scripted

Volume 14, Issue 1, June 2017

European Court of Human Rights on Finding the Right Balance in Respect of Employer Email Monitoring – An Opportunity Missed!

*Julia Hörnle**

DOI: 10.2966/scrip.140117.100

* Professor of Internet Law, Queen Mary University of London, London, United Kingdom

1 The case

In the case of *Bărbulescu v Romania*[1] the European Court of Human Rights held that an employer's monitoring of their employee's instant messenger account and the disclosure of these communications (to the Applicant's colleagues) containing highly private, sensitive information was justified and therefore not a breach of Article 8 of the European Convention of Human Rights.

The Applicant, Mr Bărbulescu was dismissed after his employers had monitored his instant messaging use and he argued that the domestic court's failure to find that dismissal unlawful, even though it had been based on a breach of his right to privacy, meant that the domestic courts failed to protect his Article 8 rights. The Applicant is an engineer who had been employed by a private sector company as a sales manager from 2004 to 2007 and in this role, on his employer's request, he had created a Yahoo Messenger Account. The employer had a strict rule against the use of "computers, photocopiers, telephones, telex and fax machines for personal purposes" in its "internal regulations".[2] The wording of this rule (for a dismissal in 2007) indicates that the employer did not update their rules. On 3 July 2007 all employees of the company received a notice warning them that their activities were being surveilled and drawing their attention to the fact that another employee had just been dismissed for using the internet, telephone and photocopiers for personal purposes. But it is disputed between the parties whether the Applicant in fact received and acknowledged this notice of 3 July.

On 13 July 2007 the employer retrospectively informed the Applicant that his Yahoo Messenger Account had been monitored over the preceding nine days

---

1 *Bărbulescu v Romania*, App no 61496/08 (ECtHR, 12 January 2016).

2 *Ibid.*, 2.

and that this monitoring showed that he had used the account for personal purposes in breach of the "internal regulations". At that point the Applicant replied in writing (untruthfully) that he had used the account only for professional purposes. In response the employer presented him with an extensive, 45-page transcript of his communications with his fiancée and his brother which he had engaged in over these nine days and they were of a personal, intimate nature containing information about the Applicant's health and sex life. The transcript also contained five brief messages exchanged with his fiancée from his private Yahoo Messenger Account, which did not contain any intimate information. The Applicant's employment was terminated on 1 August 2007 for breach of the "no personal use" rule in the company's internal regulations.

The Applicant brought proceedings before the local Romanian Court claiming unfair dismissal on the basis that by accessing his instant messages, his former employer had breached his right to privacy guaranteed in the Romanian Constitution and the Criminal Code which creates an offence in respect of illegal access. That Court found that the Applicant had been duly informed of his former employers' internal regulations and held that whether or not the monitoring was illegal did not affect the *lawfulness of the dismissal* in the instant case. The Court pointed out that the Applicant had stated in writing that he had not used the account for personal purposes and therefore could not complain that his employer monitored it. The Romanian Court held that monitoring the communications was the only way for the employer to check whether the employee had breached the "no private use" rule and that monitoring of employees' use of company computers was more broadly necessary for employers to check how employees carry out the tasks assigned to them. Therefore, the Romanian Court found that, provided employees are properly informed of the monitoring, it was not unlawful or unfair in the context of

employment law. Here the Romanian Court referred to the notice given to the employees on 3 July and therefore found that the Applicant's dismissal had been lawful.

On 17 July 2008 in a final decision the Bucharest Court of Appeal dismissed the Applicant's appeal who subsequently lodged this application before the ECtHR.

The ECtHR set out the relevant domestic law, the relevant provisions of the 1981 Council of Europe Data Protection Convention, the relevant provisions of the EU Data Protection Directive 1995/46/EC, including the prohibition in Article 8(1) to process sensitive data such as that pertaining to health or sex life, the Article 29 Working Party Opinion 8/2001 on the processing of personal data in an employment context and the Article 29 Working Party Working Document on the surveillance and monitoring of electronic communications in the workplace of May 2002.

The former Opinion sets out the following key principles: finality, transparency, legitimacy, proportionality, accuracy, security and staff awareness and setting out a balancing act between the risks an employer faces and the legitimate privacy and other interests of workers. The latter Working Document makes clear that the employer's interests and convenience alone do not justify an intrusion into employees' privacy and sets out as the main principles: transparency, necessity, fairness and proportionality. It also emphasises the importance of notice/warnings to the employee and points out that access to workplace communications may be necessary for a variety of reasons, not limited to performance and other monitoring, but also, for example, if another employee needs to take over the work of a colleague etc.

The ECtHR held that, at least in the absence of a warning, employees had a reasonable expectation of privacy in respect of telephone calls made from business premises and in respect of email and other internet communications,

such that the monitoring of these communications fell within the protection of private life in Article 8(1).[3] So Article 8(1) was clearly engaged in the workplace. However, the Court held that this case was different from *Halford* and *Copland*, in which the personal use of an office telephone was allowed or at least tolerated in practice.[4]

The ECtHR pointed out that the context of the case were disciplinary proceedings and the lawfulness of dismissal under employment law, not the adequateness of privacy protection under national law (and the national law did provide, for example, for a criminal offence in respect of interception of private communications).[5] The Court noted that the assessment from the court file whether the employee had a reasonable expectation of privacy was impossible. The question of whether the employee was given the notice on 3 July was disputed between the parties and the court file did not disclose whether the notice had been signed by the employee as claimed by the Romanian government. This factual issue, however, was for the Romanian Courts to decide. The only issue the ECtHR decided here was that Article 8(1) was engaged, but that the monitoring may well be justified by Article 8(2).

The Court reiterated its stance that states not only have a negative duty not to interfere with an individual's privacy, but also a positive obligation to protect individuals against unjustified interference of their privacy by third parties.[6] Here the ECtHR had to examine whether Romania (through her courts) has struck a fair balance between the privacy interests of the Applicant and the

---

3 *Ibid.*, para. 36; see also *Copland v UK*, ECHR 2007-I 62617/00, para. 41; *Halford v UK*, ECHR 1997-III 20605/92, paras. 44-45; *Amann v Switzerland*, ECHR 2000-II 27798/95, para. 43.

4 *Bărbulescu v Romania*, para. 39.

5 *Ibid.*, para. 41.

6 *Ibid.*, para. 52; citing *Von Hannover v. Germany (no. 2)*, [GC] ECHR 2012-I 40660/08 and 60641/08, para. 57; *Benediksdóttir v. Iceland*, App no 38079/06 (ECtHR, 16 June 2009).

employers' interests to run and protect their business. The Court noted that the Applicant had had the opportunity to raise his case in the domestic courts and these courts found that the dismissal was fair in accordance with local employment law, as he had used Yahoo Messenger during working hours for private purposes in breach of his contract.[7]

The Court also stated that the Romanian Courts had found that the employer accessed the employee's Account in the mistaken belief that it contained only professional communications and that this belief was based on the employee's (untruthful) assertions to that effect.[8] This argument based on the findings of the Romanian Courts seems illogical, as the facts of the case set out in the judgment seem to state that the employer *first* monitored the account *before* the employee subsequently, falsely stated that he had used the account only for professional purposes.[9] There is therefore an internal, unexplained inconsistency in the ECtHR's interpretation of the facts as found by the Romanian Courts.

Furthermore, the Court also stated that the content accessed from the Messenger Account as such did not determine the outcome of the Romanian Courts' decisions on the lawfulness of the dismissal[10] – again this argument seems irrelevant as it seems to be based on a misconception of the notion of privacy. The Applicant's privacy has been adversely affected[11] irrespective of whether or not the private nature of the content affected the assessment of the dismissal claim. For an assessment under Article 8(1) the only relevant question is whether the interference is justified.

---

7 *Bărbulescu v Romania*, para. 56.
8 *Ibid.*, para. 57.
9 *Ibid.*, para. 7.
10 *Ibid.*, para. 58.
11 Regardless of the question whether this invasion of privacy was justified or unjustified.

The ECtHR also stated that the fact that the private nature of the communications had not harmed the employer's business as such (in the sense that the employee had not disclosed any trade secrets or engaged in anti-competitive behaviour) did not mean that the monitoring was not justified, as he had clearly been cyberslacking and wasting his employers' resources and working time.[12] Finally, the Court said the interference with the employee's privacy was proportionate as the company had only monitored the employee's Yahoo Messenger Account and not his other communication channels or documents on his computer and that there was no explanation from the employee as to why he did use his work Yahoo Messenger Account for these private communications.[13] The Court therefore concluded that there was no reason to interfere with the judgment by the Romanian Courts, holding that their finding that the surveillance was in accordance with Romanian labour law did not unlawfully impinge on the Applicant's Article 8 rights. The Court found that there was no violation of Article 8.[14]

2 Analysis

The judgment of the majority of the ECtHR is very deferent to the decisions made by the Romanian Courts – the Court effectively refuses to engage with the requirements of the proportionality test in employment monitoring cases, and does not answer the difficult question to what extent an employer's strict "no private use of the internet" rule is compliant with Article 8(1). This deference effectively means that the Court gave very little guidance on the question of when monitoring is proportionate and therefore justified by Article 8(2). According to

12 *Bărbulescu v Romania*, para. 58.
13 *Ibid.*, paras. 60-61.
14 *Ibid.*, paras. 62-63.

this judgment, it seems that the Contracting States have discretion as to whether or not they allow employers to impose a strict "no private internet use" rule under their national laws.

The ruling restricts employers' discretion in two respects: firstly, the ECtHR made clear that notice of the fact that monitoring takes place must be given to employees – thus transparency is the absolute minimum for compliance with the right to privacy; and secondly, the Court also seemed to indicate that the blanket monitoring of all the internet communications of an employee was disproportionate.

However, the Court abstained from taking this opportunity from giving guidance as to what transparency means in these cases and whether there are other requirements (such as proving that the monitoring is necessary for a specific purpose).

As Judge Paulo Pinto de Albuquerque pointed out in his partially dissenting opinion, "the case presented an excellent occasion for the Court to develop its case-law in the field of protection of privacy with regard to employees' Internet communications".[15] This is an opportunity which has been missed.

Three aspects stand out here and it would have been helpful if the Court had provided guidance on them: 1) the question of whether a rule which *completely* prohibits the private use of workplace computers, phones, emails and other internet facilities can be legitimate, necessary and proportionate; 2) the question of *what type of notice* is required informing employees about what, if any, private use is allowed and warning them that monitoring takes place; and 3)

[15] *Ibid.*, opinion of Judge Pinto de Albuquerque, para. 2.

whether the right to privacy requires that employers show that the monitoring is *necessary for a specific and legitimate purpose* as part of the proportionality analysis.

The judgment does not really apply the proportionality test, by balancing and weighing the conflicting interests of the employer and the employee. As Judge Pinto de Albuquerque stated, the pursuit of *maximum* profitability and productivity from the workforce is not a legitimate purpose, and that therefore the Court should have examined in more detail what the legitimate interest was in this particular case and whether it falls within the legitimate objective of the employer to ensure that employees fulfil their contractual obligations under the employment contract.[16] The proportionality analysis requires necessity and therefore a blanket ban on all private internet use and comprehensive surveillance of all internet communications was an infringement of the right to privacy.[17] In this case, the employer had not proven that it had a proportionate internet policy nor that the employee had been notified of it before the monitoring started. Furthermore, the case concerned particularly sensitive personal information sent to an account labelled "Andra loves you", clearly not related to the employee's professional tasks. The transcripts of the messages were made available to the applicant's colleagues and discussed by them. Thus, the employer did not restrict access on a need-to-know basis.[18] By finding the dismissal justified, the Romanian Courts confirmed the violation of the applicant's privacy and therefore Judge Pinto de Albuquerque found in his dissenting Opinion that there was a breach of Article 8 by Romania.[19]

---

16 *Ibid.*, opinion of Judge Pinto de Albuquerque, para. 5.
17 *Ibid.*, opinion of Judge Pinto de Albuquerque, paras. 11, 13, and 14.
18 *Ibid.*, opinion of Judge Pinto de Albuquerque, paras. 19-20.
19 *Ibid.*, opinion of Judge Pinto de Albuquerque, para. 23.

> Internet surveillance in the workplace runs the risk of being abused by employers acting as distrustful Big Brother lurking over the shoulders of their employees, as though the latter had sold not only their labour but also their personal lives to employers.[20]

The more clear and transparent employers are about these rules and about their monitoring, the more likely it is that employees can adjust their behaviour (by using their own private facilities, such as their own laptop/tablet computer or mobile phone and by setting up their own private email/instant messaging etc. accounts). Therefore, employers should have a clear and comprehensive policy on internet use in the workplace.[21]

Arguably in the day and age of cloud computing and remote storage and greater mobility of devices (such as smartphones and tablets) there is less of a need for an employee to use his or her employer's facilities to access the internet. By the same token modern working environments frequently mean that there is no longer a clear and distinct separation between the employee's private space and the workplace – as employees sometimes use their own device for work (BYOD) at home or at the workplace, and frequently work from their employer's device outside the workplace at home or while travelling. The mixing of private and work-related use in the same device or at the same cloud storage facility makes both the employer's security concerns *and* the employee's privacy concerns more acute.

This also raises the question of what constitutes use of an employer's facilities – clearly this could be the use of (physical) computer devices, use of remote cloud computing accounts (e.g. Dropbox) or access to the employer's

---

[20] *Ibid.*, opinion of Judge Pinto de Albuquerque, para. 15.
[21] *Ibid.*, opinion of Judge Pinto de Albuquerque, para. 10.

network/wifi network. The point here is that the question of allowable monitoring is no longer limited to a physical device (such as a phone, printer, or computer) but unavoidably includes internet access and network use.

The case also raises the question of duties of the employer during and after the monitoring, and in particular ensuring that the contents are not widely disclosed, an issue which the judgment does not really address, but arguably which should have been addressed as part of the proportionality analysis.

Ironically, an employer who imposes a strict (draconian) no access to the internet for private purposes rule and who provides notice and transparency about this policy and about any monitoring which takes place will find it easier to argue that the employees' privacy has not been unjustifiably infringed, as the employees have no expectation of privacy. By contrast, an employer who tolerates some private use (including a BYOD) may have to be more careful in not invading employees' privacy through monitoring. This is one reason for a stricter, less tolerant policy. However, there are other good commercial reasons for a more tolerant policy: allowing some private use will lead to greater work efficiency and greater employee satisfaction, especially if the security aspects can be managed without intrusive monitoring. Furthermore, a strict "no private use" rule may breach an emerging (and by no means established) new right of internet access.

Judge Pinto de Albuquerque explicitly discusses access to the internet as a human right referring to the Court's recognition that the internet "provides an unprecedented platform for the exercise of freedom of expression" in cases such as *Delfi* and *Ahmet Yildrim*.[22] He held that internet communications are privileged, whether sent from the employee's own or the employer's device, and that

[22] *Ibid.*, opinion of Judge Pinto de Albuquerque, para. 3.

therefore strict limits must apply to internet surveillance carried out by the employer.[23] This protection applied inside and outside working hours and not only to content, but also to metadata according to Judge Pinto de Albuquerque.[24] Interestingly he derives the right to internet access from both the Article 8 right to privacy and the Article 10 right to freedom of expression and hence, both sets of restrictions, namely Article 8(2) (in particular the rights and freedoms of the employer and other employees) and Article 10(2) (such as the protection of the reputation or rights of the employer or other employees and the prevention of the disclosure of information received in confidence) apply. Hence, the grounds for restricting the right can be found in Article 8(2) and Article 10(2).[25]

This is relevant in the context of employees' internet monitoring as many employees have difficulties in practice avoiding using their employers' facilities for accessing the internet during working hours (for example, even if they use their own device and their own accounts, they are likely to use their employers' internet connection, such as wifi). The consequence of allowing employers to completely ban any internet access for private purposes at the workplace or during working hours severely limits employees' access to the internet. If internet access emerges as a new human right,[26] this would mean that employers

---

23 *Ibid*.

24 *Ibid.*, opinion of Judge Pinto de Albuquerque, para. 5.

25 *Ibid*.

26 See for example the Note by the UN Secretary General, A/68/362 of 4 September 2013 "Promotion and protection of the right to freedom of opinion and expression", para. 18 (Frank La Rue) and A/HRC/32/38 of 16 May 2016 UN Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (David Kaye). See also the French Constitutional Council Decision, No. 2009/580DC, 10 June 2009, para. 12; see also for example Colin Crawford, "Cyberplace: Defining a Right to Internet Access through Public Accommodation Law" (2003) 76 *Temp Law Review* 225-280; but c.f. Paul de Hert and Dariusz Kloza, "Internet (Access) as a New Fundamental Right. Inflating the Current Rights Framework?" (2012) 3(3) *European Journal of Law and Technology*.

could not entirely ban an employee's internet access, but only to the extent that this is necessary and proportionate.

Of interest is also a doctrine of German human rights protection, established by the German Constitutional Court in different contexts, namely the "Kernbereichslehre"[27] (core protection doctrine), according to which the most personal and intimate sphere of a human life is absolutely protected against infringements.[28] An employer monitoring employees' internet communications may not know whether or not it will find highly personal or sensitive communications. However, if all communications of employees are monitored (and in particular if this is combined with other forms of surveillance, such as audio and video-surveillance), this total surveillance makes it more likely that personal and intimate communications (and conduct) are captured. Thus, the intensity of surveillance has a direct impact on the sensitivity of the content likely to be disclosed. Thus, this doctrine can be used as an argument that the right to privacy is infringed by total surveillance.

Therefore, two strands of this judgment stand out: 1) the Court's reluctance to engage in a proportionality analysis on employees' workplace monitoring and 2) the mentioning of the right to internet access in the dissenting Opinion. Both will provide food for further development in later cases and it is to be hoped that a future court would be more willing to engage in the proportionality issues raised by employment monitoring cases.

---

[27] See further Ilmer Dammann, *Der Kernbereich der privaten Lebensgestaltung. Zum Menschenwürde-und Wesensgehaltsschutz im Bereich der Freiheitsgrundrechte* (Berlin: Duncker & Humblot, 2011).

[28] See for example BVerfG 109, 279 "Grosser Lauschangriff" concerning audio surveillance of suspects' homes – which is not justified if it is done in such a way that it intrudes on a person's most intimate sphere, and the proportionality principles does not apply.