Surveillance in the workplace: States' positive obligations in the case-law of the European Court of Human Rights

di Elena Yurkina

Title: Sorveglianza sul luogo di lavoro: obblighi positivi degli Stati nella giurisprudenza della Corte Edu

Keywords: Surveillance in workplace; Positive obligations; Private life.

1. – In January 2016 the European Court on Human Rights adopted a judgment in a case concerning the surveillance in the workplace (*Bărbulescu v. Romania* Application no. 61496/08, Merits and Just Satisfaction, 12 January 2016), which later was sent for re-examination by the Grand Chamber. The facts of the case are as follows. The applicant was dismissed from a private company for a breach of internal policy, which prohibited the use of the company's computers for personal purposes. Mr Bărbulescu used his Yahoo Messenger account – which he had installed at the request of the company for client-related communication – to correspond with his fiancée and brother. At some point, the applicant was accused by the company of using that Yahoo account for personal communications. The surveillance revealed that the applicant was having personal communications on both his professional and his personal Yahoo accounts. He was subsequently dismissed. The applicant challenged his dismissal in the domestic courts based on the unlawful monitoring of his computer, in breach of his right to respect for his private life.

The domestic courts ruled against the applicant. Their reasoning was that the company had the right to check the manner in which professional tasks were being completed; the monitoring procedures were transparent as the applicant had been aware of a similar procedure applied to his colleague, who had been dismissed as a result; the necessity of the monitoring was founded on "the possibilities that, through use of the Internet, employees could damage the company's IT systems, or engage in illicit activities in the company's name, or reveal the company's commercial secrets".

2. – The European Court found no violation of Article 8, on the following grounds. The employer's interference was limited in scope, proportionate and served a legitimate aim – to act as a disciplinary measure for an offence committed by the applicant. The domestic authorities managed to strike a fair balance between the applicant's right to respect for his private life under Article 8 and the interests of the company in ensuring its employees' compliance with their professional obligations during working hours.

In its analysis, the Court distinguished the case in question from its previous cases concerning surveillance in the workplace: namely, *Halford v. the UK* (Application no. 20605/92, Merits and Just Satisfaction, 25 June 1997) and *Copland v. the UK* (Application no. 62617/00, Merits and Just Satisfaction, 3 April 2007).

The *Halford* case concerns interception by the police of the telephone calls of a police officer who sued her local police department for discrimination against her on the grounds of her sex. In this case the applicant had a telephone in her workplace for personal use. She sought assurance from her boss that she had authorisation to use that telephone to discuss her discrimination case with her lawyer. The applicant received such assurance and therefore reasonably expected that her employer would respect her privacy. At some point she was informed by an anonymous that her calls made from her home and her office telephones were intercepted with the primary aim of gathering material to assist in the defence of the sex-discrimination proceedings brought against them. Ms Halford applied to the Interception of Communications Tribunal for an investigation and than brought a complaint to the European Court. The Court found a violation of Article 8 since the domestic law did not provide adequate protection to Ms Halford against interferences by the police with her right to respect for her private life and correspondence.

In *Copland v. the UK*, the ECHR ruled that Article 8 was breached when an employer monitored the applicant's phone calls, e-mails and Internet use in the workplace to determine whether she was using workplace tools excessively for personal purposes in the absence of any internal regulation.

Thus, the main distinction between those cases and the *Bărbulescu* case is that in those cases the applicants had reasonable expectation of privacy because the personal use of professional technical equipment was allowed, or at least tolerated, by their employers. Such reasonable expectation may arise in the absence of any prior warning of monitoring of computers or telephones in the workplace (*Bărbulescu v. Romania*, Supra n 1, at paras 38 and 39). In the *Bărbulescu* case, the applicant was aware of the company's internal policy prohibiting employees from using computers for their personal purposes.

3. – The important issue here is whether work-related correspondence falls under protection from interception. The Government argued among other things that the case was inadmissible as the applicant had declared that his Yahoo account contained only his professional correspondence, which, according to the Government, was not covered by Article 8.

The Court did not accept that argument and pointed out that communication from the workplace fell within the scope of Article 8, with reference to the cases of Halford v. the UK, Copland v. the UK and *Amann v. Switzerland* (Application no. 27798/95, Merits and Just Satisfaction, 16 February 2000). However, in those cases the interference concerned personal communication, while the Government argued that in *Bărbulescu* it concerned professional communication. This is an important nuance: should professional and personal correspondence and communication enjoy the same level of protection? Unfortunately, the *Bărbulescu* judgment omits the respective analysis and the Court simply concluded that all correspondence is covered by Article 8. However, it may be assumed that the level of protection may vary depending on whether the communication is personal or professional. If professional and personal correspondence enjoy the same level of protection, a reasoned explanation of that approach would be very helpful in understanding the legal aspects of surveillance in the workplace.

4. – In its admissibility analysis, the Court stated that the decisive factors of the admissibility of such cases are (i) whether an employee had a reasonable expectation of privacy (which is the case if the employee was not notified of the monitoring beforehand) and (ii) whether personal communication was tolerated by the company (*Bărbulescu v. Romania*, Supra n 1, at para 42). It follows from this approach that if no personal communication is allowed and the person was notified of the possible monitoring of his or her communications, an application to the European Court would be inadmissible. However, the Court decided that the case was admissible, even though the parties disagreed as to whether the applicant had been notified of the monitoring before the company had started it (*Bărbulescu v. Romania*, Supra n 1, at

para 43). Does this mean that the absence of prior notification in fact is not decisive for the admissibility of the case? It appears that a clear position of the Court as to the admissibility factors is absent from the judgment.

It is not clear whether these two factors (employer's tolerance and notification of the employee) were present in the case. Following the logic of the Court in absence of any of these factors the application should be declared inadmissible. However, in this case the Court did not find out whether both factors were present and proceeded to examine the case on the merits. It may appear to be contradictory.

Some commentators (S. Peers, *Is Workplace Privacy Dead? Comments on the Barbulescu judgment*, in *EU Law Analysis*, available at eulawanalysis.blogspot.fr , accessed 2-9-2016) argue that the crucial distinction between this case and the previous case-law on surveillance in the workplace was not the employer's tolerance, but the absence of notification of the monitoring. «That's a crucial distinction because it's not clear whether the employee knew about the surveillance in this case … Of course, the point has much broader relevance: there may be many other employers in Europe which have a blanket ban on employee use of the Internet, but which have not informed their employees about surveillance. Is that failure to inform crucial (*Copland*), or (apparently) not (*Bărbulescu*)? Or is it only crucial where the private use of employer equipment is not banned?» (*Steve Peers*, *ibid.*). It appears that internal regulations which place a blanket ban on personal use of the Internet in the workplace cannot justify the interception of personal messages and specific warning of monitoring should be given before its commencement. Otherwise, any employer could monitor any employee's correspondence merely on the basis of the relevant provision of the internal regulations. This could give employers total control. Unfortunately, the Court left the question of prior notification unanswered and did not underline the importance of such notification.

It appears from the facts of the case that the applicant had two Yahoo accounts: one, professional, installed at the request of the employer (*Bărbulescu v. Romania*, *supra* n. 1, at para 6), and another, private one (par. 31). The company monitored both of them. The Court did not examine the issue of the monitoring of the personal account and only looked into the question of the monitoring of the applicant's professional account: «The Court must therefore examine whether in the present case the applicant had a reasonable expectation of privacy when communicating from the Yahoo Messenger account that he had registered at his employer's request'» (par. 38). But what about his personal Yahoo Messenger account? Should the applicant have had an expectation of privacy in its regard? If the question is asked in a broader way, is communication from personal messengers or mail boxes in the workplace covered by the right to privacy? And, if it is prohibited to use the Internet for personal purposes, is no protection of personal communication to be expected? Can the right to privacy at the workplace be denied so easily if a company has internal regulations prohibiting to use the Internet for personal purposes?

5. – In the *Bărbulescu* case, the Court verified how the applicant's right to respect for his private life under Article 8 was balanced against the interest of the company in verifying that its employees were discharging their professional duties during working hours.

Certain commentators criticise the judgment because it did not explicitly consider all the criteria laid down in paragraph 2 of Article 8 of the Convention. In particular, the Court did not explain why the interference was 'in accordance with the law'. In fact, the threefold test of interference (an interference should be (1) based on law, (2) pursue a legitimate aim of public interest (3) be necessary, and proportionate) is applied to cases concerning negative obligations of the States. In positive obligation cases, however, this test is not used as the interference is not performed by the State but rather by a third party. The State's role in such cases is only to ensure that human rights are protected in private relationships. In cases concerning positive obligations, the Court applies a twofold test: «[…] the European Court has had to devise a specific method for reviewing compliance with positive obligations, being unable to apply in full the methods envisaged by the Convention for reviewing interference'»

(Jean-François Akandji-Kombe *Positive obligations under the European Convention on Human Rights. A guide to the implementation of the European Convention on Human Rights*, Council of Europe, 2007, 19).

The twofold test applied to positive obligation cases comprises the following elements. First, the Court examines the justifications for the domestic authorities' actions, i.e. whether there was a legitimate general interest. Secondly, it reviews the appropriateness of the State's conduct, which is analogous to the review of necessity and proportionality in the test applied to cases where States interfere with human rights. The Court applied the twofold test and came to the conclusion that there had been a fair balance between the applicant's right to respect for his private life and the interests of the company.

6. – It appears that the domestic courts balanced the right to respect for private life against different legitimate interests: professional discipline and protection of the company's IT system. As mentioned in the judgment, the first-instance court stated that «[s]ome of the reasons that make the employer's checks necessary are the possibilities that through use of the Internet employees could damage the company's IT systems, or engage in illicit activities in the company's name, or reveal the company's commercial secrets» (*Bărbulescu v. Romania*, Supra n 1, at para 10). In the final judgment, the national court stated that «… it cannot be held that …] the proper balance between the need to protect [the applicant's] private life and the right of the employer to supervise the functioning of its business was not struck» (*Bărbulescu v. Romania*, Supra n 1, at para 10). The European Court in its turn analysed the appropriateness of the interference as balanced against the general interest of the company to maintain discipline: «the Court finds that it is not unreasonable for an employer to want to verify that the employees are completing their professional tasks during working hours» (para. 59). As to the interest of the employer in maintaining its IT system undamaged, the Court only stated that no damage had been done: «it is true that it had not been claimed that the applicant had caused actual damage to his employer». Why did the Court refrain from balancing the need for the interference against all the interests of the company which were mentioned in the proceedings at the national level? Why did the Court neglect to balance the interference against the need to protect the IT system from harm? Moreover, the interest of maintaining discipline in the company may be open to criticism from the point of view of balancing that interest against the right to personal privacy. Can the requirement of discipline justify interference in personal life? If so, to what extent?

Yet another question is whether the employer must have a real suspicion of a breach of discipline before starting to monitor its employees? Or should companies be able to randomly monitor all their employees for the sake of checking on discipline? Probably not, as stated by Judge Pinto De Albuquerque in his partly dissenting opinion: «… only targeted surveillance based on well founded suspicions is admissible» (Para. 13 of the partly dissenting opinion of Judge Pinto De Albuquerque to the *Bărbulescu judgment*)

7. – On the basis of some of the arguments set out above, it appears that clearer, stricter rules on corporate surveillance of employees should be adopted by State parties to the ECHR. Otherwise, a general ban on personal communications at work could allow corporations to carry out unrestricted surveillance.

One of the main instruments in the European Union regulating personal data is the Directive 95/46/EC (Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OL J 281) which provides for instruction to the Member States to prohibit processing of personal data (*Bărbulescu v. Romania*, *supra* n 1, at para 18) and establishes a Data Protection Working Party ('DPWP') in order to examine the issue of surveillance of electronic communications in the workplace and to evaluate the implications of data protection for employees and employers. DPWP, an independent EU advisory body, in May 2002 produced the Working document on the surveillance and the monitoring of electronic communications in the

workplace. The document offers a list of four tests that any monitoring measure must pass: transparency, necessity, fairness and proportionality. Had these criteria been applied to the *Bărbulescu* case, the monitoring would not have passed the test.

First, transparency: transparency means that employees should be informed of any monitoring before it is carried out. As mentioned in section 0 above, the parties disagreed as to whether the applicant had been notified of the monitoring of his Yahoo account prior to the monitoring. It also appears that no notification of the monitoring of the private Yahoo account was given to the employee.

Secondly, necessity: again, there is the question of why the monitoring of the applicant's communications was necessary. The issue of the necessity of the monitoring is examined in section 0 above.

Thirdly, fairness: in relation to this point, the remarks of Steve Peers may be used as an illustration. «[I]n the presentation of the facts (at para 7), the accusation that the employee was using work equipment for personal reasons was based on placing him under surveillance. In other words, he was put under surveillance first. This isn't a minor quibble, because it raises an important question of whether employers which impose a general ban on the private use of work equipment have a general prerogative to place their employees under surveillance, or whether there must be some specific reason (such as the employee's denial of an accusation to that effect) to do so» (Steve Peers, *supra*).

How to guarantee that corporations act fairly when using their right to monitor employees' use of the Internet? As rightly stated by Judge Pinto De Albuquerque in his partly dissenting opinion, with reference to the Working party Working Document, «a blanket ban on personal use of the Internet by employees is inadmissible, as is any policy of blanket, automatic, continuous monitoring of Internet usage by employees» (Dissenting opinion, para 11). «Before implementing any concrete monitoring measure, the employer should assess whether the benefits of that measure outweigh the adverse impact on the right to privacy of the concerned employee and of third persons who communicate with him or her» (Dissenting opinion, para 11).

Fourthly, proportionality: the question here is who should decide whether the interference is proportionate? Can an assessment of proportionality made by a company which monitors its employees be considered as impartial? In this regard, an argument put forward by Judge Pinto De Albuquerque is very pertinent: «Unconsented collection, access and analysis of the employee's communications, including metadata, may be permitted only exceptionally, with judicial authorisation, since employees suspected of policy breaches in disciplinary or civil proceedings must not be treated less fairly than presumed offenders in criminal procedure. Only targeted surveillance in respect of well-founded suspicions of policy violations is admissible, with general, unrestricted monitoring being manifestly excessive snooping on employees» (Dissenting opinion, para 11).

Indeed, if monitoring by States requires court authorisation, why should corporations be able do it without any independent control? Should there be control by an independent body, such as a trade union, for example? How can we guarantee that the data collected will not be used for purposes other than those for which they were collected?

8. – Judge Pinto De Albuquerque raises another issue in his Dissenting opinion: «the transcripts of the messages in the applicant's personal account were made available to the applicant's colleagues and even discussed by them: Even if one were to accept that the interference with the applicant's right to respect for private life was justified in this case, which it was not, the employer did not take the necessary precautionary measures to ensure that the highly sensitive messages were restricted to the disciplinary proceedings. In other words, the employer's interference went far beyond what was necessary» (Dissenting opinion, para 20).

Yet another point to be considered by the Grand Chamber.

One of the Court's arguments in the case is that the domestic courts did not ground their conclusions on the content of the messages (Dissenting opinion, para 58). This means

that the content was not decisive for the national courts. Neither was it for the European Court. Why then was the information about the content of the messages, specifically sex and health related issues of the applicant mentioned in the judgment? (Dissenting opinion, para 58) Especially taking into account that such information is sensitive for every person who is the subject of it. It may be presumed that the content of the messages is disclosed in the judgment in order to specify the kind of data concerned, as there are special requirements when sensitive data is processed, and sensitive data includes sex and health issues (see whereas 10 and articles 2 and 8, Directive 95/46/EC). According to Steve Peers: «Another issue is that some of the data concerned the employee's health and sex life. EU law prohibits processing this and other 'sensitive' personal data. But this prohibition is a legal fiction, as in fact a number of grounds for processing sensitive data are permitted. In practice, it's more accurate to say that it's harder to justify processing such data. Applying that rule to this case, the Directive states that such data can be processed if 'necessary' to carry out the employer's obligations and rights 'in the specific field of employment law', if that is 'authorized by national law providing for adequate safeguards'. It's hard to know if these criteria were met in this case» (Steve Peers, *supra*).

The judgment does not contain an analysis related to special protection of sensitive personal data which would excuse such mention of the content of the applicant's personal messages. Should the European Court itself have refrained from touching upon the content of the messages by merely mentioning that the messages contained intimate or sensitive or very personal information? Is this a good example of the protection of personal life enshrined in Article 8 of the Convention?

9. – Today many employees use the Internet and communication programs, including e-mails, outside their working hours and office premises for work-related purposes. In such circumstances is it possible to limit the use of the Internet by employees to strictly professional purposes?

As stated by Judge Pinto De Albuquerque «Internet surveillance in the workplace is not at the employer's discretionary power. In a time when technology has blurred the dividing line between work life and private life, and some employers allow the use of company-owned equipment for employees» personal purposes, others allow employees to use their own equipment for work-related matters and still other employers permit both, the employer's right to maintain a compliant workplace and the employee's obligation to complete his or her professional tasks adequately does not justify unfettered control of the employee's expression on the Internet (Dissenting opinion, para 4).

Indeed, how can an employer expect employees not to use work equipment for personal purposes and at the same time require them to set up a messaging service designed for personal correspondence for professional use? Is there a balance?

The United Nations' Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression stated in his report on the use of encryption and anonymity in digital communications that «As e-mail, instant-messaging, Voice-over-Internet Protocols, videoconferencing and social media moved from niche services to predominant and easily monitored modes of communication, individuals developed a need for security online, so that they could seek, receive and impart information without the risk of repercussions, disclosure, surveillance… A common thread in the law is that, because the rights to privacy and to freedom of expression are so foundational to human dignity and democratic governance, limitations must be narrowly drawn, established by law and applied strictly and only in exceptional circumstances. In a digital age, protecting such rights demands exceptional vigilance» (David Kaye, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/HRC/29/32, 22 May 2015, available at www.ohchr.org).

It is thus crucial that individuals should enjoy privacy on line and that Governments should provide for this in law and policy.

There is an opportunity to lay down clearer guidelines in this domain. It is hoped that the Grand Chamber will clarify the limits of companies' surveillance of their employees and set out clear principles on the conditions of the legitimacy of surveillance. These could be based on existing regulations, such as those of the Working Party, and would not be less strict than the requirements applicable to surveillance by the State. If this is not done, there will be a loophole which could be used to the detriment of the protection of human rights and, in particular, to respect for privacy.