronic mail at the workplace, as follows[6]:

- The principle of necessity: processing personal data must be necessary for a specified, explicit purpose;

[1]https://www.cbc.ca/news/technology/how-new-data-collection-technology-might-change-office-culture-1.3196065

[2] http://www.hitachi.com/New/cnews/month/2015/02/150209.html

[3] In the case Digital Rights, C- 293/12 and C – 594/12 decision of 8 April 2014, Google Spain, C – 131/12, decision of 13 May 2014, Rymes, C-212/13, decision of 11 December 2014.

[4] Which was implemented in domestic legislation through Law nr. 676/2001 on the protection of personal data, abrogated through Law 506/2004.

[5] Directive 95/46/CE of the European Parliament and Council of 24 October 1995 on the protection of individuals concerning processing of personal data and the free movement of such data, published in JO L 281, 23 November 1995, Special edition 13/vol.17, p. 10 and was abrogated through Regulation (EU) 2016/679 of the European Parliament and Council of 27 April 2016 on protecting individuals concerning processing of personal data and the free movement of such data and abrogation of Directive 95/46/CE (General regulation on data protection), published in JO L 119 of 4 May 2016.

[6] See decision Bărbulescu v. Romania of 5 September 2017.

- The principle of finality: personal data must be collected for an explicit legitimate purpose;
- The principle of transparency: the employer must give employees all the information regarding data processing;
- The principle of legitimacy: processing personal data may only take place for a legitimate purpose;
- The principle of proportionality: the processing of personal data „must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed"[7];
- The principle of security: the employer is bound to take all security measures so that personal data processed is not accessible to third parties.

A working party for data protection[8] was established under art. 29 of the „Directive nr. 95/46/CE of the European Parliament and the Council of the European Union of the 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data", with the purpose to examine any question „related to the surveillance of electronic communication in the workplace" and to evaluate its consequences for the protection of data belonging to employees and employers equally (Popescu, 2017). This working party published a document entitled „*Working document on the surveillance of electronic communications in the workplace*"[9].

„Workers do not abandon their right to privacy and data protection every morning at the doors of the workplace. They do have a legitimate expectation of a certain degree of privacy in the workplace as they develop a significant part of their relationships with other human beings within the workplace. However, this right must be balanced with other legitimate rights and interests of the employer, in particular the employer's right to run his business efficiently to a certain extent, and above all, the right to protect himself from the liability or the harm that workers' actions may create. These rights and interests constitute legitimate grounds that may justify appropriate measures to limit the worker's right to privacy. The clearest example of this would be those cases where the employer is victim of a worker's criminal offence."

„Regulation (EC) nr. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data"[10] establishes the same principales for institutions and organizations of the European Communities.

---

[7] See Directive 95/46/EC of The European Parliament and of The Council, alin. 28.

[8] The party was replaced starting 25 May 2018 with the European Committee concerning Data Protection following the coming into effect of the Regulation nr. 2016/679/UE. The documents adopted by this party remain valid as long as the provisions of the directive remain. See Daniel-Mihail Șandru – *Protecția datelor personale: surse legislative, jurisprudențiale și soft law.*

[9] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp55_en.pdf

[10] Regulation (CE) nr. 45/2001 published in JO L 8, 12 January 2001, Special edition, 13/Vol. 30

Also, the „Directive nr. 2002/58/CE of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)"[11] regulates the processing of personal processing of personal data and the protection of privacy in the electronic communications sector.

Another relevant document is the „Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)"[12], which underlines in its art. 15 that Member States shall not impose a general obligation on providers of internet/email services, because such an obligation would represent „a violation of the freedom" of information and the confidentiality of correspondence.

Regulation (EU) nr. 2016/679 did not significantly change the status of personal data protection concerning work relations, but introduced drastic sanctions that could reach, for companies, up to 4% of the total global turnover corresponding to the previous financial year[13].

The European Court of Human Rights had an opportunity to judge on the decisions given in the case Bărbulescu v. Romania from 12 January 2016 and 5 September 2017.

Thus, in the decision given on 12 January 2016[14], the Court stated: *As to the use of the transcript of the applicant's communications on Yahoo Messenger as evidence before the domestic courts, the Court does not find that the domestic courts attached particular weight to it or to the actual content of the applicant's communications in particular. The domestic courts relied on the transcript only to the extent that it proved the applicant's disciplinary breach, namely that he had used the company's computer for personal purposes during working hours. There is, indeed, no mention in their decisions of particular circumstances that the applicant communicated; the identity of the parties with whom he communicated is not revealed either. Therefore, the Court takes the view that the content of the communications was not a decisive element in the domestic courts' findings.*

---

[11] Directive nr. 2002/58/CE of the European Parliament and Council of 12 July 2002 on processing personal data and protecting confidentiality in the public communications sector, published in JO L 201, 31 July 2002, Special edition 13/vol. 36, p. 63. The Directive was modified through the Directive nr. 2009/136/CE of the European Parliament and Council of 25 November to modify the Directive nr. 2002/22/CE on universal service and user rights concerning networks and services of electronic communications, of Directive nr. 2002/58/CE on processing personal data and protecting confidentiality in the public communications sector, of Regulation CE nr. 2006/2004 on the cooperation between national authorities charged with applying legislation concerning consumer protection, published in JO L 337, 18 December 2009, p. 11.

[12] Directive 2000/31/CE of the European Parliament and Council of 8 June 2000 on certain judicial aspects of services of the informational society, especially electronic commerce, on the internal market (directive concerning electronic commerce) was published in *OJ L 178, of 17 July 2000,* 13/Vol. 29, *p. 1–16*

[13] See art. 83, alin. 5 of the Regulation.

[14] *Published on https://hudoc.echr.coe.int/eng#{"itemid":["001-159906"]}*

The Court decided „that there had been no violation of Article 8 (right to respect for private and family life, the home and correspondence) of the European Convention on Human Rights", arguing that it was not unreasonable that an employer would want to verify that employees „were completing their professional tasks during working hours". The Court also noted that only the Yahoo Messenger conversations were examined, but not other data or documents saved on the computer. It follows that the employee surveillance was limited in its scope, and proportional. It was also noted that the plaintiff had not convincingly explained the reason for using the Yahoo Messenger account for personal purposes. Therefore, the Court decided „that the domestic courts had struck a fair balance between Mr Bărbulescu's right to respect for his private life and correspondence under Article 8 and the interests of his employer". The case made the topic of intense debates[15].

This follows a previous judgment of the European Court of Human Rights, Copland v. UK[16], where the decision had been the opposite in that the monitoring of personal data concerning Mrs. Copland, employee of a state institution, and more specifically her use of the phone, electronic mail, and internet, violated her right to the respect of private life and correspondence and this breach was not foreseen by the law, considering that at the moment of that breach, there was no domestic law regulating monitoring. Admitting that the monitoring of an employee's use of the phone and internet can have legitimate aims, the Court considered that in the particular case at hand it was not necessary pronounce on the matter of the breach being legitimate or not.

In the case Bărbulescu v. Romania, the decision of 5 September 2017[17], invoking the breach of art. 8 of the Convention, the plaintiff stated „that his employer's decision to dismiss him was based on a violation of the plaintiff's right to respect for his private life and correspondence, and that domestic courts failed to fulfill their obligation to protect this right as they did not cancel said measure".

The plaintiff complained both to domestic courts and the European Court of Human Rights, about the monitoring of his employer of the plaintiff's communications made via his account of Yahoo Messenger and using these communications during the disciplinary procedures directed against him.

The plaintiff stated that the communications made through telephone or electronic mail made by an employee from within the workplace belong to the area of „private life" and „correspondence" and consequently benefit from the protection granted by art. 8 of the Convention. He also stated that his dismissal was illegal, and that the employer violated criminal law by monitoring his communications and their content.

Particularly, concerning the moral prejudice suffered, the plaintiff recalled the manner in which he was dismissed and stated that the employer submitted him to

---

15 *Vasile Bozeşan* Neîncălcarea dreptului la viaţă privată şi corespondenţă în cazul accesării şi verificării de angajator a contului profesional Yahoo Messenger utilizat de un angajat al său, *published on http://www.hotararicedo.ro/index.php/news /2016/01 /nencalcarea-dreptului-la-viata-privata-si-corespondenta-n-cazul-accesarii-si-verificarii-de-angajator-a-contului-profesional-yahoo-messenger-utilizat-de-un-angajat-al-sau***.**

[16] Request nr. 62617/00, decision of 3 April 2007.

[17] Published on the website https://www.csm1909.ro/321/5245/Cauza--Bărbulescu-împotriva-României-(nr.-61496-08)-–-Hotărârea-din-5-septembrie-2017

harassment which, according to the plaintiff, consisted in the monitoring of his communications and revealing their content to „colleagues involved in various ways in the dismissal procedure".

The Court's conclusion was that the plaintiff's communications at the workplace belonged to the sphere of „private life" and „correspondence" and that the domestic authorities did not adequately protect the plaintiff's right „to the respect of private life and correspondence, and therefore did not ensure a just balance between the interests at stake".

Also, the Court noted that domestic courts omitted on the one hand to verify particularly if the plaintiff had been warned about his employer about the possibility that his communications via Yahoo Messenger might be monitored and on the other hand they did not take into account the fact that the plaintiff had not been informed about the degree of monitoring he was submitted to, nor about the degree of intrusion in his private life and correspondence. What is more, domestic courts did not establish the exact reasons that justified the monitoring measures nor if the employer could have applied less intrusive measures regarding the private life and correspondence of the plaintiff, and finally, if it was possible that the access to the content of the communications had occurred without the plaintiff's knowledge.

The Court considered that the domestic authorities did not adequately protect the plaintiff's right to respect of his private life and correspondence and therefore did not ensure a just balance between the interests at stake. Consequently, there was a violation of art. 8 of the Convention.

Regarding the factors that should be taken into account when the employer takes measures toward monitoring, the Court notes that the following essential elements must be taken into consideration:

- Informing the employee about the possibility for the employer to adopt measures of monitoring the correspondence and other communications, as well as enforcing such measures. In this sense, it is important to make a distinction between monitoring the flux of communication and its actual content. Also, it must be considered if all communications or just a part of them were monitored and if this surveillance was limited in time or not, as well as the amount of people who had access to its results;
- Invoking legitimate reasons, by the employer, to justify the monitoring of these communications and access to their actual content. Monitoring the content of communications is, by its very nature, a much more invasive method that requires more serious justification;
- Analyzing the possibility to institute a monitoring system based on means and measures less intrusive than direct access to the content of employee communications. In this sense, it is necessary to appreciate in light of specific circumstances of each case if the employer's aims can be reached without direct, complete access to the content of employee communications;
- Mentioning if the employee was offered sufficient guarantees especially when the monitoring measures of the employer had an intrusive nature. These guarantees must particularly allow denying the employer's access to the actual content of the communications, when the employee was not previously informed about the possibility of monitoring taking place.

Analyzing the arguments of the „European Court of Human Rights", we can conclude that informing employees, and the company policy on this level regarding this aspect, should be particularized and clarified as far as all aspects of monitoring go, namely that the following aspects should be detailed in advance[18]: if the flux of communications is the sole object of surveillance or if it is also the content of communications; if all communications are monitored or only a part of them; if the surveillance is limited in time and who has access to these communications; the consequences of monitoring for concerned employees; the use of the results of the surveillance by the employer.

Through the decision of the Chamber of 28 November 2017 in the case Antović and Mirković v. Montenegro (request nr. 70838/13)[19], the European Court of Human Rights ruled that the video surveillance of university classrooms violated the right to private life, and that therefore art. 8 of the Convention was violated. The case concerned the request forwarded by two professors of the Mathematics Faculty of the University of Montenegro, Nevenka Antović and Jovan Mirković, following the setup of video surveillance cameras in classrooms. The professors claimed that their right to private life and personal data was violated and declared that they had no effective control over collected information and that the video surveillance was illegal.

Domestic courts rejected requests for indemnity filed by the plaintiffs, motivating that the issue of private life could not be raised considering that the classrooms where the plaintiffs taught courses were public domain.

The Court rejected the Government argument according to which the cause was inadmissible due to the fact that the space submitted to video surveillance was public domain destined to professional activities.

Upon the merits of the case, it was noted that video surveillance was a violation of the right to private life and evidence showed that the monitoring violated provisions of domestic law. Indeed, domestic courts did not consider legal justifications of the surveillance because it was decided from the beginning that there was no violation of private life.

The Court mentioned that in previous decisions it was found that the notion of „private life" could encompass professional activities or activities taking place in public spaces and underlined that university classrooms were the place where professors undertook their professional activity, where they not only taught class but also interacted with students, establishing relations and affirming their social identity. At the same time, the Court noted previously that hidden video surveillance in the workplace represented a violation of the right to private life of employees and there was no reason to consider video surveillance that was not hidden in any different way.

Internally, Law nr. 190/2018 is currently in place, concerning measures of applications of the „Regulation (EU) 2016/679 of the European Parliament and Council of 27 April

---

[18] Emeric Domokos-Hancu, Adriana Radu – European Court of Human Rights: Employers can monitor the employees' e-mails under limited conditions, published on https://www.hotnews.ro/stiri-specialisti_schoenherr_asociatii-21992610-curtea-europeana-drepturilor-omului-angajatorii-pot-monitoriza-mailul-angajatilor-conditii-limitate.htm.

[19] https://www.lhr.md/ro/2017/12/ctedo-supravegherea-video-salilor-universitare-contrara-conventiei/

2016 on the protection of individuals concerning processing personal data and the free movement of such data and of abrogation of Directive 95/46/CE (General regulation concerning data protection) ". Art. 5 of this normative act foresees the following: *If monitoring systems are used, through electronic communication means and/or video surveillance means at the workplace, processing personal data*[20] *of employees, with the purpose of fulfilling legitimate aims of the employer, is only permitted if:*

a) legitimate aims of the employer are dutifully justified and outvalue interests or rights and freedoms of individuals;

b) the employer carried out the mandatory prior information in a complete and explicit manner towards employees;

c) the employer consulted the syndicate or the employee representatives before introducing the monitoring systems;

d) other means and manners, less intrusive, to attain the aims of the employer did not previously prove their efficacy;

e) the period of storage of personal data is proportional to the aim of the processing, but not longer than 30 days, excepting situations specifically regulated by law or duly substantiated cases..

Concerning sanctions, Law nr. 190/2018 references the provisions of Regulation (EU) 2016/679[21]. The person harmed through the violation of these provisions can submit an action for damages, without excluding also a criminal complaint according to the provisions of art. 302 of the Penal Code for violation of the confidentiality of correspondence, if the legal provisions are met.

To conclude, one can note that domestic legislation is in accordance with principles found in European legislation and case law. If the employer decides to use monitoring at the workplace through means of surveillance of electronic communications or video surveillance, he will need to prove compliance with legal provisions. Special attention will be given to conditions foreseen by art.5, lit.a and d of the law, concerning legitimate aims of the employer, which must prevail over interests or rights and freedoms of concerned individuals, namely identifying less intrusive means and manners to fulfill the purpose of the employers which have not proven their efficacy previously.

The analyzed theme is also relevant from the perspective of the entry into force of Law nr. 81/2018 on the reglementation of remote work[22].

---

[20] According to art. 4, pct. 1 of the Regulation,

1. „personal data" is any information concerning an identified or identifiable individual („the individual concerned"); an identifiable individual is a person who can be identified, directly or indirectly, particularly through an element of identification such as a name, an identification number, localization data, an online handle, one or more specific elements, characteristic to their physical, physiological, genetic, psychologic, economic, social or cultural identity;

[21] Art. 12, alin. 4 of the Regulation.

[22] Remote work is, according to art. 2, lit. a of Law nr. 81/2018, is the organizational form of work through which the employee, regularly and voluntarily, fulfills specific attributions to his position, company, role, or position that he has, in a place different than

REFERENCES

Șandru , D.-M., 2017. Curtea de Justiție a Uniunii Europene și protecția datelor personale ale angajaților în relațiile de muncă, , pag. 98.. *Romanian Magazine of European Law nr. 4/2017*, Issue 4, p. 98.

Popescu, R.-M., 2017. Interzicerea utilizării telefonului personal în timpul programului de lucru. *Romanian Magazine for Labour Law ,* Issue 3, p. 95.

the workplace organized by the employer, for at least one day a month, using the information and communications technology;