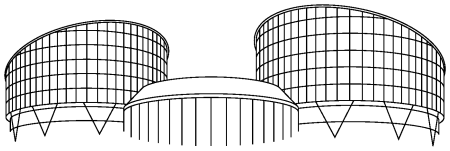

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

FOURTH SECTION

CASE OF BĂRBULESCU v. ROMANIA

(Application no. 61496/08)

JUDGMENT

STRASBOURG

12 January 2016

This judgment will become final in the circumstances set out in Article 44 § 2 of the Convention. It may be subject to editorial revision.

In the case of Bărbulescu v. Romania,

The European Court of Human Rights (Fourth Section), sitting as a Chamber composed of:

András Sajó, *President,*
Vincent A. De Gaetano,
Boštjan M. Zupančič,
Nona Tsotsoria,
Paulo Pinto de Albuquerque,
Egidijus Kūris,
Iulia Antoanella Motoc, *judges,*
and Fatoş Aracı, *Deputy Section Registrar,*

Having deliberated in private on 1 December 2015,

Delivers the following judgment, which was adopted on that date:

PROCEDURE

1. The case originated in an application (no. 61496/08) against Romania lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by a Romanian national, Mr Bogdan Mihai Bărbulescu ("the applicant"), on 15 December 2008.

2. The applicant was represented by Mr D. Costinescu and Mr O. Juverdeanu, lawyers practising in Bucharest. The Romanian Government ("the Government") were represented by their Agent, Ms C. Brumar, of the Ministry of Foreign Affairs.

3. The applicant alleged, in particular, that his employer's decision to terminate his contract had been based on a breach of his right to respect for his private life and correspondence and that the domestic courts had failed to protect his right.

4. On 18 December 2012 the application was communicated to the Government.

THE FACTS

I. THE CIRCUMSTANCES OF THE CASE

5. The applicant was born in 1979 and lives in Bucharest.

6. From 1 August 2004 to 6 August 2007, he was employed by a private company ("the employer") as an engineer in charge of sales. At his

employer's request, he created a Yahoo Messenger account for the purpose of responding to clients' enquiries.

7. On 13 July 2007 the employer informed the applicant that his Yahoo Messenger communications had been monitored from 5 to 13 July 2007 and that the records showed that he had used the Internet for personal purposes, contrary to internal regulations. The applicant replied in writing that he had only used Yahoo Messenger for professional purposes. When presented with a forty-five-page transcript of his communications on Yahoo Messenger, the applicant notified his employer that, by violating his correspondence, they were accountable under the Criminal Code. The forty-five pages contained transcripts of all the messages that the applicant had exchanged with his fiancée and his brother during the period when his communications had been monitored; they related to personal matters involving the applicant. The transcript also contained five short messages that the applicant had exchanged with his fiancée on 12 July 2007 using a personal Yahoo Messenger account; these messages did not disclose any intimate information.

8. On 1 August 2007 the employer terminated the applicant's employment contract for breach of the company's internal regulations which stated, *inter alia*:

> "It is strictly forbidden to disturb order and discipline within the company's premises and especially ... to use computers, photocopiers, telephones, telex and fax machines for personal purposes."

9. The applicant challenged his employer's decision before the Bucharest County Court ("the County Court"). He complained that this decision had been null and void since, by accessing his communications, his employer had violated his right to correspondence protected by the Romanian Constitution and the Criminal Code.

10. In a judgment of 7 December 2007, the County Court dismissed his complaint on the grounds that the employer had complied with the dismissal proceedings provided for by the Labour Code and noted that the applicant had been duly informed of the employer's regulations that prohibited the use of company resources for personal purposes. The County Court's judgment reads, in its relevant parts:

> "The court takes the view that the monitoring of the [applicant]'s Yahoo Messenger communications from the company's computer ... during working hours – regardless of whether the employer's actions were or were not illegal (*îmbracă sau nu forma ilicitului penal*) – cannot affect the validity of the disciplinary proceedings in the instant case...
>
> However, since the [applicant] claimed during the disciplinary proceedings that he had not used Yahoo Messenger for personal purposes but rather for advising clients on the products offered by his employer, the court finds that checking the content of the [applicant]'s communications was the only method for the employer to verify the [applicant]'s line of defence.

> The employer's right to monitor their employees' use of the company's computers in the workplace falls within the broad scope of the right to check the manner in which professional tasks are complete.
>
> As long as the employees' attention ... had been drawn to the fact that, not long before the applicant had received a disciplinary sanction, another colleague had been dismissed for having used the Internet, the telephone and the photocopiers for personal purposes and they had been warned that their activity was under surveillance (see notice no 2316 of 3 July 2007 that the applicant had signed ...) it cannot be held against the employer that he had not proven transparency and that he had not been open with regard to his activities in monitoring the use of the computers by its employees.
>
> The Internet in the workplace must remain a tool at the employee's disposal. It was granted by the employer for professional use and it is indisputable that the employer, by virtue of the right to monitor the employees' activities, has the prerogative to keep personal use of the Internet monitored.
>
> Some 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."

11. The applicant appealed against this judgment. He claimed that e-mails were also protected by Article 8 of the Convention as pertaining to "private life" and "correspondence". He also complained that the County Court had not allowed him to call witnesses to prove that the employer had not suffered as a result of his actions.

12. In a final decision of 17 June 2008, the Bucharest Court of Appeal ("the Court of Appeal") dismissed his appeal and upheld the judgment rendered by the County Court. Relying on EU Directive 95/46/EC, the Court of Appeal ruled that the employer's conduct had been reasonable and that the monitoring of the applicant's communications had been the only method of establishing if there had been a disciplinary breach. With regard to his procedural rights, the Court of Appeal dismissed the applicant's arguments, stating that the evidence already before it was sufficient. The Court of Appeal's decision reads, in its relevant parts:

> "In view of the fact that the employer has the right and the obligation to ensure the functioning of the company and, to this end, [the right] to check the manner in which its employees complete their professional tasks, and of the fact that [the employer] holds the disciplinary power of which it can legitimately dispose and which [entitled it] to monitor and to transcribe the communications on Yahoo Messenger that the employee denied having had for personal purposes, after having been, together with his other colleagues, warned against using the company's resources for personal purposes, it cannot be held that the violation of his correspondence (*violarea secretului corespondenței*) was not the only manner to achieve this legitimate aim and that the proper balance between the need to protect his private life and the right of the employer to supervise the functioning of its business was not struck."

II. RELEVANT DOMESTIC LAW

13. The Romanian Constitution guarantees the right to the protection of intimate, private and family life (Article 26) as well as private correspondence (Article 28).

14. Article 195 of the Criminal Code provides that:

> "Anyone who unlawfully opens somebody else's correspondence or intercepts somebody else's conversations or communication by telephone, by telegraph or by any other long distance means of transmission shall be liable to imprisonment for between six months to three years."

15. The Labour Code in force at the time of events provided in Article 40(1)(d) that the employer had the right to monitor the manner in which the employees completed their professional tasks. Article 40(2)(i) provided that the employer had a duty to guarantee the confidentiality of the employees' personal data.

16. Law no. 677/2001 on the protection of individuals with regard to the processing of personal data and the free movement of personal data ("Law no. 677/2001") applies the provisions of EU Directive 95/46/EC (see paragraph 18 below). It defines "personal data" as "any data related to an identified or identifiable individual" (Article 3(a)). It provides that data can only be processed if the person concerned consented to it and it sets out a list of exceptions when consent is not necessary. Exceptions refer, among other situations, to the completion of a contract to which the concerned individual is a party and to securing a legitimate interest of the data operator (Article 5(2)(a and e)). It also provides that when processing data, public authorities remain under the obligation to protect the individuals' intimate, private and family life (Article 5(3)). Lastly, anyone who suffered prejudice as a result of illegal processing of his/her personal data can ask the courts to allow him/her reparation (Article 18(2)).

II. RELEVANT INTERNATIONAL LAW

A. Council of Europe instruments

17. The 1981 Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data ("the Data Protection Convention") defines "personal data" as "any information relating to an identified or identifiable individual". The Convention provides, *inter alia*, as follows:

Article 2 – Definitions

"For the purposes of this Convention:

(...)

(c) 'automatic processing' includes the following operations if carried out in whole or in part by automated means: storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination ..."

Article 3 – Scope

"(1) The Parties undertake to apply this Convention to automated personal data files and automatic processing of personal data in the public and private sectors."

(...)

Article 5 – Quality of data

"Personal data undergoing automatic processing shall be:

(a) obtained and processed fairly and lawfully;

(b) stored for specified and legitimate purposes and not used in a way incompatible with those purposes;

(c) adequate, relevant and not excessive in relation to the purposes for which they are stored;

(d) accurate and, where necessary, kept up to date;

(e) preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored."

(...)

Article 8 – Additional safeguards for the data subject

"Any person shall be enabled:

(a) to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;

(b) to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form (...)"

B. European Union instruments

18. Directive 95/46/EC of the European Parliament and of the Council of the European Union 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 provides that the object of national laws in this area is notably to protect the right to privacy as recognised both in Article 8 of the Convention and the general principles of EU law. The Directive defines personal data as "any information relating to an identified or identifiable natural person" (Article 2(a)) and asks for the Member States to prohibit processing of personal data concerning, among other things, "health or sex life" (Article 8(1)).

19. A Data Protection Working Party ("the Working Party") was established under Article 29 of the Directive 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. It is an independent EU advisory body. The Working Party issued in September 2001 opinion 8/2001 on the processing of personal data in an employment context, which summarises the fundamental data protection principles: finality, transparency, legitimacy, proportionality, accuracy, security and staff awareness. With regard to monitoring of employees, it suggested that it should be:

> "A proportionate response by an employer to the risks it faces taking into account the legitimate privacy and other interests of workers".

20. In May 2002 the Working Party produced the "Working document on the surveillance and the monitoring of electronic communications in the workplace" ("the working document"). This working document asserts that the simple fact that monitoring or surveillance conveniently serves an employer's interest could not justify an intrusion into workers' privacy. The document suggests that any monitoring measure must pass a list of four tests: transparency, necessity, fairness and proportionality.

21. From a technical point of view, the working document indicates that:

> "Prompt information can be easily delivered by software such as warning windows, which pop up and alert the worker that the system has detected and/or has taken steps to prevent an unauthorised use of the network."

22. More specifically, with regard to the question of access to an employee's e-mails, the working document holds that:

> "Opening an employee's e-mail may also be necessary for reasons other than monitoring or surveillance, for example in order to maintain correspondence in case the employee is out of office (for example due to sickness or leave) and correspondence cannot be guaranteed otherwise (for example via an autoreply or automatic forwarding)."

THE LAW

I. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

23. The applicant complained that his employer's decision to terminate his contract had been based on a breach of his right to respect for his private life and correspondence and that the domestic courts had failed to protect his right; he relied on Article 8 of the Convention, which reads as follows:

> "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."

A. Admissibility

1. The parties' submissions

24. The Government submitted that Article 8 of the Convention was not applicable in the present case. They noted that the applicant had set up the Yahoo Messenger account for professional use and he furthermore claimed that he had only used it for this purpose; the Government inferred that the applicant could not claim an "expectation of privacy" while at the same time denying any private use.

25. They further submitted that a number of Council of Europe member States required an assertion of the private nature of the communication for which the protection of privacy was sought; they relied, among other things, on the case-law of the French Court of Cassation that held that e-mails sent by an employee with means put at his disposal by his employer should be deemed to have a professional character and be accessible to the employer unless expressly identified as private.

26. Taking into consideration the differences between e-mail and instant messaging (the latter lacks a subject field), the Government argued that an assertion of the private character of the communication was essential for it to fall within the scope of Article 8. Thus, they pointed out that the applicant had been given an opportunity to claim that the use he had made of Yahoo Messenger had been, at least in part, private, and he had clearly stated that this had not been the case as he had declared that he had only communicated with clients on behalf of his employer.

27. The Government inferred that the applicant had been given proper prior notice that his employer could monitor his communications; they relied on the employer's notice of 3 July 2007 and on the findings of the County Court that the applicant had not challenged in his appeal. They did not submit a copy of the notice.

28. Finally, the Government pointed out that the present case was different from the cases of *Halford v. the United Kingdom* (25 June 1997, *Reports of Judgments and Decisions* 1997-III, where one of the landlines of the office had been designated for the applicant's personal use), and *Copland v. the United Kingdom* (no. 62617/00, ECHR 2007-I, where personal use was allowed and the surveillance aimed to determine whether the applicant had made "excessive use" of the facilities); in the instant case, the employer's regulations explicitly prohibited all personal use of company facilities, including computers and Internet access.

29. The applicant contested the Government's submissions and claimed that his communications on Yahoo Messenger had had a private character and therefore fell within the scope of Article 8 of the Convention. Referring to the State's positive obligations according to Article 8, he argued that this provision was applicable on account of the Romanian State's failure to protect his private sphere from interference by his employer. He pointed out that he had consistently raised this argument before the domestic authorities.

30. In the applicant's opinion, it could not be disputed that the data intercepted by his employer represented both "personal data" and "sensitive personal data" within the meaning of Law no. 677/2001 and EU Directive 95/46/EC; the information related to identified persons (the applicant, his fiancée and his brother) and concerned sensitive issues (such as the applicant's health and sex life). The applicant did not explain why he had used Yahoo Messenger for personal purposes, but suggested that at the material time the prices for mobile phones had been very high and that the requests for his professional services, as an engineer charged with selling heating equipment, had been very low in July 2007.

31. The applicant also complained that his employer had also accessed his personal Yahoo Messenger account, which had a different ID from the one he had registered for professional purposes. Moreover, the transcript of his communications had been made available to his colleagues who had discussed it publicly.

32. Relying on the case of *Niemietz v. Germany* (16 December 1992, Series A no. 251-B), the applicant contended that denying the protection of Article 8 on the grounds that the measure complained of related only to professional activities could lead to inequality of treatment in that such protection would be available only to persons whose professional and non-professional activities were so intermingled that they could not be distinguished. With reference to the case of *Chappell v. the United Kingdom* (30 March 1989, Series A no. 152-A), he argued that the Court had not excluded the applicability of Article 8 of the Convention in the case of a search of the business premises.

33. The applicant insisted that the Yahoo Messenger software was by its nature designed for personal use and that the nature of the instant messaging service had entitled him to expect that his communications would be private. Had he not expected privacy, he would have refrained from disclosing intimate information. He had felt reassured by his employer instructing him to protect his Yahoo Messenger account by choosing his own password. He denied having been given proper prior notice of his employer's monitoring; he argued that the general prohibition in the employer's internal regulations could not have amounted to prior notice of monitoring. He believed that the notice of 3 July 2007 had been identified after the facts**;** he submitted a copy of this notice which however does not bear the employees' signatures.

34. The applicant found the Government's submissions that he had initially asserted that he had used that account for professional purposes artificial; irrespective of his initial position, the fact that the actual use of the instant messaging service had been for personal purposes remains undisputed. He concluded that an employee's right to establish and develop personal relationships during business hours could not be suppressed at the discretion or by a decision of their employer.

2. The Court's assessment

35. The Court has consistently held that the notion of private life is a broad concept (see, *E.B. v. France* [GC], no. 43546/02, § 43, 22 January 2008, and *Bohlen v. Germany*, no. 53495/09, § 45, 19 February 2015). It encompasses, for example, the right to establish and develop relationships with other human beings, and the right to identity and personal development (*Niemietz*, cited above, § 29, and *Fernández Martínez v. Spain* [GC], no. 56030/07, § 126, ECHR 2014 (extracts)). A broad reading of Article 8 does not mean, however, that it protects every activity a person might seek to engage in with other human beings in order to establish and develop such relationships. It will not, for example, protect interpersonal relations of such broad and indeterminate scope that there can be no conceivable direct link between the action or inaction of a State and a person's private life (see, *mutatis mutandis*, *Botta v. Italy*, 24 February 1998, § 35, *Reports of Judgments and Decisions* 1998-I).

36. Thus, according to the Court's case-law, telephone calls from business premises are prima facie covered by the notions of "private life" and "correspondence" for the purposes of Article 8 § 1 (see *Halford*, cited above, § 44, and *Amann v. Switzerland* [GC], no. 27798/95, § 43, ECHR 2000-II). The Court further held that e-mails sent from work should be similarly protected under Article 8, as should information derived from the monitoring of personal Internet usage (see *Copland*, cited above, § 41).

37. In the absence of a warning that one's calls would be liable to monitoring, the applicant had a reasonable expectation as to the privacy of calls made from a work telephone (see *Halford*, cited above, § 45) and the same expectation should apply in relation to an applicant's e-mail and Internet usage (see *Copland*, cited above, § 41). In a case in which the applicant's workspace at a prosecutor's office had been searched and some of his belongings had been seized (*Peev v. Bulgaria*, no. 64209/01, 26 July 2007), the Court held that the search amounted to an interference with the applicant's "private life"; the Court found that the applicant had a reasonable expectation of privacy with regard to the personal belongings that he kept in his office (ibid., § 39). The Court further held that:

> "39. ... such an arrangement is implicit in habitual employer-employee relations and there is nothing in the particular circumstances of the case – such as a regulation or stated policy of the applicant's employer discouraging employees from storing

personal papers and effects in their desks or filing cabinets – to suggest that the applicant's expectation was unwarranted or unreasonable".

38. 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. In this connection, it notes that it is not disputed that the applicant's employer's internal regulations strictly prohibited employees from using the company's computers and resources for personal purposes (see paragraph 8 above).

39. It follows that the case is different, as suggested by the Government, from the *Halford* and *Copland* cases (cited above), in which the personal use of an office telephone was allowed or, at least, tolerated. The case must also be distinguished from the *Peev* case (cited above), in which the employer's regulations did not forbid employees to keep personal belongings in their professional office.

40. The Court notes that the applicant chose to raise before the domestic courts his complaint under Article 8 of the Convention within the framework of labour law proceedings. The main object of his case before the domestic courts was indeed his dismissal and the fact that his dismissal had resulted from a breach of his right to respect of his private life was the argument he used in order to prove the nullity of his employer's decision.

41. It follows that the object of his complaint before the Court is limited to the monitoring of his communications within the framework of disciplinary proceedings; the employer's decision to terminate the applicant's contract was not based on either the actual content of his communications nor on the fact of their eventual disclosure. In this regard, the Court notes that the applicant did not argue that he had had no other fora in which to bring these arguments separately before the domestic courts. The domestic law in force at the time of events provided for other remedies designed principally to protect private life (such as a criminal complaint based on Article 195 of the Criminal Code or a complaint based on Article 18(2) of Law no. 677/2001; see paragraphs 14 and 16 above), and the applicant did not claim that they were ineffective.

42. The Court must therefore determine whether, in view of the general prohibition imposed by his employer, the applicant retained a reasonable expectation that his communications would not be monitored. In this regard, the Court takes notice that the Data Protection Convention sets up clear principles applying to automatic data processing in order to enable an individual to establish the existence of an automated personal data file and its main purposes (see Articles 5 and 8 of the Data Protection Convention in paragraph 17 above). The relevant EU law goes in the same direction, notably in the field of surveillance of electronic communications in the workplace (see paragraphs 18, 19 and 20 above).

43. In the instant case, the Court notes that the elements in the file do not easily allow a straightforward answer. Indeed, the parties dispute whether the applicant had been given prior notice that his communications could have been monitored and their content accessed and eventually disclosed. The Government claimed that the applicant had been given proper prior notice that his employer could have monitored his communications (see paragraph 27 above), but the applicant denied having received such specific prior notice (see paragraph 33 above). The Court notes that the Government did not provide a signed copy of the employer's notice of 3 July 2007 (see paragraph 27 above) and that the copy provided by the applicant does not bear any signatures (see paragraph 33 above).

44. The Court attaches importance to the fact that the employer accessed the applicant's Yahoo messenger account and that the transcript of his communications was further used as a piece of evidence in the domestic labour court proceedings. It also notes that, according to applicant's submissions, that the Government did not explicitly dispute, the content of his communications with his fiancée and his brother was purely private, and related to, among other things, very intimate subjects such as the applicant's health or sex life (see paragraphs 7 and 30 above). It is also mindful of the applicant's argument that his employer had also accessed his personal Yahoo Messenger account (see paragraphs 7 and 31 above).

45. Having regard to these circumstances, and especially to the fact that the content of the applicant's communications on Yahoo messenger was accessed and that the transcript of these communications was further used in the proceedings before the labour courts, the Court is satisfied that the applicant's "private life" and "correspondence" within the meaning of Article 8 § 1 were concerned by these measures (*mutatis mutandis*, *Köpke v. Germany*, (dec.), no. 420/07, 5 October 2010). It therefore finds that Article 8 § 1 is applicable in the present case.

46. The Court further notes that this complaint is not manifestly ill-founded within the meaning of Article 35 § 3 (a) of the Convention and that it is not inadmissible on any other grounds. It must therefore be declared admissible.

B. Merits

1. The parties' submissions

47. The applicant took the view that there had been an interference with his private life and correspondence within the meaning of Article 8 of the Convention, and that this interference had not been justified under the second paragraph of Article 8. He submitted that this interference had not been in accordance with the law, as the applicable legislation, namely the Labour Code, lacked sufficient foreseeability; in this connection, he claimed

that the Court's findings in the case of *Oleksandr Volkov v. Ukraine* (no. 21722/11, ECHR 2013) were applicable to the present case. He pointed out that neither the Labour Code nor Law no. 677/2001 provided procedural safeguards as regards the surveillance of an employee's electronic communications.

48. He further argued that the interference had not been proportionate to the legitimate aim pursued. He refuted the findings of the domestic courts that his employer had had no other choice than to intercept his communications, and complained that no alternative means had been sought so that less damage to his fundamental rights would have been caused whilst fulfilling the same aim. He also mentioned that he had had a tense relationship with his employer and referred to another set of labour law proceedings in which the domestic courts had found in his favour.

49. The Government argued that the State authorities had met their positive obligations required by Article 8 of the Convention. They submitted that a wide variety of approaches existed among Council of Europe member States with regard to the regulation of monitoring of employees by an employer, and that there was no European consensus on the personal use of the Internet in the workplace.

50. They contended that in the instant case the authorities had allowed the applicant sufficient protection because of effective domestic court scrutiny of his case. Relying on the findings of the domestic courts, they noted that the applicant's denial of any personal use of his computer had made it necessary for the employer to ascertain the content of the communications. He had thus been presented with the transcripts of his communications for a limited period, that is to say those messages between 5 and 13 July 2007, which demonstrated that he had been blatantly wasting time. The Government further argued that the courts would have proceeded to a different balancing act if the applicant had asserted from the beginning that he had used Yahoo Messenger for personal purposes.

51. The Government also submitted that the ban on personal use of the company's resources was explicitly contained in the company regulations, and that both its enforcement and consequences had been known to the employees. They concluded that the domestic courts had struck a fair balance between the applicant's rights and his employer's legitimate interests.

2. The Court's assessment

52. The Court reiterates that although the purpose of Article 8 is essentially to protect an individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private life. These obligations may involve the adoption of measures designed to secure respect

for private life even in the sphere of the relations of individuals between themselves (see *Von Hannover v. Germany (no. 2)* [GC], nos. 40660/08 and 60641/08, § 57, ECHR 2012, and *Benediksdóttir v. Iceland* (dec.), no. 38079/06, 16 June 2009). The boundary between the State's positive and negative obligations under Article 8 does not lend itself to precise definition. In both contexts regard must be had to the fair balance that has to be struck between the competing interests – which may include competing private and public interests or Convention rights (see *Evans v. the United Kingdom* [GC], no. 6339/05, §§ 75 and 77, ECHR 2007-I) – and in both contexts the State enjoys a certain margin of appreciation (see *Von Hannover*, cited above; and *Jeunesse v. the Netherlands* [GC], no. 12738/10, § 106, 3 October 2014).

53. In the instant case, the Court finds that the applicant's complaint must be examined from the standpoint of the State's positive obligations since he was employed by a private company, which could not by its actions engage State responsibility under the Convention. The Court's findings in the case of *Oleksandr Volkov* (cited above), which concerned the dismissal of a judge, are therefore not applicable in the present case, as suggested by the applicant (see paragraph 47 above).

54. Therefore, the Court has to examine whether the State, in the context of its positive obligations under Article 8, struck a fair balance between the applicant's right to respect for his private life and correspondence and his employer's interests.

55. In this regard, the Court refers to its findings as to the scope of the complaint which is limited to the monitoring of the applicant's communications within the framework of disciplinary proceedings (see paragraphs 40 and 41 above).

56. The Court notes that the applicant was able to raise his arguments related to the alleged breach of his private life and correspondence by his employer before the domestic courts. It further notes that they duly examined his arguments and found that the employer had acted in the context of the disciplinary powers provided for by the Labour Code (see paragraphs 10 and 15 above). The domestic courts also found that the applicant had used Yahoo Messenger on the company's computer and that he had done so during working hours; his disciplinary breach was thus established (see paragraph 12 above).

57. In this context, the Court notes that 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 (see paragraphs 10 and 12 above). 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. The Court sees no reason to question these findings.

58. 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.

59. While it is true that it had not been claimed that the applicant had caused actual damage to his employer (compare and contrast *Pay v. United Kingdom*, (dec.), no. 32792/05, 16 September 2008 where the applicant was involved outside work in activities that were not compatible with his professional duties, and *Köpke* (cited above), where the applicant had caused material losses to her 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.

60. 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 (compare and contrast *Wieser and Bicos Beteiligungen GmbH v. Austria*, no. 74336/01, §§ 59 and 63, ECHR 2007-IV, and *Yuditskaya and Others v. Russia*, no. 5678/06, § 30, 12 February 2015).

61. Furthermore, the Court finds that the applicant has not convincingly explained why he had used the Yahoo messenger account for personal purposes (see paragraph 30 above).

62. 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.

63. There has accordingly been no violation of Article 8 of the Convention.

II. ALLEGED VIOLATION OF ARTICLE 6 OF THE CONVENTION

64. Relying on Article 6 of the Convention, the applicant also complained that the proceedings before the domestic courts had been unfair,

in particular as he had not been allowed to present witnesses as part of his case.

65. The Court notes that the applicant was able to raise these arguments before the Court of Appeal, which ruled, in a sufficiently reasoned decision, that hearing additional witnesses was not relevant to the case (see paragraph 12 above). Such a decision was delivered in a public hearing conducted in an adversarial manner and does not seem arbitrary (see *García Ruiz v. Spain* [GC], no. 30544/96, §§ 28-29, ECHR 1999-I).

66. It follows that this complaint is manifestly ill-founded and must be rejected in accordance with Article 35 §§ 3 (a) and 4 of the Convention.

FOR THESE REASONS, THE COURT

1. *Declares*, unanimously, the complaint concerning Article 8 of the Convention admissible and the remainder of the application inadmissible;

2. *Holds*, by six votes to one, that there has been no violation of Article 8 of the Convention;

Done in English, and notified in writing on 12 January 2016, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

Fatoş Aracı	András Sajó
Deputy Registrar	President

In accordance with Article 45 § 2 of the Convention and Rule 74 § 2 of the Rules of Court, the separate opinion of Judge Pinto de Albuquerque is annexed to this judgment.

A.S.
F.A.

PARTLY DISSENTING OPINION OF JUDGE PINTO DE ALBUQUERQUE

1. *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. I have no reservations in joining the majority in finding the Article 6 complaint inadmissible.

2. 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.

Access to the Internet as a human right

3. As the Court's Grand Chamber recently stated, user-generated expressive activity on the Internet provides an unprecedented platform for the exercise of freedom of expression[2]. In the light of its accessibility and capacity to store and communicate vast amounts of information, the Internet also plays an important role in enhancing the public's access to news and facilitating the dissemination of information in general[3]. Along the same line of reasoning, the French Constitutional Council has affirmed that "in the current state of means of communication and given the generalised development of public online communication services and the importance of the latter for the participation in democracy and the expression of ideas and opinions, this right (to freedom of expression) implies freedom to

[1] This case-law is still limited (see *Copland v. the United Kingdom*, no. 62617/00, ECHR 2007-I, and *Peev v. Bulgaria*, no. 64209/01, 26 July 2007).
[2] *Delfi AS v. Estonia* [GC], no. 64569/09, §§ 110 and 118, 16 June 2015, following *Ahmet Yıldırım v. Turkey*, no. 3111/10, § 48, ECHR 2012, and *Times Newspapers Ltd (nos. 1 and 2) v. the United Kingdom*, nos. 3002/03 and 23676/03, § 27, ECHR 2009.
[3] *Ahmet Yıldırım*, cited above, § 48, and *Times Newspapers Ltd*, cited above, § 27.

access such services."[4] Thus, States have a positive obligation to promote and facilitate universal Internet access, including the creation of the infrastructure necessary for Internet connectivity[5]. In the case of private communications on the Internet, the obligation to promote freedom of expression is coupled with the obligation to protect the right to respect for private life. States cannot ensure that individuals are able to freely seek and receive information or express themselves without also respecting, protecting and promoting their right to privacy. At the same time, the risk of harm posed by Internet communications to the exercise and enjoyment of human rights and freedoms, particularly the right to respect for private life, is certainly higher than that posed by the press[6]. For example, States should counter racial or religious discrimination or hate speech over the Internet[7]. In other words, situations may emerge where the freedom of expression of the content provider, protected by Article 10, may collide with the right to respect for private life of others enshrined in Article 8, or where both the freedom of expression and the right to respect for private life of those involved in Internet communications may conflict with the rights and freedoms of others. The present case pertains to this second type of situation.

---

[4] Constitutional Council decision no. 2009/580DC, 10 June 2009, paragraph 12.

[5] See, at the regional level, Recommendation CM/Rec(2007)16 of the Committee of Ministers to member States on measures to promote the public service value of the Internet, 7 November 2007, and, most importantly, Recommendation CM/Rec(2011)8 of the Committee of Ministers to member States on the protection and promotion of the universality, integrity and openness of the Internet, 21 September 2011, and the other Council of Europe Resolutions, Recommendations and Declarations, in addition to the Convention on Cybercrime and its Additional Protocol mentioned in my separate opinion joined to *Ahmet Yildirim*, cited above; and at the global level, the UN Millennium Declaration approved by GA Resolution 55/2, 18 September 2000, A/RES/55/2; International Telecommunications Union, Geneva Declaration of Principles, World Summit on the Information Society, 10 December 2003 ("commitment to build a people-centred, inclusive and development-oriented Information society, where everyone can create, access, utilise and share information and knowledge"); the Joint Declaration on Freedom of expression and the Internet by the UN Special rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the media, the OAS Special rapporteur on Freedom of Expression and the ACHPR Special Rapporteur on Expression and Access to Information, 1 June 2011, paragraph 6; and, in the UN committees' work, for example, the Human Rights Committee General Comment no. 34, Freedoms of expression and opinion (art. 19), 12 September 2011, CCPR/C/GC/34, paragraph 12; and the International Committee on Economic, Social and Cultural Rights, Concluding Observations on China, 25 April-13 May 2005, E/2006/22, paragraphs 168 and 197.

[6] *Delfi AS*, cited above, § 133, and *Editorial Board of Pravoye Delo and Shtekel v. Ukraine*, no. 33014/05, §§ 63-64, ECHR 2011.

[7] *Delfi AS*, cited above, §§ 136 and 162; Committee on the Elimination of Racial Discrimination General Recommendation XXX, Discrimination against Non-citizens, 20 August 2004, A/59/18, paragraph 12, page 95; and Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 7 September 2012 (A/67/357), paragraph 87.

Protection of employees' Internet communications in international law

4. 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[8]. 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 provided by the employer.

5. 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[9]. 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[10]. In the absence of a

[8] Thus, I find it hard to agree with the majority's very broad statement in paragraph 58 of the judgment.

[9] In *Niemietz v. Germany*, 16 December 1992, Series A no. 251-B, § 28, *Halford v. the United Kingdom*, 25 June 1997, Reports 1997-III, § 44, and *Amann v. Switzerland* [GC], no. 27798/95, § 43, ECHR 2000-II, the Court considered interferences with communications and correspondence in a work or business environment in the light of the concept of private life and correspondence for the purposes of Article 8, no distinction being made between private or professional communication and correspondence. The Court has already stated that privacy rights may not be asserted in the context of conduct away from the workplace, relied upon by an employer as grounds for dismissal (*Pay v. the United Kingdom (dec.)*, no. 32792/05, 16 September 2008).

[10] Inspired by *Malone v. the United Kingdom*, 2 August 1984, § 84, Series A no. 82, the Court affirmed in *Copland*, cited above, § 43, that, even if the monitoring is limited to "information relating to the date and length of telephone conversations and in particular the numbers dialled", as well as to e-mail and Internet usage, and without access to the content of the communications, it still violates Article 8 of the Convention. The same point was

warning from the employer that communications are being monitored, the employee has a "reasonable expectation of privacy"[11]. 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[12], namely the protection of the rights and freedoms of the employer or other employees (Article 8 § 2)[13] 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)[14].

---

made by the Court of Justice of the European Union, Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* and *Seitlinger and Others*, Judgment of 8 April 2014, paragraphs 26-27, and 37, and the Report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, 30 June 2014, paragraph 19 (A/HRC/27/37).

[11] *Halford*, cited above, §§ 44 and 45; *Copland*, cited above, §§ 41 and 42; and *Peev*, cited above, § 39. It is not clear what the Court meant by this, since the Court refers to various factors such as lack of warning, provision of private space and assurance of private use of the employer's communication devices, but does not clarify their relative importance and whether these factors are essential or case-sensitive. Thus, the Court neglects the normative value of the "reasonability" criterion, leaving the impression that the employee's privacy at work is always deferential to pure management interests, as if the employer had the ultimate word on what kind of activity is not regarded as private in the workplace. Worse still, the Court does not provide any guidance on the interests that the employer may invoke under Article 8 § 2 to justify interferences with the employee's privacy. The problem with this concept lies in the way it was fashioned at birth. The employee's expectation of privacy in the context of the "operational realities of the workplace" was affirmed by the United States Supreme Court in *O'Connor v. Ortega*, 480 US 709 (1983), which addressed the issue on a weak case-by-case basis, leading to the absence of generally applicable principles, as the critical concurring opinion of Justice Scalia also noted. In my view, the "reasonable expectation" test is a mixed objective-subjective test, since the person must actually have held the belief (subjectively), but it must have also been reasonable for him or her to have done so (objectively). This objective, normative limb of the test cannot be forgotten.

[12] *Amann*, cited above, § 65, and *Copland*, cited above, § 43. In a broader context, see also my separate opinion joined to *Yildirim v. Turkey*, no. 3111/10, 18 December 2012.

[13] The pursuance of the interests of national security, public safety or the economic well-being of the country, prevention of disorder or crime, the protection of health or morals is not in the purview of the employer, and therefore do not justify the interference with the Convention right. Hence, for example, it would be inappropriate for a private employer to perform surveillance tasks with regard to his or her employees on the basis of public security concerns. Here, I assume that different rules must apply in any case to State surveillance operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law. A similar assumption is made in paragraph 1.5 of Council of Europe Recommendation No. R (89)2 and Article 3 (2) of EU Directive 95/46/EC.

[14] The pursuit of the interests of national security, territorial integrity or public safety, prevention of disorder or crime, protection of health or morals, and maintenance of the authority and impartiality of the judiciary are not in the purview of the employer and therefore do not justify interference with the Convention right.

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[15].

6. 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[16]. 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.

7. 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

[15] For example, in an Article 10 case, *Palomo Sánchez and Others v. Spain*, nos. 28955/06, 28957/06, 28959/06 and 28964/06, 12 September 2011.
[16] ETS no. 108.

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[17], the Working Document on the surveillance and the monitoring of electronic communications in the workplace, adopted on 29 May 2002[18], the Working Document on a common interpretation of Article 26(1) of Directive 95/46/EC, adopted on 25 November 2005[19], and Article 29 Working Party Opinion 2/2006 on privacy issues related to the provision of email screening services, adopted on 21 February 2006[20], 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"[21].

8. Finally, both the 1980 Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and

[17] 5062/01/EN/Final.
[18] 5401/01/EN/Final.
[19] 2093/05/EN.
[20] 00451/06/EN.
[21] Important decisions have been delivered in this area by the Luxembourg Court of Justice, such as *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*, Joined cases C-468/10 and C-469/10, 24 November 2011, on the implementation of Article 7 (f) of the Data Protection Directive in national law; *Deutsche Telekom AG v. Bundesrepublik Deutschland*, C-543/09, 5 May 2011, on the necessity of renewed consent; *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer*, C-553/07, 7 May 2009, on the right of access of the data subject; *Dimitrios Pachtitis v. European Commission*, F-35/08, 15 June 2010, and *V v. European Parliament*, F-46/09, 5 July 2011, both on the usage of personal data in the context of employment in EU institutions.

Transborder Flows of Personal Data[22], 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.

9. 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[23]. 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[24]. 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[25]. Particular forms of personal data processing, for example of the employees' usage of Internet and electronic communications in the workplace, warrant detailed regulation[26].

10. 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

---

[22] These Guidelines were updated in 2013, but I will refer to both versions, taking into account the date of the facts in the present case.

[23] While the template is to some extent parochial, the lens offered by the Court should be universal, in the sense that the Court should seek a principled approach to Internet communications. This top-down international regulation, imposed by the Court in certain fundamental aspects, does not call into question the free, multi-stakeholder governance of the Internet. On the contrary, it guarantees it. In my view, the Court should not forget the highly political nature of the Internet as a social equaliser and an instrument for furthering human rights, which engages private interests in public decisions. Such an omission would prove particularly regrettable in the context of employment law, whose primarily purpose is to redress the imbalance between vulnerable employees and more powerful employers in their contractual relationships.

[24] Paragraph 14.1 of Council of Europe Recommendation Rec (2015)5: "The content, sending and receiving of private electronic communications at work should not be monitored under any circumstances", and paragraph 15.1: "The introduction and use of information systems and technologies for the direct and principal purpose of monitoring employee's activity and behaviour should not be permitted.".

[25] However, the mere existence of a labour code or a general employment law which regulates the relationship between employers and employees does not suffice if they do not provide for a specific set of rules on employees' personal data protection, including Internet usage policy in the workplace.

[26] In its updated General Comment on Article 19, the Human Rights Committee pointed out the need to take greater account of free speech on the Internet and digital media (CCPR/C/GC/34, 12 September 2011, paragraph 12).

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[27].

11. A blanket ban on personal use of the Internet by employees is inadmissible[28], as is any policy of blanket, automatic, continuous monitoring of Internet usage by employees[29]. 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[30].

12. 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[31]. All employees should be notified personally of the said policy and consent to it explicitly[32]. Before a

---

[27] Paragraph 6.14.1 of the 1997 ILO Code of Practice and paragraph 15 of the revised 2013 OECD Guidelines, which introduces a concept of a privacy management programme and articulates its essential elements.

[28] Article 29 Working Party Working document on the surveillance of electronic communications in the workplace, pages 4 and 24. As the Handbook on European data protection law, 2014, puts it, "Such a general prohibition could, however, be disproportionate and unrealistic."

[29] Article 29 Working Party Working document on the surveillance of electronic communications in the workplace, page 17, and, previously, the Office of the Australian Federal Privacy Commissioner, Guidelines on Workplace E-mail, Web Browsing and Privacy, 30 March 2000.

[30] See Article 6 of the 1981 Council of Europe Convention, paragraph 10.1 of Council of Europe Recommendation No. R (89)2, paragraph 6.5 of the 1997 ILO Code of practice, and paragraph 9.1 of Council of Europe Recommendation Rec (2015)5.

[31] Rules on the transparency of any processing of an employee's personal data can be found in paragraph 12 of the 1980 OECD Guidelines; paragraph 3.1 of Council of Europe Recommendation No. R (89)2; paragraph 5.8 of the 1997 ILO Code of practice; Article 29 Working Party Working document on the surveillance of electronic communications in the workplace, pages 4 and 5; Article 29 Working Party Working document on the surveillance of electronic communications in the workplace, pages 13, 14, 22 and 25; and paragraphs 10.1-10.4 and especially paragraph 14.1 and 21 (a) of Council of Europe Recommendation Rec (2015)5.

[32] The principle of informed and explicit consent has been affirmed in paragraph 7 of the 1980 OECD Guidelines, paragraph 3.2 of Council of Europe Recommendation No. R (89)2, paragraphs 6.1-6.4 of the 1997 ILO Code of Practice, Article 29 Working Party Opinion no. 8/2001, pages 3 and 23, Article 29 Working Party Working document on the surveillance of electronic communications in the workplace, page 21, and paragraphs 14.3, 20.2 and 21 (b) and (c) of Council of Europe Recommendation Rec (2015)5. According to the Council of Europe Employment Recommendation, employers should inform their employees in advance about the introduction or adaptation of automated systems for the processing of personal data of employees or for monitoring the movements or the productivity of employees. In the EU framework, the Data Protection Working Party analysed the significance of consent as a legal basis for processing employment data and found that the economic imbalance between the employer asking for consent and the employee giving consent will often raise doubts about whether consent was given freely or

monitoring policy is put in place, employees must be aware of the purposes, scope, technical means and time schedule of such monitoring[33]. 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[34]. 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.

13. 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[35]. 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[36]. 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

---

not. Hence, the circumstances under which consent is requested should be carefully considered when assessing the validity of consent in the employment context.

[33] Commentary to paragraph 6.14 of the 1997 ILO Code of practice, and Article 29 Working Party Opinion no. 8/2001, page 25.

[34] Paragraph 13 of the 1980 OECD Guidelines, Article 8 of the 1981 Council of Europe Convention, paragraphs 11 and 12 of Council of Europe Recommendation No. R (89)2, paragraphs 11.1-11.3, and 11.9 of the 1997 ILO Code of Practice and paragraphs 11.1-11.9 of Council of Europe Recommendation Rec (2015)5.

[35] See my separate opinion in *Yildirim*, cited above, on the minimum criteria for Convention-compatible legislation on Internet blocking measures; and also paragraph 8 of the 1980 OECD Guidelines; Article 5 (c), (d) of the 1981 Council of Europe Convention; paragraph 4.2 of Council of Europe Recommendation No. R (89)2; paragraph 5.1-5.4 of the 1997 ILO Code of Practice; Article 29 Working Party Opinion no. 8/2001, page 25; Article 29 Working Party Working document on the surveillance of electronic communications in the workplace, pages 17 and 18; and paragraphs 4.1, 5.2 and 5.5 of Council of Europe Recommendation (2015)5.

[36] Article 29 Working Party Working document on the surveillance of electronic communications in the workplace, page 13, and paragraph 20.1 of Council of Europe Recommendation Rec (2015)5.

employees[37]. The least intrusive technical means of monitoring should be preferred[38]. Since blocking Internet communications is a measure of last resort[39], filtering mechanisms may be considered more appropriate, if at all necessary, to avoid policy infringements[40]. 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[41]. 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[42].

14. 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[43]. 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.

15. 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

---

[37] Paragraph 6.14.2 of the 1997 ILO Code of practice.

[38] Article 29 Working Party Opinion no. 8/2001, pages 4 and 25, and paragraph 14.3 of Council of Europe Recommendation Rec (2015)5.

[39] See my separate opinion in *Yildirim*, cited above, on the minimum criteria for Convention-compatible legislation on Internet blocking measures.

[40] Paragraph 14.2 of Council of Europe Recommendation Rec (2015)5. As the Article 29 Data Protection Working Party document on surveillance and monitoring of electronic communications in the workplace, page 24, put it, "the interest of the employer is better served in preventing Internet misuse rather than in detecting such misuse."

[41] Paragraph 13 of Council of Europe Recommendation No. R (89)2, and paragraph 12.1 of Council of Europe Recommendation Rec (2015)5.

[42] Paragraph 14 of Council of Europe Recommendation No. R (89)2, and paragraph 13.1 of Council of Europe Recommendation Rec (2015)5.

[43] At this juncture it is worth noting the Court's demanding threshold for accepting dismissal in *Vogt v. Germany*, no. 17851/91, 26 September 1995, where the penalty of dismissal was found excessive for the employee's participation in political activities outside work with no impact on her professional role, and *Fuentes Bobo v. Spain*, no. 39293/98, 29 February 2000, where the penalty of dismissal for offensive remarks broadcast about the employer was also found to be too severe, taking into account the employee's length of service.

doing, they will be acting in accordance with the principled international-law approach to Internet freedom as a human right[44].

The absence of a workplace policy on Internet use

16. The Government argue that the company's internal regulations provided for a prohibition on the use of computers for personal purposes. Although true, the argument is not relevant, since the given internal regulations omitted any reference to an Internet surveillance policy being implemented in the workplace. In this context, it should not be overlooked that the Government also refer to notice 2316 of 3 July 2007, which "highlighted that another employee had been let go on disciplinary grounds, specifically due to personal use of the company's Internet connection and phones" and "reiterated that the employer verifies and monitors the employees' activity, specifically stating that they should not use the Internet, phones or faxes for issues unrelated to work", in other words, which "reiterated" the existence of a policy of Internet surveillance in the company[45]. Also according to the Government, the employees had been informed about this notice, and it had even been signed by the applicant. The applicant disputes these facts. The majority themselves acknowledge that it is contested whether the company's Internet surveillance policy had been notified to the applicant prior to the interference with his Internet communications[46]. Unfortunately, the majority did not elaborate further on this crucial fact.

17. Since the existence of prior notice was alleged by the Government and disputed by the applicant, the Government had the burden of providing evidence to that effect, which they did not[47]. Moreover, the only copy of the notice 2316 available in the Court's file is not even signed by the employee[48]. In other words, there is not sufficient evidence in the file that the company's employees, and specifically the applicant, were aware that

---

[44] See also my separate opinion joined to *Yildirim*, cited above; ILO, Conditions of Work Digest, volume 12, Part I, Monitoring and Surveillance in the Workplace (1993), p. 77; the Joint Declaration by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, adopted on 21 December 2005; and Reports by the UN Human Rights Council's Special Rapporteur on the promotion and protection of the right to Freedom of Opinion and Expression, Frank La Rue (A/HRC/17/27), 16 May 2011, and (A/66/290), 10 August 2011, especially the latter text, on access to online content (section III) and access to Internet connection (section IV).

[45] Page 2 of the Government's observations.

[46] Paragraph 41 of the judgment.

[47] Paragraph 27 of the judgment.

[48] Paragraphs 33 and 43 of the judgment. I find it odd, to say the least, that the County Court referred to notice 2316 as having been signed (paragraph 10 of the judgment), but the Government was not in a position to present a copy of the contested item of evidence to the Court.

monitoring software had been installed by the employer and recorded in real time the employees' communications on the company's computers, produced statistical records of each employee's Internet use and transcripts of the content of the communications exchanged by them, and could block their communication[49].

18. Even assuming that notice 2316 did exist and was indeed notified to the employees, including the applicant, prior to the events in question, this would not suffice to justify the termination of his contract, given the extremely vague character of the notice. A mere communication by the employer to employees that "their activity was under surveillance"[50] is manifestly insufficient to provide the latter with adequate information about the nature, scope and effects of the Internet surveillance programme implemented[51]. Such a poorly-drafted "policy", if existent, offered precious little protection to employees. In spite of its crucial importance for the outcome of the case, the majority did not care to consider the terms of the notice on the company's alleged Internet surveillance policy. Taking into account the evidence before the Court, I cannot but consider that the notice did not identify the minimum elements of an Internet usage and surveillance policy, including the specific misconduct being monitored, the technical means of surveillance and the employee's rights regarding the monitored materials.

The personal and sensitive nature of the employee's communications

19. The delicate character of the present case is significantly heightened by the nature of certain of the applicant's messages. They referred to the sexual health problems affecting the applicant and his fiancée[52]. This subject pertains to the core of the applicant's private life and requires the most intense protection under Article 8. Other than this sensitive data, the messages also dealt with other personal information, such as his uneasiness with the hostile working environment. The employer accessed not only the

[49] The employer used IMFirewall Software - Wfilter to intercept the applicant's communications, which is characterised by real time recording and the possibility to block messages (see paragraph 13 of the applicant's observations, not disputed by the Government).

[50] Paragraph 10 of the judgment, referring to the County Court's description of the notice.

[51] This was exactly the same point made by the Article 29 Working Party Working document on the surveillance of electronic communications in the workplace: "Some interpreters point out that this seems to also imply as (although it was not specified in the judgement) that if a worker is warned in advance by an employer about the possibility of their communications being intercepted, then he may lose his expectation of privacy and interception will not constitute a violation of Article 8 of the Convention. The Working Party would not be of the opinion that advance warning to the worker is sufficient to justify any infringement of their data protection rights" (page 8).

[52] Paragraph 45 of the judgment.

professional Yahoo Messenger account created by the applicant, but also his own personal account[53]. The employer had no proprietary rights over the employee's Yahoo messenger account, notwithstanding the fact that the computer used by the employee belonged to the employer[54]. Furthermore, the employer was aware that some of the communications exchanged by the applicant were directed to an account entitled "Andra loves you", which could evidently have no relationship with the performance of the applicant's professional tasks[55]. Yet the employer accessed the content of this

[53] Paragraph 5.3 of Council of Europe Recommendation (2015)5 states clearly that "Employers should refrain from requiring or asking an employee or a job applicant access to information that he or she shares with others online, notably through social networking." As the English High Court stated in *Smith v. Trafford Housing Trust* (2013) IRLR 86, the employer's obligation not to promote religious beliefs does not extend to the employee's Facebook postings, and thus a Christian employee may express his views on gay marriage on social networks without committing professional misconduct. But employee termination may be related to his or her "after hours" commercial activities on eBay, which included videos objectionable to the employer, as decided by the US Supreme Court in *San Diego v. Roe*, 543 US 77 (2004).

[54] The ownership argument is not lacking in logical appeal, but it should be approached with caution. It can be questioned whether it is appropriate to approach the matter in black-or-white reasoning, arguing that the employee no longer has any expectation of privacy whenever he or she uses IT facilities belonging to the employer, and, conversely, the employer has such an expectation whenever he or she uses his or her own IT facilities. A more nuanced approach is necessary, as emerges from the Article 29 Working Party Working document on surveillance and monitoring of electronic communications in the workplace, page 20: "In any case, the location and ownership of the electronic means used do not rule out secrecy of communications and correspondence as laid down in fundamental legal principles and constitutions." Recently, the Canadian Supreme Court underscored the same idea, asserting the employee's reasonable expectation of privacy over his personal information stored in company-owned equipment (*R. v. Cole*, (2012) SCC 53). By the same token, the working time argument, which claims that an individual at work is not on "private time" and that therefore no right to privacy applies in the workplace, is also misleading. To borrow the words of Justice Blackmun writing for the minority in *O'Connor v. Ortega*, cited above, "the reality of work in modern time, whether done by public or private employees, reveals why a public employee's expectation of privacy in the workplace should be carefully safeguarded and not lightly set aside. It is, unfortunately, all too true that the workplace has become another home for most working Americans. Many employees spend the better part of their days and much of their evenings at work ... As a result, the tidy distinctions (to which the plurality alludes) between the workplace and professional affairs, on the one hand, and personal possessions and private activities, on the other, do not exist in reality."

[55] Thus, the explanation provided by the employer, which the majority accept in paragraph 57, that the employer accessed the applicant's account "in the belief that it contained professional messages", is not convincing. Moreover, the majority contradict themselves when they argue in paragraph 58 that "the Court takes the view that the content of the communications was not a decisive element in the domestic courts' findings". On the one hand, the majority consider that the interference with the employee's right to respect for private life was "legitimate", because, "as the domestic courts found", the employee acted on the "assumption that the information in question had been related to professional activities", but, on the other hand, the majority state that the private nature of the

communication and made transcripts of it against the applicant's explicit will and without a court order[56].

The lack of necessity of the employer's interference

20. In addition, the employer's interference had wide adverse social effects, since the transcripts of the messages were made available to the applicant's colleagues and even discussed by them[57]. 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[58].

21. Having said that, the termination of the applicant's employment relationship with the company could not be based on evidence that did not meet the Convention standards of protection of employees' privacy. In ratifying the employer's dismissal decision, the domestic courts accepted as legal evidence of the breach of the applicant's professional duties records of private communications which merited Convention protection and had nonetheless been accessed, used and publicised by the employer, in violation of the Convention standard[59]. Moreover, the termination of the applicant's employment contract can hardly be said to be proportionate in itself, bearing in mind that it was not proven that the applicant had caused

---

communication was not decisive for the domestic courts' confirmation of the dismissal. This makes no sense. In the domestic courts' view, it was precisely the private, non-professional nature of the communications that was the decisive element for their finding the employee's disciplinary breach as established.

[56] In fact, the employer also accessed communications between the applicant and his brother's Yahoo messenger account, entitled "meistermixyo", which included, for example, information on a car accident sustained by the latter (see paragraph 11 of the applicant's observations, not contested by the Government).

[57] Paragraph 4 of the applicant's observations, which was not disputed by the Government, and paragraph 31 of the judgment.

[58] This was explicitly in breach of the applicable rules on internal use of personal data set out in paragraph 10 of the 1980 OECD Guidelines, paragraph 6.1 of Council of Europe Recommendation No. R (89)2, paragraph 10.6 of the 1997 ILO Code of Practice, and paragraph 6.1 of Council of Europe Recommendation (2015)5.

[59] In other words, the interference with the employee's right to privacy, especially with regard to the sensitive data collected, was so intolerable that it tainted the evidence collected and hence the *Schenk* standard does not apply here (*Schenk v. Switzerland*, no. 10862/84, 12 July 1988). A similar approach was taken by the Portuguese Constitutional Court, in its judgment no. 241/2002, on the nullity of evidence collected in a dismissal case on the basis of the labour court's request to Telepac and Portugal Telecom for traffic data and billing information concerning the employee's home phone line.

actual damage to his employer, or that he had adopted the same pattern of behaviour for a considerable period of time[60].

Conclusion

22. "Workers do not abandon their right to privacy and data protection every morning at the doors of the workplace."[61] New technologies make prying into the employee's private life both easier for the employer and harder for the employee to detect, the risk being aggravated by the connatural inequality of the employment relationship. A human-rights centred approach to Internet usage in the workplace warrants a transparent internal regulatory framework, a consistent implementation policy and a proportionate enforcement strategy by employers. Such a regulatory framework, policy and strategy were totally absent in the present case. The interference with the applicant's right to privacy was the result of a dismissal decision taken on the basis of an *ad hoc* Internet surveillance measure by the applicant's employer, with drastic spill-over effects on the applicant's social life. The employee's disciplinary punishment was subsequently confirmed by the domestic courts, on the basis of the same evidence gathered by the above-mentioned contested surveillance measure. The clear impression arising from the file is that the local courts willingly condoned the employer's seizure upon the Internet abuse as an opportunistic justification for removal of an unwanted employee whom the company was unable to dismiss by lawful means.

23. Convention rights and freedoms have a horizontal effect, insofar as they are not only directly binding on public entities in the Contracting Parties to the Convention, but also indirectly binding on private persons or entities, the Contracting State being responsible for preventing and remedying Convention violations by private persons or entities. This is an obligation of result, not merely an obligation of means. The domestic courts did not meet this obligation in the present case when assessing the legality of the employer's dismissal decision, adopted in the disciplinary proceedings against the employee. Although they could have remedied the violation of the applicant's right to respect for private life, they opted to confirm that violation. This Court did not provide the necessary relief either. For that reason, I dissent.

---

[60] It should be recalled that if a worker is asked questions that are inconsistent with the prohibition of collection of data on the worker's sex life by the employee, and the worker gives an inaccurate or incomplete answer, the worker should not be subject to termination of the employment relationship or any other disciplinary measure (paragraph 6.8 of the 1997 ILO Code of Practice).

[61] Article 29 Working Party Working document on surveillance and monitoring of electronic communications in the workplace, page 4.