EELA EUROPEAN EMPLOYMENT LAWYERS ASSOCIATION

SUMMARY

ECtHR 12 January 2016, application 61496/08. (Bărbulescu), Fundamental Rights

Summary

An employee was dismissed for using a professional Yahoo account privately in breach of his employer's regulations, which strictly prohibited personal use of the company's resources. The domestic courts dismissed his complaint regarding breach of Article 8 ECHR. The ECtHR, distinguishing the case from those in its judgments in Halford and Copland, agreed with those courts by six votes to one. A partly dissenting opinion provides an in-depth analysis of the rules on interception of private emails by employers.

Facts

The applicant, Bogdan Mihai Bărbulescu, is a Romanian national who was born in 1979 and lives in Bucharest.From 1 August 2004 until 6 August 2007 Mr Bărbulescu was employed by a private company as an engineer in charge of sales. At his employers' request, he created a Yahoo Messenger account for the purpose of responding to clients' enquiries. On 13 July 2007 Mr Bărbulescu was informed by his employer that his Yahoo Messenger communications had been monitored from 5 to 13| July 2007 and that the records showed he had used the internet for personal purposes. Mr Bărbulescu replied in writing that he had only used the service for professional purposes. He was presented with a transcript of his communication including transcripts of messages he had exchanged with his brother and his fiancée relating to personal matters such as his health and sex life. On 1| August 2007 the employer terminated Mr Bărbulescu's employment contract for breach of the company's internal regulations that prohibited the use of company resources for personal purposes.

National proceedings

Mr Bărbulescu challenged his employer's decision before the courts complaining that the decision to terminate his contract was null and void as his employer had violated his right to correspondence in accessing his communications in breach of the Constitution and Criminal Code. His complaint was dismissed on the grounds that the employer had complied with the dismissal proceedings provided for by the Labour Code and that Mr Bărbulescu had been duly informed of the company's regulations. Mr Bărbulescu appealed claiming that e-mails were protected by Article 8 (right to respect for private and family life, the home and correspondence) of the European Convention and that the first-instance court had not allowed him to call witnesses to prove that his employer had not suffered as a result of his actions. In a final decision on 17 June 2008 the Court of Appeal dismissed his appeal and, relying on EU law, held that the employer's conduct had been reasonable and that the monitoring of Mr Bărbulescu's communications had been the only method of establishing whether there had been a disciplinary breach. Furthermore, the Court of Appeal held that the evidence before the first-instance court had been sufficient.On 15 December 2008, Mr Barbulescu lodged an application with the ECtHR, complaining that his employer's decision to terminate his contract had been based on a breach of his privacy and that the proceedings before the domestic courts had been unfair.Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (the "Convention") provides:

"1. Everyone has the right to respect for his private and family life, his home and his correspondence.2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

ECtHR's findings

-

The Court noted that it was not disputed that the applicant's employer's internal regulations strictly prohibited employees from using the company's computers and resources for personal purposes. It follows that the case is different from the Halford and Copland cases, in which the personal use of an office telephone was allowed or, at least, tolerated (§| 38-39).

-
The Government claimed that the applicant had been given proper prior notice that his employer could have monitored his communications, but the applicant denied having received such specific prior notice (§ 43).

-
Both the County Court and the Court of Appeal attached particular importance to the fact that the employer had accessed the applicant's Yahoo Messenger account in the belief that it had contained professional messages, since the latter had initially claimed that he had used it in order to advise clients. It follows that the employer acted within its disciplinary powers since, as the domestic courts found, it had accessed the Yahoo Messenger account on the assumption that the information in question had been related to professional activities and that such access had therefore been legitimate (§ 57).

-
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 (§58).

-
While it is true that it had not been claimed that the applicant had caused actual damage to his employer, 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 (§59).

-
In addition, the Court notes that it appears that the communications on his Yahoo Messenger account were examined, but not the other data and documents that were stored on his computer. It therefore finds that the employer's monitoring was limited in scope and proportionate (§60).

-
Furthermore, the Court finds that the applicant has not convincingly explained why he had used the Yahoo messenger account for personal purposes (§61).

-
Having regard to the foregoing, the Court concludes in the present case that there is nothing to indicate that the domestic authorities failed to strike a fair balance, within their margin of appreciation, between the applicant's right to respect for his private life under Article 8 and his employer's interests. There has accordingly been no violation of Article 8 of the Convention (§62-63).

-
As for the applicant's complaint that the domestic proceedings had been unfair, he was able to raise this argument before the Court of Appeal, which ruled, in a sufficiently reasoned decision, that hearing additional witnesses was not relevant to the case. The decision was delivered in a public hearing conducted in an adversarial manner and does not seem arbitrary. It follows that this complaint is manifestly ill-foun|ded and must be rejected (§64-66).

Judgment

The ECtHR held, by six votes to one, that there has been no violation of Article 8 of the Convention.

Judge Pinto de Albuquerque's partly dissenting opinion:

"Bărbulescu v. Romania concerns the surveillance of Internet usage in the workplace. The majority accept that there has been an interference with the applicant's right to respect for private life and correspondence within the meaning of Article 8 of the European Convention on Human Rights ("the Convention"), but conclude that there has been no violation of this Article, since the employer's monitoring was limited in scope and proportionate. I share the majority's starting point, but I disagree with their conclusion.[....]The case presented an excellent occasion for the European Court of Human Rights ("the Court") to develop its case-

law in the field of protection of privacy with regard to employees' Internet communications[1]. The novel features of this case concern the non-existence of an Internet surveillance policy, duly implemented and enforced by the employer, the personal and sensitive nature of the employee's communications that were accessed by the employer, and the wide scope of disclosure of these communications during the disciplinary proceedings brought against the employee. These facts should have impacted on the manner in which the validity of the disciplinary proceedings and the penalty was assessed. Unfortunately, both the domestic courts and the Court's majority overlooked these crucial factual features of the case.[....]Internet surveillance in the workplace is not at the employer's discretionary power. In a time when technology has blurred the diving 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. Even where there exist suspicions of cyberslacking, diversion of the employer's IT resources for personal purposes, damage to the employer's IT systems, involvement in illicit activities or disclosure of the employer's trade secrets, the employer's right to interfere with the employee's communications is not unrestricted. Given that in modern societies Internet communication is a privileged form of expression, including of private information, strict limits apply to an employer's surveillance of Internet usage by employees during their worktime and, even more strictly, outside their working hours, be that communication conducted through their own computer facilities or those provi|ded by the employer.The Convention principle is that Internet communications are not less protected on the sole ground that they occur during working hours, in the workplace or in the context of an employment relationship, or that they have an impact on the employer's business activities or the employee's performance of contractual obligations. This protection includes not only the content of the communications, but also the metadata resulting from the collection and retention of communications data, which may provide an insight into an individual's way of life, religious beliefs, political convictions, private preferences and social relations. In the absence of a warning from the employer that communications are being monitored, the employee has a "reasonable expectation of privacy". Any interference by the employer with the employee's right to respect for private life and freedom of expression, including the mere storing of personal data related to the employee's private life, must be justified in a democratic society by the protection of certain specific interests covered by the Convention, namely the protection of the rights and freedoms of the employer or other employees (Article 8 § 2) or the protection of the reputation or rights of the employer or other employees and the prevention of the disclosure of

information received by the employee in confidence (Article 10 § 2). Hence, the pursuit of maximum profitability and productivity from the workforce is not per se an interest covered by Article 8 § 2 and Article 10 § 2, but the purpose of ensuring the fair fulfilment of contractual obligations in an employment relationship may justify certain restrictions on the above-mentioned rights and freedoms in a democratic society.Other than the Court's case-law, the international standards of personal data protection both in the public and private sectors have been set out in the 1981 Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data. In this Convention the protection of personal data was for the first time guaranteed as a separate right granted to an individual. Specific rules for data protection in employment relations are contained in the Council of Europe Committee of Ministers Recommendation Rec(89)2 to member states on the protection of personal data used for employment purposes, 18 January 1989, recently replaced by Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment. Also extremely valuable in this context are Recommendation No.R(99) 5 for the protection of privacy on the Internet, adopted on 23 February 1999, and Recommendation CM/Rec(2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling, adopted on 23 November 2010.In the legal framework of the European Union (EU), respect for private life and protection of personal data have been recognised as separate fundamental rights in Articles 7 and 8 of the EU Charter of Fundamental Rights. The central piece of EU legislation is Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Employment relations are specifically referred to only in the context of the processing of sensitive data. Regulation (EC) No 45/2001 lays down the same rights and obligations at the level of the EC institutions and bodies. It also establishes an independent supervisory authority with the task of ensuring that the Regulation is complied with. Directive 2002/58/EC concerns the processing of personal data and the protection of privacy in the electronic communications sector, regulating issues like confidentiality, billing and traffic data and spam. The confidentiality of communications is protected by Article 5 of the Directive, which imposes on Member States an obligation to ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular they are to prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so. The interception of communications over private networks, including e-mails, instant messaging services, and phone calls, and generally private communications, are not covered, as the

Directive refers to publicly available electronic communications services in public communication networks. Also relevant is 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, which specifies that Member States may not impose general monitoring obligations on providers of internet/email services, because such an obligation would constitute an infringement of freedom of information as well as of the confidentiality of correspondence (Article 15). Within the former third pillar of the EU, Framework Decision 2008/977/JHA dealt with the protection of personal data processed in the framework of police and judicial co-operation in criminal matters. Finally, Article 29 Working Party Opinion 8/2001 on the processing of personal data in the employment context, adopted on 13 September 2001, the Working Document on the surveillance and the monitoring of electronic communications in the workplace, adopted on 29 May 2002, the Working Document on a common interpretation of Article 26(1) of Directive 95/46/EC, adopted on 25 November 2005, and Article 29 Working Party Opinion 2/2006 on privacy issues related to the provision of email screening services, adopted on 21 February 2006, are also important for setting the standards of data protection applicable to employees in the EU. In its 2005 annual report, the Working Party affirmed that "[i]t is not disputed that an e-mail address assigned by a company to its employees constitutes personal data if it enables an individual to be identified".Finally, both the 1980 Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, and the International Labour Office's 1997 Code of Practice on the protection of workers' personal data, provide important soft-law guidance to employers, employees and courts.From this international legal framework, a consolidated, coherent set of principles can be drawn for the creation, implementation and enforcement of an Internet usage policy in the framework of an employment relationship. Any information related to an identified or identifiable employee that is collected, held or used by the employer for employment purposes, including with regard to private electronic communications, must be protected in order to respect the employee's right to privacy and freedom of expression. Consequently, any processing of personal data for the purposes of recruitment, fulfilment or breach of contractual obligations, staff management, work planning and organisation and termination of an employment relationship in both the public and private sectors must be regulated either by law, collective agreement or contract. Particular forms of personal data processing, for example of the employees' usage of Internet and electronic communications in the workplace, warrant detailed regulation.Hence, a comprehensive Internet usage policy in the workplace must be put in place, including specific rules on the use of email, instant messaging, social networks, blogging and web surfing. Although policy may be tailor-made to the needs of each corporation as a whole and each sector of the corporation infrastructure in

particular, the rights and obligations of employees should be set out clearly, with transparent rules on how the Internet may be used, how monitoring is conducted, how data is secured, used and destroyed, and who has access to it.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. Personal data relating to racial origin, political opinions or religious or other beliefs, as well as personal data concerning health, sexual life or criminal convictions are considered as "sensitive data" requiring special protection.Employees must be made aware of the existence of an Internet usage policy in force in their workplace, as well as outside the workplace and during out-of-work hours, involving communication facilities owned by the employer, the employee or third parties. All employees should be notified personally of the said policy and consent to it explicitly. Before a monitoring policy is put in place, employees must be aware of the purposes, scope, technical means and time schedule of such monitoring. Furthermore, employees must have the right to be regularly notified of the personal data held about them and the processing of that personal data, the right to access all their personal data, the right to examine and obtain a copy of any records of their own personal data and the right to demand that incorrect or incomplete personal data and personal data collected or processed inconsistently with corporation policy be deleted or rectified. In event of alleged breaches of Internet usage policy by employees, opportunity should be given to them to respond to such claims in a fair procedure, with judicial oversight.The enforcement of an Internet usage policy in the workplace should be guided by the principles of necessity and proportionality, in order to avoid a situation where personal data collected in connection with legitimate organisational or information-technology policies is used to control employees' behaviour. 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. 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. The least intrusive technical means of monitoring should be preferred. Since blocking Internet communications is a measure of last resort, filtering mechanisms may be considered more appropriate, if at all necessary, to avoid policy infringements. The collected data may not be used for any purpose other than that originally intended, and must be protected from alteration, unauthorised access and any other form of misuse. For example, the collected data must not be made available to other employees who are not concerned by it. When no longer needed, the collected personal data

should be deleted.Breaches of the internal usage policy expose both the employer and the employee to sanctions. Penalties for an employee's improper Internet usage should start with a verbal warning, and increase gradually to a written reprimand, a financial penalty, demotion and, for serious repeat offenders, termination of employment. If the employer's Internet monitoring breaches the internal data protection policy or the relevant law or collective agreement, it may entitle the employee to terminate his or her employment and claim constructive dismissal, in addition to pecuniary and non-pecuniary damages.Ultimately, without such a policy, Internet surveillance in the workplace runs the risk of being abused by employers acting as a 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. In order to avoid such commodification of the worker, employers are responsible for putting in place and implementing consistently a policy on Internet use along the lines set out above. In so doing, they will be acting in accordance with the principled international-law approach to Internet freedom as a human right."

Creator: European Court of Human Rights (ECtHR)
Verdict at: 2016-01-12
Case number: 61496/08