CASE OF BĂRBULESCU v. ROMANIA

ZBIRNI PODATKI
Številka zadeve: 61496/08
Ključne besede: (Art. 41) Pecuniary damage, (Art. 8-1) Respect for correspondence, (Art. 8) Right to respect for private and family life, (Art. 41) Non-pecuniary damage, (Art. 8-1) Respect for private life, Margin of appreciation, (Art. 41) Just satisfaction, (Art. 41) Just satisfaction-{general}
Ločeno mnenje: Yes
Datum odločitve: 5.09.2017
Vrsta odločitve: Judgment (Merits and Just Satisfaction)
Domače pravo_2: International Labour Office (ILO) issued a Code of Practice on the Protection of Workers' Personal Data ("the ILO Code of Practice") issued in 1997; 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;Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment, which was adopted on 1 April 2015
ECLI: ECLI:CE:ECHR:2017:0905JUD006149608
Pravna pomembnost zadeve: 1
PublishedIn: Reports of Judgments and Decisions 2017
Praksa ESČP: Pretty v. the United Kingdom, no. 2346/02, § 61, ECHR 2002-III, Özpınar v. Turkey, no. 20999/04, § 45 in fine, 19 October 2010, Klass and Others v. Germany, 6 September 1978, § 50, Series A no. 28, K.U. v. Finland, no. 2872/02, §§ 43 and 49, ECHR 2008, Roman Zakharov v. Russia [GC], no. 47143/06, § 173, ECHR 2015, Palomo Sánchez and Others v. Spain [GC], nos. 28955/06 and 3 others, ECHR 2011, Halford v. the United Kingdom, 25 June 1997, §§ 44-45, Reports of Judgments and Decisions 1997 III, Christine Goodwin v. the United Kingdom [GC], no. 28957/95, § 90, ECHR 2002-VI, X and Y v. the Netherlands, 26 March 1985, § 23, Series A no. 91, Demir and Baykara v. Turkey [GC], no. 34503/97, §§ 140 146, ECHR 2008, Von Hannover v. Germany (no. 2) [GC], nos. 40660/08 and 60641/08, §§ 95 and 98, ECHR 2012, Obst v. Germany, no. 425/03, §§ 40 and 43, 23 September 2010, Söderman v. Sweden [GC], no. 5786/08, § 85, ECHR 2013, Köpke v. Germany (dec.), no. 420/07, 5 October 2010, Amann v. Switzerland [GC], no. 27798/95, § 44, ECHR 2000 II, Fernández Martínez v. Spain [GC], no. 56030/07, § 110, ECHR 2014 (extracts), Smirnova v. Russia, nos. 46133/99 and 48183/99, § 95, ECHR 2003 IX (extracts), Niemietz v. Germany, 16 December 1992, § 29, Series A no. 251 B, K.A. and A.D. v. Belgium, nos. 42758/98 and 45558/99, § 83, 17 February 2005, Sidabras and Džiautas v. Lithuania, nos. 55480/00 and 59330/00, § 43, ECHR 2004 VIII, Giuliani and Gaggio v. Italy [GC], no. 23458/02, § 180, ECHR 2011 (extracts), Codarcea v. Romania, no. 31675/04, §§ 102-104, 2 June 2009, Gustafsson v. Sweden, 25 April 1996, § 45, Reports 1996 II, Saumier v. France, no. 74734/14, § 60, 12 January 2017, M.C. v. Bulgaria, no. 39272/98, § 150, ECHR 2003 XII, Hämäläinen v. Finland [GC], no. 37359/09, § 62, ECHR 2014, Axel Springer AG v. Germany [GC], no. 39954/08, § 95, 7 February 2012, Wretlund v. Sweden (dec.), no. 46210/99, 9 March 2004, K. and T. v. Finland [GC], no. 25702/94, §§ 140-141, ECHR 2001 VII, D.H. and Others v. the Czech Republic [GC], no. 57325/00, § 109, ECHR 2007 IV, Lupeni Greek Catholic Parish and Others v. Romania [GC], no. 76943/11, § 187, ECHR 2016 (extracts), Blokhin v. Russia [GC], no. 47152/06, § 91, ECHR 2016, Schüth v. Germany, no. 1620/03, §§ 54 and 57, ECHR 2010, Aydan v. Turkey, no. 16281/10, § 69, 12 March 2013, Bigaeva v. Greece, no. 26713/05, § 22, 28 May 2009, Mustafa Tunç and Fecire Tunç v. Turkey [GC], no. 24014/05, § 182, 14 April 2015, Oleksandr Volkov v. Ukraine, no. 21722/11, §§ 165-166, ECHR 2013
Oddelek: Court (Grand Chamber)
Povezava do dokumenta na portalu IUS-INFO

GRAND CHAMBER *(Application no. 61496/08)*

CASE OF BĂRBULESCU v. ROMANIA JUDGMENT

STRASBOURG

5 September 2017

This judgment is final but it may be subject to editorial revision.

In the case of Bărbulescu v. Romania,

The European Court of Human Rights, sitting as a Grand Chamber composed of:

Guido Raimondi, *President* , Angelika Nußberger, Mirjana Lazarova Trajkovska, *judges* , Luis López Guerra, ad hoc *judge* , Ledi Bianku, Işıl Karakaş, Nebojša Vučinić, André Potocki, Paul Lemmens, Dmitry Dedov, Jon Fridrik Kjølbro, Mārtiņš Mits, Armen Harutyunyan, Stéphanie Mourou-Vikström, Georges Ravarani, Marko Bošnjak, Tim Eicke, *judges* , and Søren Prebensen, *Deputy Grand Chamber Registrar* ,

Having deliberated in private on 30 November 2016 and on 8 June 2017,

Delivers the following judgment, which was adopted on the lastmentioned 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 E. Domokos-Hâncu 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 complained, 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 as enshrined in Article 8 of the Convention and that the domestic courts had failed to comply with their obligation to protect that right.

4. The application was allocated to the Fourth Section of the Court (Rule 52 § 1 of the Rules of Court). On 12 January 2016 a Chamber of that Section, composed of András Sajó, President, Vincent A. De Gaetano, Boštjan M. Zupančič, Nona Tsotsoria, Paulo Pinto de Albuquerque, Egidijus Kūris and Iulia Motoc, judges, and Fatoş Aracı, Deputy Section Registrar, unanimously declared the complaint concerning Article 8 of the Convention admissible and the remainder of the application inadmissible. It held, by six votes to one, that there had been no violation of Article 8 of the Convention. The dissenting opinion of Judge Pinto de Albuquerque was annexed to the Chamber judgment.

5. On 12 April 2016 the applicant requested the referral of the case to the Grand Chamber in accordance with Article 43 of the Convention and Rule 73. On 6 June 2016 a panel of the Grand Chamber accepted the request.

6. The composition of the Grand Chamber was determined in accordance with Article 26 §§ 4 and 5 of the Convention and Rule 24. Iulia Motoc, the judge elected in respect of Romania, withdrew from sitting in the case (Rule 28). Luis López Guerra was consequently appointed by the President to sit as an *ad hoc* judge (Article 26 § 4 of the Convention and Rule 29 § 1).

7. The applicant and the Government each filed further written observations (Rule 59 § 1).

8. In addition, third-party comments were received from the French Government and the European Trade Union Confederation, both having been given leave by the President to intervene in the written procedure (Article 36 § 2 of the Convention and Rule 44 § 3).

9. A hearing took place in public in the Human Rights Building, Strasbourg, on 30 November 2016 (Rule 59 § 3).

There appeared before the Court:

(a) *for the Government* Ms C. Brumar, *Agent* , Mr G.V. Gavrilă, member of the national legal service seconded to the Department of the Government Agent, *Counsel* , Ms L.A. Rusu, Minister Plenipotentiary, Permanent Representation of Romania to the Council of Europe, *Adviser* ;

(b) *for the applicant* Mr E. Domokos-Hâncu, Mr O. Juverdeanu, *Counsel* .

The Court heard addresses by Mr Domokos-Hâncu, Mr Juverdeanu, Ms Brumar and Mr Gavrilă, and also their replies to questions from judges.

THE FACTS

I. THE CIRCUMSTANCES OF THE CASE

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

11. From 1 August 2004 to 6 August 2007 he was employed in the Bucharest office of S., a Romanian private company (“the employer”), as a sales engineer. At his employer’s request, for the purpose of responding to customers’ enquiries, he created an instant messaging account using Yahoo Messenger, an online chat service offering real-time text transmission over the internet. He already had another personal Yahoo Messenger account.

12. The employer's internal regulations prohibited the use of company resources by employees in the following terms:

Article 50

"Any disturbance of order and discipline on company premises shall be strictly forbidden, in particular:

...

– ... personal use of computers, photocopiers, telephones or telex or fax machines."

13. The regulations did not contain any reference to the possibility for the employer to monitor employees' communications.

14. It appears from documents submitted by the Government that the applicant had been informed of the employer's internal regulations and had signed a copy of them on 20 December 2006 after acquainting himself with their contents.

15. On 3 July 2007 the Bucharest office received and circulated among all its employees an information notice that had been drawn up and sent by the Cluj head office on 26 June 2007. The employer asked employees to acquaint themselves with the notice and to sign a copy of it. The relevant parts of the notice read as follows:

"1. ... Time spent in the company must be quality time for everyone! Come to work to deal with company and professional matters, and not your own personal problems! Don't spend your time using the internet, the phone or the fax machine for matters unconnected to work or your duties. This is what [elementary education], common sense and the law dictate! The employer has a duty to supervise and monitor employees' work and to take punitive measures against anyone at fault!

Your misconduct will be carefully monitored and punished!

2. Because of repeated [disciplinary] offences *vis-à-vis* her superior, [as well as] her private use of the internet, the telephone and the photocopier, her negligence and her failure to perform her duties, Ms B.A. was dismissed on disciplinary grounds! Take a lesson from her bad example! Don't make the same mistakes!

3. Have a careful read of the collective labour agreement, the company's internal regulations, your job description and the employment contract you have signed! These are the basis of our collaboration! Between employer and employee! ..."

16. It also appears from the documents submitted by the Government, including the employer's attendance register, that the applicant acquainted himself with the notice and signed it between 3 and 13 July 2007.

17. In addition, it transpires that from 5 to 13 July 2007 the employer recorded the applicant's Yahoo Messenger communications in real time.

18. On 13 July 2007 at 4.30 p.m. the applicant was summoned by his employer to give an explanation. In the relevant notice he was informed that his Yahoo Messenger communications had been monitored and that there was evidence that he had used the internet for personal purposes, in breach of the internal regulations. Charts were attached indicating that his internet activity was greater than that of his colleagues. At that stage, he was not informed whether the monitoring of his communications had also concerned their content. The notice was worded as follows:

"Please explain why you are using company resources (internet connection, Messenger) for personal purposes during working hours, as shown by the attached charts."

19. On the same day, the applicant informed the employer in writing that he had used Yahoo Messenger for work-related purposes only.

20. At 5.20 p.m. the employer again summoned him to give an explanation in a notice worded as follows:

"Please explain why the entire correspondence you exchanged between 5 to 12 July 2007 using the S. Bucharest [internet] site ID had a private purpose, as shown by the attached forty-five pages."

21. The forty-five pages mentioned in the notice consisted of a transcript of the messages which the applicant had exchanged with his brother and his fiancée during the period when he had been monitored; the messages related to personal matters and some were of an intimate nature. The transcript also included five messages that the applicant had exchanged with his fiancée using his personal Yahoo Messenger account; these messages did not contain any intimate information.

22. Also on 13 July, the applicant informed the employer in writing that in his view it had committed a criminal offence, namely breaching the secrecy of correspondence.

23. On 1 August 2007 the employer terminated the applicant's contract of employment.

24. The applicant challenged his dismissal in an application to the Bucharest County Court ("the County Court"). He asked the court, firstly, to set aside the dismissal; secondly, to order his employer to pay him the amounts he was owed in respect of wages and any other entitlements and to reinstate him in his post; and thirdly, to order the employer to pay him 100,000 Romanian lei (approximately 30,000 euros) in damages for the harm resulting from the manner of his dismissal, and to reimburse his costs and expenses.

25. As to the merits, relying on *Copland v. the United*

Kingdom (no. 62617/00, §§ 43-44, ECHR 2007I), he argued that an employee's telephone and email communications from the workplace were covered by the notions of "private life" and "correspondence" and were therefore protected by Article 8 of the Convention. He also submitted that the decision to dismiss him was unlawful and that by monitoring his communications and accessing their contents his employer had infringed criminal law.

26. With regard specifically to the harm he claimed to have suffered, the applicant noted the manner of his dismissal and alleged that he had been subjected to harassment by his employer through the monitoring of his communications and the disclosure of their contents "to colleagues who were involved in one way or another in the dismissal procedure".

27. The applicant submitted evidence including a full copy of the transcript of his Yahoo Messenger communications and a copy of the information notice (see paragraph 15 above).

28. In a judgment of 7 December 2007 the County Court rejected the applicant's application and confirmed that his dismissal had been lawful. The relevant parts of the judgment read as follows:

"The procedure for conducting a disciplinary investigation is expressly regulated by the provisions of Article 267 of the Labour Code.

In the instant case it has been shown, through the written documents included in the file, that the employer conducted the disciplinary investigation in respect of the applicant by twice summoning him in writing to explain himself [and] specifying the subject, date, time and place of the interview, and that the applicant had the opportunity to submit arguments in his defence regarding his alleged acts, as is clear from the two explanatory notices included in the file (see copies on sheets 89 and 91).

The court takes the view that the monitoring of the internet conversations in which the employee took part using the Yahoo Messenger software on the company's computer during working hours – regardless of whether or not the employer's actions were illegal in terms of criminal law – cannot undermine the validity of the disciplinary proceedings in the instant case.

The fact that the provisions containing the requirement to interview the suspect (*învinuitul*) in a case of alleged misconduct and to examine the arguments submitted in that person's defence prior to the decision on a sanction are couched in imperative terms highlights the legislature's intention to make respect for the rights of the defence a prerequisite for the validity of the decision on the sanction.

In the present case, since the employee maintained during the disciplinary investigation that he had not used Yahoo Messenger for personal purposes but in order to advise customers on the products being sold by his employer, the court takes the view that an inspection of the content of the [applicant's] conversations was the only way in which the employer could ascertain the validity of his arguments.

The employer's right to monitor (*monitoriza*) employees in the workplace, [particularly] as regards their use of company computers, forms part of the broader right, governed by the provisions of Article 40 (d) of the Labour Code, to supervise how employees perform their professional tasks.

Given that it has been shown that the employees' attention had been drawn to the fact that, shortly before the applicant's disciplinary sanction, another employee had been dismissed for using the internet, the telephone and the photocopier for personal purposes, and that the employees had been warned that their activities were being monitored (see notice no. 2316 of 3 July 2007, which the applicant had signed [after] acquainting himself with it – see copy on sheet 64), the employer cannot be accused of showing a lack of transparency and of failing to give its employees a clear warning that it was monitoring their computer use.

Internet access in the workplace is above all a tool made available to employees by the employer for professional use, and the employer indisputably has the power, by virtue of its right to supervise its employees' activities, to monitor personal internet use.

Such checks by the employer are made necessary by, for example, the risk that through their internet use, employees might damage the company's IT systems, carry out illegal activities in cyberspace for which the company could incur liability, or disclose the company's trade secrets.

The court considers that the acts committed by the applicant constitute a disciplinary offence within the meaning of Article 263 § 2 of the Labour Code since they amount to a culpable breach of the provisions of Article 50 of S.'s internal regulations ..., which prohibit the use of computers for personal purposes.

The aforementioned acts are deemed by the internal regulations to constitute serious misconduct, the penalty for which, in accordance with Article 73 of the same internal regulations, [is] termination of the contract of employment on disciplinary grounds.

Having regard to the factual and legal arguments set out above, the court considers that the decision complained of is well-founded and lawful, and dismisses the application as unfounded."

29. The applicant appealed to the Bucharest Court of Appeal ("the Court of Appeal"). He repeated the arguments he had submitted before the first-instance court and contended in addition that that court had not struck a fair

balance between the interests at stake, unjustly prioritising the employer's interest in enjoying discretion to control its employees' time and resources. He further argued that neither the internal regulations nor the information notice had contained any indication that the employer could monitor employees' communications.

30. The Court of Appeal dismissed the applicant's appeal in a judgment of 17 June 2008, the relevant parts of which read:

"The first-instance court has rightly concluded that the internet is a tool made available to employees by the employer for professional use, and that the employer is entitled to set rules for the use of this tool, by laying down prohibitions and provisions which employees must observe when using the internet in the workplace; it is clear that personal use may be refused, and the employees in the present case were duly informed of this in a notice issued on 26 June 2007 in accordance with the provisions of the internal regulations, in which they were instructed to observe working hours, to be present at the workplace [during those hours and] to make effective use of working time.

In conclusion, an employer who has made an investment is entitled, in exercising the rights enshrined in Article 40 § 1 of the Labour Code, to monitor internet use in the workplace, and an employee who breaches the employer's rules on personal internet use is committing a disciplinary offence that may give rise to a sanction, including the most serious one.

There is undoubtedly a conflict between the employer's right to engage in monitoring and the employees' right to protection of their privacy. This conflict has been settled at European Union level through the adoption of Directive no. 95/46/EC, which has laid down a number of principles governing the monitoring of internet and email use in the workplace, including the following in particular.

- Principle of necessity: monitoring must be necessary to achieve a certain aim.

- Principle of purpose specification: data must be collected for specified, explicit and legitimate purposes.

- Principle of transparency: the employer must provide employees with full information about monitoring operations.

- Principle of legitimacy: data-processing operations may only take place for a legitimate purpose.

- Principle of proportionality: personal data being monitored must be relevant and adequate in relation to the specified purpose.

- Principle of security: the employer is required to take all possible security measures to ensure that the data collected are not accessible to third parties.

In view of the fact that the employer has the right and the duty to ensure the smooth running of the company and, to that end, [is entitled] to supervise how its employees perform their professional tasks, and the fact [that it] enjoys disciplinary powers which it may legitimately use and which [authorised it in the present case] to monitor and transcribe the communications on Yahoo Messenger which the employee denied having exchanged for personal purposes, after he and his colleagues had been warned that company resources should not be used for such purposes, it cannot be maintained that this legitimate aim could have been achieved by any other means than by breaching the secrecy of his correspondence, or that a fair balance was not struck between the need to protect [the employee's] privacy and the employer's right to supervise the operation of its business.

...

Accordingly, having regard to the considerations set out above, the court finds that the decision of the first-instance court is lawful and well-founded and that the appeal is unfounded; it must therefore be dismissed, in accordance with the provisions of Article 312 § 1 of the C[ode of] Civ[il] Pr[ocedure]."

31. In the meantime, on 18 September 2007 the applicant had lodged a criminal complaint against the statutory representatives of S., alleging a breach of the secrecy of correspondence. On 9 May 2012 the Directorate for Investigating Organised Crime and Terrorism (DIICOT) of the prosecutor's office attached to the Supreme Court of Cassation and Justice ruled that there was no case to answer, on the grounds that the company was the owner of the computer system and the internet connection and could therefore monitor its employees' internet activity and use the information stored on the server, and in view of the prohibition on personal use of the IT systems, as a result of which the monitoring had been foreseeable. The applicant did not avail himself of the opportunity provided for by the applicable procedural rules to challenge the prosecuting authorities' decision in the domestic courts.

II. RELEVANT DOMESTIC LAW

A. The Constitution

32. The relevant parts of the Romanian Constitution provide:

Article 26

"1. The public authorities shall respect and protect intimate, family and private life."

Article 28

"The secrecy of letters, telegrams, other postal communications, telephone conversations and any other lawful means of communication is inviolable."

B. The Criminal Code

33. The relevant parts of the Criminal Code as in force at the material time read as follows:

Article 195 – Breach of secrecy of correspondence

"1. 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 and three years."

C. The Civil Code

34. The relevant provisions of the Civil Code as in force at the time of the events were worded as follows:

Article 998

"Any act committed by a person that causes damage to another shall render the person through whose fault the damage was caused liable to make reparation for it."

Article 999

"Everyone shall be liable for damage he has caused not only through his own acts but also through his failure to act or his negligence."

D. The Labour Code

35. As worded at the material time, the Labour Code provided:

Article 40

"1. The employer shall in principle have the following rights:

...

(d) to supervise how [employees] perform their professional tasks;

...

2. The employer shall in principle have the following duties:

...

(i) to guarantee the confidentiality of employees' personal data."

E. Law no. 677/2001 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

36. The relevant parts of Law no. 677/2001 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("Law no. 677/2001"), which reproduces certain provisions of 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 (see paragraph 45 below), provide:

Article 3 – Definitions

"For the purposes of this Law:

(a) 'personal data' shall mean any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

..."

Article 5 – Conditions for the legitimacy of data processing

"1. Personal data ... may not be processed in any way unless the data subject has explicitly and unambiguously consented to it.

2. The consent of the data subject shall not be necessary in the following circumstances:

(a) where processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

...

(e) where processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject;

...

3. The provisions of paragraph 2 are without prejudice to the statutory provisions governing the public authorities' duty to respect and protect intimate, family and private life."

Article 18 – Right to apply to the courts

"1. Data subjects shall be entitled, without prejudice to the

possibility of lodging a complaint with the supervisory authority, to apply to the courts for protection of the rights safeguarded by this Act that have been infringed.

2. Any person who has suffered damage as a result of the unlawful processing of his or her personal data may apply to the competent court for compensation [for the damage].

..."

III. INTERNATIONAL LAW AND PRACTICE

A. United Nations standards

37. The Guidelines for the regulation of computerized personal data files, adopted by the United Nations General Assembly on 14 December 1990 in Resolution 45/95 (A/RES/45/95), lay down the minimum guarantees that should be provided for in national legislation. The relevant principles read as follows:

" **1. Principle of lawfulness and fairness**

Information about persons should not be collected or processed in unfair or unlawful ways, nor should it be used for ends contrary to the purposes and principles of the Charter of the United Nations.

2. Principle of accuracy

Persons responsible for the compilation of files or those responsible for keeping them have an obligation to conduct regular checks on the accuracy and relevance of the data recorded and to ensure that they are kept as complete as possible in order to avoid errors of omission and that they are kept up to date regularly or when the information contained in a file is used, as long as they are being processed.

3. Principle of purpose specification

The purpose which a file is to serve and its utilization in terms of that purpose should be specified, legitimate and, when it is established, receive a certain amount of publicity or be brought to the attention of the person concerned, in order to make it possible subsequently to ensure that:

(a) All the personal data collected and recorded remain relevant and adequate to the purposes so specified;

(b) None of the said personal data is used or disclosed, except with the consent of the person concerned, for purposes incompatible with those specified;

(c) The period for which the personal data are kept does not exceed that which would enable the achievement of the purposes so specified.

4. Principle of interested-person access

Everyone who offers proof of identity has the right to know whether information concerning him is being processed and to obtain it in an intelligible form, without undue delay or expense, and to have appropriate rectifications or erasures made in the case of unlawful, unnecessary or inaccurate entries and, when it is being communicated, to be informed of the addressees. Provision should be made for a remedy, if need be with the supervisory authority specified in principle 8 below. The cost of any rectification shall be borne by the person responsible for the file. It is desirable that the provisions of this principle should apply to everyone, irrespective of nationality or place of residence.

...

6. Power to make exceptions

Departures from principles 1 to 4 may be authorized only if they are necessary to protect national security, public order, public health or morality, as well as, *inter alia* , the rights and freedoms of others, especially persons being persecuted (humanitarian clause) provided that such departures are expressly specified in a law or equivalent regulation promulgated in accordance with the internal legal system which expressly states their limits and sets forth appropriate safeguards.

..."

38. The International Labour Office (ILO) issued a Code of Practice on the Protection of Workers' Personal Data ("the ILO Code of Practice") in 1997, laying down the following principles:

" **5. General principles**

5.1. Personal data should be processed lawfully and fairly, and only for reasons directly relevant to the employment of the worker.

5.2. Personal data should, in principle, be used only for the purposes for which they were originally collected.

5.3. If personal data are to be processed for purposes other than those for which they were collected, the employer should ensure that they are not used in a manner incompatible with the original purpose, and should take the necessary measures to avoid any misinterpretations caused by a change of context.

5.4. Personal data collected in connection with technical or organizational measures to ensure the security and proper operation of automated information systems should not be used to control the behaviour of workers.

5.5. Decisions concerning a worker should not be based solely on the automated processing of that worker's personal data.

5.6. Personal data collected by electronic monitoring should not be the only factors in evaluating worker performance.

5.7. Employers should regularly assess their data processing practices:

(a) to reduce as far as possible the kind and amount of personal data collected; and

(b) to improve ways of protecting the privacy of workers.

5.8. Workers and their representatives should be kept informed of any data collection process, the rules that govern that process, and their rights.

...

5.13. Workers may not waive their privacy rights."

39. With regard to the more specific issue of monitoring of workers, the ILO Code of Practice states as follows:

" **6. Collection of personal data**

6.1. All personal data should, in principle, be obtained from the individual worker.

...

6.14. (1) If workers are monitored they should be informed in advance of the reasons for monitoring, the time schedule, the methods and techniques used and the data to be collected, and the employer must minimize the intrusion on the privacy of workers.

(2) Secret monitoring should be permitted only:

(a) if it is in conformity with national legislation; or

(b) if there is suspicion on reasonable grounds of criminal activity or other serious wrongdoing.

(3) Continuous monitoring should be permitted only if required for health and safety or the protection of property."

40. The ILO Code of Practice also includes an inventory of workers' individual rights, particularly as regards information about the processing of personal data, access to such data and reviews of any measures taken. The relevant parts read as follows:

" **11. Individual rights**

11.1. Workers should have the right to be regularly notified of the personal data held about them and the processing of that personal data.

11.2. Workers should have access to all their personal data, irrespective of whether the personal data are processed by automated systems or are kept in a particular manual file regarding the individual worker or in any other file which includes workers' personal data.

11.3. The workers' right to know about the processing of their personal data should include the right to examine and obtain a copy of any records to the extent that the data contained in the record includes that worker's personal data.

...

11.8. Employers should, in the event of a security investigation, have the right to deny the worker access to that worker's personal data until the close of the investigation and to the extent that the purposes of the investigation would be threatened. No decision concerning the employment relationship should be taken, however, before the worker has had access to all the worker's personal data.

11.9. Workers should have the right to demand that incorrect or incomplete personal data, and personal data processed inconsistently with the provisions of this code, be deleted or rectified.

...

11.13. In any legislation, regulation, collective agreement, work rules or policy developed consistent with the provisions of this code, there should be specified an avenue of redress for workers to challenge the employer's compliance with the instrument. Procedures should be established to receive and respond to any complaint lodged by workers. The complaint process should be easily accessible to workers and be simple to use."

41. In addition, on 18 December 2013 the United Nations General Assembly adopted Resolution no. 68/167 on the right to privacy in the digital age (A/RES/68/167), in which, *inter alia* , it called upon States:

"(*a*) To respect and protect the right to privacy, including in the context of digital communication;

(*b*) To take measures to put an end to violations of those rights and to create the conditions to prevent such violations, including by ensuring that relevant national legislation complies with their obligations under international human rights law;

(*c*) To review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law;

(*d*) To establish or maintain existing independent, effective domestic oversight mechanisms capable of ensuring

transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data[.]"

B. Council of Europe standards

42. The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981, ETS no. 108), which came into force in respect of Romania on 1 June 2002, includes the following provisions in particular:

Article 2 – Definitions

"For the purposes of this Convention:

(a) 'personal data' means any information relating to an identified or identifiable individual ('data subject');

...

(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;

...

(d) to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with."

Article 9 – Exceptions and restrictions

"...

2. Derogation from the provisions of Articles 5, 6 and 8 of this Convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:

(a) protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;

(b) protecting the data subject or the rights and freedoms of others;

..."

Article 10 – Sanctions and remedies

"Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter."

43. Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment, which was adopted on 1 April 2015, states in particular:

" **4. Application of data processing principles**

4.1. Employers should minimise the processing of personal data to only the data necessary to the aim pursued in the individual cases concerned.

...

6. Internal use of data

6.1. Personal data collected for employment purposes should only be processed by employers for such purposes.

6.2. Employers should adopt data protection policies, rules and/or other instruments on internal use of personal data in compliance with the principles of the present recommendation.

...

10. Transparency of processing

10.1. Information concerning personal data held by employers should be made available either to the employee concerned directly or through the intermediary of his or her representatives, or brought to his or her notice through other appropriate means.

10.2. Employers should provide employees with the following information:

– the categories of personal data to be processed and a description of the purposes of the processing;

– the recipients, or categories of recipients of the personal data;

– the means employees have of exercising the rights set out in principle 11 of the present recommendation, without prejudice to more favourable ones provided by domestic law or in their legal system;

– any other information necessary to ensure fair and lawful processing.

10.3. A particularly clear and complete description must be provided of the categories of personal data that can be collected by ICTs, including video surveillance and their possible use. This principle also applies to the particular forms of processing provided for in Part II of the appendix to the present recommendation.

10.4. The information should be provided in an accessible format and kept up to date. In any event, such information should be provided before an employee carries out the activity or action concerned, and made readily available through the information systems normally used by the employee.

...

14. Use of Internet and electronic communications in the workplace

14.1. Employers should avoid unjustifiable and unreasonable interferences with employees' right to private life. This principle extends to all technical devices and ICTs used by an employee. The persons concerned should be properly and periodically informed in application of a clear privacy policy, in accordance with principle 10 of the present recommendation. The information provided should be kept up to date and should include the purpose of the processing, the preservation or back-up period of traffic data and the archiving of professional electronic communications.

14.2. In particular, in the event of processing of personal data relating to Internet or Intranet pages accessed by the employee, preference should be given to the adoption of preventive measures, such as the use of filters which prevent particular operations, and to the grading of possible monitoring on personal data, giving preference for nonindividual random checks on data which are anonymous or in some way aggregated.

14.3. Access by employers to the professional electronic communications of their employees who have been informed in advance of the existence of that possibility can only occur, where necessary, for security or other legitimate reasons. In case of absent employees, employers should take the necessary measures and foresee the appropriate procedures aimed at enabling access to professional electronic communications only when such access is of professional necessity. Access should be undertaken in the least intrusive way possible and only after having informed the employees concerned.

14.4. The content, sending and receiving of private electronic communications at work should not be monitored under any circumstances.

14.5. On an employee's departure from an organisation, the employer should take the necessary organisational and technical measures to automatically deactivate the employee's electronic messaging account. If employers need to recover the contents of an employee's account for the efficient running of the organisation, they should do so before his or her departure and, when feasible, in his or her presence."

IV. EUROPEAN UNION LAW

44. The relevant provisions of the Charter of Fundamental Rights of the European Union (2007/C 303/01) are worded as follows:

Article 7 – Respect for private and family life

"Everyone has the right to respect for his or her private and family life, home and communications."

Article 8 – Protection of personal data

"1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it

rectified.

3. Compliance with these rules shall be subject to control by an independent authority."

45. 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 ("Directive 95/46/EC") states that the object of national laws on the processing of personal data is notably to protect the right to privacy, as recognised both in Article 8 of the Convention and in the general principles of Community law. The relevant provisions of Directive 95/46/EC read as follows:

Article 2 – Definitions

"For the purposes of this Directive:

(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

..."

Article 6

"1. Member States shall provide that personal data must be:

(a) processed fairly and lawfully;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes . Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

2. It shall be for the controller to ensure that paragraph 1 is complied with."

Article 7

"Member States shall provide that personal data may be processed only if:

(a) the data subject has unambiguously given his consent; or

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

(d) processing is necessary in order to protect the vital interests of the data subject; or

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1)."

Article 8 – The processing of special categories of data

"1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

2. Paragraph 1 shall not apply where:

(a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or

(b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or

(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or

...

(e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

...

4. Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority."

46. A Working Party on Data Protection ("the Working Party") has been set up under Article 29 of the Directive and, in accordance with Article 30, is empowered to:

"(a) examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures;

(b) give the Commission an opinion on the level of protection in the Community and in third countries;

(c) advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms;

(d) give an opinion on codes of conduct drawn up at Community level."

The Working Party is an independent advisory body of the European Union. It issued an opinion in September 2001 on the processing of personal data in an employment context (opinion 8/2001), which summarises the fundamental data-protection principles: finality, transparency, legitimacy, proportionality, accuracy, security and staff awareness. In the opinion, which it adopted in conformity with its role of contributing to the uniform application of national measures adopted under Directive 95/46/EC, the Working Party pointed out that the monitoring of email involved the processing of personal data, and expressed the view that any monitoring of employees had to be

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

47. In May 2002 the Working Party produced a working document on surveillance and monitoring of electronic communications in the workplace ("the working document"), in which it expressly took into account the provisions of Directive 95/46/EC read in the light of the provisions of Article 8 of the Convention. The working document asserts that the simple fact that a monitoring activity or surveillance is considered convenient to serve an employer's interest cannot in itself justify an intrusion into workers' privacy, and that any monitoring measure must satisfy four criteria: transparency, necessity, fairness and proportionality.

48. Regarding the technical aspect, the working document states:

"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."

49. More specifically, with regard to the question of access to employees' emails, the working document includes the following passage:

"It would only be in exceptional circumstances that the monitoring of a worker's [e]mail or Internet use would be considered necessary. For instance, monitoring of a worker's email may become necessary in order to obtain confirmation or proof of certain actions on his part. Such actions would include criminal activity on the part of the worker insofar as it is necessary for the employer to defend his own interests, for example, where he is vicariously liable for the actions of the worker. These activities would also include detection of viruses and in general terms any activity carried out by the employer to guarantee the security of the system.

It should be mentioned that opening an employee's email 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 (e.g. due to sickness or leave) and correspondence cannot be guaranteed otherwise (e.g. via auto reply or automatic forwarding)."

50. The Court of Justice of the European Union has interpreted the provisions of Directive 95/46/EC in the light of the right to respect for private life, as guaranteed by Article 8 of the Convention, in the case of *Österreichischer Rundfunk and Others* (C-465/00, C138/01 and C139/01, judgment of 20 May 2003, ECLI:EU:C:2003:294, paragraphs 71 et seq.).

51. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), published in OJ 2016 L 119/1, entered into force on 24 May 2016 and will repeal Directive 95/46/EC with effect from 25 May 2018 (Article 99). The relevant provisions of the Regulation read as follows:

Article 30 – Records of processing activities

"1 Each controller and, where applicable, the controller's representative, shall maintain a record of processing

activities under its responsibility. That record shall contain all of the following information:

(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

(b) the purposes of the processing;

(c) a description of the categories of data subjects and of the categories of personal data;

(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(f) where possible, the envisaged time limits for erasure of the different categories of data;

(g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

2. Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

(a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;

(b) the categories of processing carried out on behalf of each controller;

(c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

4. The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.

5. The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10."

Article 47 – Binding corporate rules

"1. The competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism set out in Article 63, provided that they:

(a) are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;

(b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and

(c) fulfil the requirements laid down in paragraph 2.

2. The binding corporate rules referred to in paragraph 1 shall specify at least:

(a) the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;

(b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;

(c) their legally binding nature, both internally and externally;

(d) the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;

(e) the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 22, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with Article 79, and to obtain redress and, where appropriate, compensation for a breach

of the binding corporate rules;

(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union; the controller or the processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage;

(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in addition to Articles 13 and 14;

(h) the tasks of any data protection officer designated in accordance with Article 37 or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling;

(i) the complaint procedures;

(j) the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred to in point (h) and to the board of the controlling undertaking of a group of undertakings, or of the group of enterprises engaged in a joint economic activity, and should be available upon request to the competent supervisory authority;

(k) the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority;

(l) the cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority the results of verifications of the measures referred to in point (j);

(m) the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and

(n) the appropriate data protection training to personnel having permanent or regular access to personal data.

3. The Commission may specify the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).”

Article 88 – Processing in the context of employment

“1. Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees’ personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer’s or customer’s property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

2. Those rules shall include suitable and specific measures to safeguard the data subject’s human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place.

3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.”

V. COMPARATIVE LAW

52. The documents available to the Court concerning the legislation of the Council of Europe member States, in particular a study of thirty-four of them, indicate that all the States concerned recognise in general terms, at constitutional or statutory level, the right to privacy and to secrecy of correspondence. However, only Austria, Finland, Luxembourg, Portugal, Slovakia and the United Kingdom have explicitly regulated the issue of workplace privacy, whether in labour laws or in special legislation.

53. With regard to monitoring powers, thirty-four Council of Europe member States require employers to give employees prior notice of monitoring. This may take a number of forms, for example notification of the personal data-protection authorities or of workers’ representatives. The existing legislation in Austria, Estonia, Finland, Greece, Lithuania, Luxembourg, Norway, Poland, Slovakia and the former Yugoslav Republic of Macedonia requires employers

to notify employees directly before initiating the monitoring.

54. In, Austria, Denmark, Finland, France, Germany, Greece, Italy, Portugal and Sweden, employers may monitor emails marked by employees as "private", without being permitted to access their content. In Luxembourg employers may not open emails that are either marked as "private" or are manifestly of a private nature. The Czech Republic, Italy and Slovenia, as well as the Republic of Moldova to a certain extent, also limit the extent to which employers may monitor their employees' communications, according to whether the communications are professional or personal in nature. In Germany and Portugal, once it has been established that a message is private, the employer must stop reading it.

THE LAW

I. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

55. The applicant submitted that his dismissal by his employer had been based on a breach of his right to respect for his private life and correspondence and that, by not revoking that measure, the domestic courts had failed to comply with their obligation to protect the right in question. He relied on Article 8 of the Convention, which 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."

A. The Chamber's findings

56. In its judgment of 12 January 2016 the Chamber held, firstly, that Article 8 of the Convention was applicable in the present case. Referring to the concept of reasonable expectation of privacy, it found that the present case differed from *Copland* (cited above, § 41) and *Halford v. the United Kingdom* (25 June 1997, § 45, *Reports of Judgments and Decisions* 1997III) in that the applicant's employer's internal regulations in the present case strictly prohibited employees from using company computers and resources for personal purposes. The Chamber had regard to the nature of the applicant's communications and the fact that a transcript of them had been used as evidence in the domestic court proceedings, and concluded that the applicant's right to respect for his "private life" and "correspondence" was at stake.

57. Next, the Chamber examined the case from the standpoint of the State's positive obligations, since the decision to dismiss the applicant had been taken by a private-law entity. It therefore determined whether the national authorities had struck a fair balance between the applicant's right to respect for his private life and correspondence and his employer's interests.

58. The Chamber noted that the applicant had been able to bring his case and raise his arguments before the labour courts. The courts had found that he had committed a disciplinary offence by using the internet for personal purposes during working hours, and to that end they had had regard to the conduct of the disciplinary proceedings, in particular the fact that the employer had accessed the contents of the applicant's communications only after the applicant had declared that he had used Yahoo Messenger for work-related purposes.

59. The Chamber further noted that the domestic courts had not based their decisions on the contents of the applicant's communications and that the employer's monitoring activities had been limited to his use of Yahoo Messenger.

60. Accordingly, it held that there had been no violation of Article 8 of the Convention.

B. Scope of the case before the Grand Chamber

61. The Court notes that in the proceedings before the Chamber the applicant alleged 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 as enshrined in Article 8 of the Convention and that, by not revoking that measure, the domestic courts had failed to comply with their obligation to protect the right in question. The Chamber declared this complaint admissible on 12 January 2016.

62. The Court reiterates that the case referred to the Grand Chamber is the application as it has been declared admissible by the Chamber (see *K. and T. v. Finland* [GC], no. 25702/94, §§ 140-41, ECHR 2001VII; *D.H. and Others v. the Czech Republic* [GC], no. 57325/00, § 109, ECHR 2007IV; and *Blokhin v. Russia* [GC], no. 47152/06, § 91, ECHR 2016).

63. In his observations before the Grand Chamber, the applicant complained for the first time about the rejection in 2012 of the criminal complaint filed by him in connection with an alleged breach of the secrecy of correspondence (see paragraph 90 below).

64. This new complaint was not mentioned in the decision of 12 January 2016 as to admissibility, which defines the boundaries of the examination of the application. It therefore falls outside the scope of the case as referred to the Grand Chamber, which accordingly does not have jurisdiction to deal with it and will limit its examination to the complaint that

was declared admissible by the Chamber.

C. Applicability of Article 8 of the Convention

1. The parties' submissions

(a) The Government

65. The Government argued that the applicant could not claim any expectation of "privacy" as regards the communications he had exchanged via an instant messaging account created for professional use. With reference to the case-law of the French and Cypriot courts, they submitted that messages sent by an employee using the technical facilities made available to him by his employer had to be regarded as professional in nature unless the employee explicitly identified them as private. They noted that it was not technically possible using Yahoo Messenger to mark messages as private; nevertheless, the applicant had had an adequate opportunity, during the initial stage of the disciplinary proceedings, to indicate that his communications had been private, and yet had chosen to maintain that they had been work-related. The applicant had been informed not only of his employer's internal regulations, which prohibited all personal use of company resources, but also of the fact that his employer had initiated a process for monitoring his communications.

66. The Government relied on three further arguments in contending that Article 8 of the Convention was not applicable in the present case. Firstly, there was no evidence to suggest that the transcript of the applicant's communications had been disclosed to his work colleagues; the applicant himself had produced the full transcript of the messages in the proceedings before the domestic courts, without asking for any restrictions to be placed on access to the documents concerned. Secondly, the national authorities had used the transcript of the messages as evidence because the applicant had so requested, and because the prosecuting authorities had already found that the monitoring of his communications had been lawful. Thirdly, the information notice had contained sufficient indications for the applicant to have been aware that his employer could monitor his communications, and this had rendered them devoid of any private element.

(b) The applicant

67. The applicant did not make any submissions as to the applicability of Article 8 of the Convention, but repeatedly maintained that his communications had been private in nature.

68. He further argued that, since he had created the Yahoo Messenger account in question and was the only person who knew the password, he had had a reasonable expectation of privacy regarding his communications. He also asserted that he had not received prior notification from his employer about the monitoring of his communications.

2. The Court's assessment

69. The Court notes that the question arising in the present case is whether the matters complained of by the applicant fall within the scope of Article 8 of the Convention.

70. At this stage of its examination it considers it useful to emphasise that "private life" is a broad term not susceptible to exhaustive definition (see *Sidabras and Džiautas v. Lithuania* , nos. 55480/00 and 59330/00, § 43, ECHR 2004VIII). Article 8 of the Convention protects the right to personal development (see *K.A. and A.D. v. Belgium* , nos. 42758/98 and 45558/99, § 83, 17 February 2005), whether in terms of personality (see *Christine Goodwin v. the United Kingdom* [GC], no. 28957/95, § 90, ECHR 2002-VI) or of personal autonomy, which is an important principle underlying the interpretation of the Article 8 guarantees (see *Pretty v. the United Kingdom* , no. 2346/02, § 61, ECHR 2002-III). The Court acknowledges that everyone has the right to live privately, away from unwanted attention (see *Smirnova v. Russia* , nos. 46133/99 and 48183/99, § 95, ECHR 2003IX (extracts)). It also considers that it would be too restrictive to limit the notion of "private life" to an "inner circle" in which the individual may live his or her own personal life as he or she chooses, thus excluding entirely the outside world not encompassed within that circle (see *Niemietz v. Germany* , 16 December 1992, § 29, Series A no. 251B). Article 8 thus guarantees a right to "private life" in the broad sense, including the right to lead a "private social life", that is, the possibility for the individual to develop his or her social identity. In that respect, the right in question enshrines the possibility of approaching others in order to establish and develop relationships with them (see *Bigaeva v. Greece* , no. 26713/05, § 22, 28 May 2009, and *Özpınar v. Turkey* , no. 20999/04, § 45 *in fine* , 19 October 2010).

71. The Court considers that the notion of "private life" may include professional activities (see *Fernández Martínez v. Spain* [GC], no. 56030/07, § 110, ECHR 2014 (extracts), and *Oleksandr Volkov v. Ukraine* , no. 21722/11, §§ 165-66, ECHR 2013), or activities taking place in a public context (see Von Hannover v. Germany (no. 2) [GC], nos. 40660/08 and 60641/08, § 95, ECHR 2012). Restrictions on an individual's professional life may fall within Article 8 where they have repercussions on the manner in which he or she constructs his or her social identity by developing relationships with others. It should be noted in this connection that it is in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity to develop relationships with the outside world (see *Niemietz* , cited above, § 29).

72. Furthermore, as regards the notion of "correspondence", it should be noted that in the wording of Article 8 this word is not qualified by any adjective, unlike the term "life". And indeed, the Court has already held that,

in the context of correspondence by means of telephone calls, no such qualification is to be made. In a number of cases relating to correspondence with a lawyer, it has not even envisaged the possibility that Article 8 might be inapplicable on the ground that the correspondence was of a professional nature (see *Niemietz* , cited above, § 32, with further references). Furthermore, it has held that telephone conversations are covered by the notions of "private life" and "correspondence" within the meaning of Article 8 (see *Roman Zakharov v. Russia* [GC], no. 47143/06, § 173, ECHR 2015). In principle, this is also true where telephone calls are made from or received on business premises (see *Halford* , cited above, § 44, and *Amann v. Switzerland* [GC], no. 27798/95, § 44, ECHR 2000II). The same applies to emails sent from the workplace, which enjoy similar protection under Article 8, as does information derived from the monitoring of a person's internet use (see *Copland* , cited above, § 41 *in fine*).

73. It is clear from the Court's case-law that communications from business premises as well as from the home may be covered by the notions of "private life" and "correspondence" within the meaning of Article 8 of the Convention (see *Halford* , cited above, § 44; and *Copland* , cited above, § 41). In order to ascertain whether the notions of "private life" and "correspondence" are applicable, the Court has on several occasions examined whether individuals had a reasonable expectation that their privacy would be respected and protected (ibid.; and as regards "private life", see also *Köpke v. Germany* (dec.), no. 420/07, 5 October 2010). In that context, it has stated that a reasonable expectation of privacy is a significant though not necessarily conclusive factor (see *Köpke* , cited above).

74. Applying these principles in the present case, the Court first observes that the kind of internet instant messaging service at issue is just one of the forms of communication enabling individuals to lead a private social life. At the same time, the sending and receiving of communications is covered by the notion of "correspondence", even if they are sent from an employer's computer. The Court notes, however, that the applicant's employer instructed him and the other employees to refrain from any personal activities in the workplace. This requirement on the employer's part was reflected in measures including a ban on using company resources for personal purposes (see paragraph 12 above).

75. The Court further notes that with a view to ensuring that this requirement was met, the employer set up a system for monitoring its employees' internet use (see paragraphs 17 and 18 above). The documents in the case file, in particular those relating to the disciplinary proceedings against the applicant, indicate that during the monitoring process, both the flow and the content of the applicants' communications were recorded and stored (see paragraphs 18 and 20 above).

76. The Court observes in addition that despite this requirement on the employer's part, the applicant exchanged messages of a personal nature with his fiancée and his brother (see paragraph 21 above). Some of these messages were of an intimate nature (ibid.).

77. The Court considers that it is clear from the case file that the applicant had indeed been informed of the ban on personal internet use laid down in his employer's internal regulations (see paragraph 14 above). However, it is not so clear that he had been informed prior to the monitoring of his communications that such a monitoring operation was to take place. Thus, the Government submitted that the applicant had acquainted himself with the employer's information notice on an unspecified date between 3 and 13 July 2007 (see paragraph 16 above). Nevertheless, the domestic courts omitted to ascertain whether the applicant had been informed of the monitoring operation before the date on which it began, given that the employer recorded communications in real time from 5 to 13 July 2007 (see paragraph 17 above).

78. In any event, it does not appear that the applicant was informed in advance of the extent and nature of his employer's monitoring activities, or of the possibility that the employer might have access to the actual contents of his communications.

79. The Court also takes note of the applicant's argument that he himself had created the Yahoo Messenger account in question and was the only person who knew the password (see paragraph 68 above). In addition, it observes that the material in the case file indicates that the employer also accessed the applicant's personal Yahoo Messenger account (see paragraph 21 above). Be that as it may, the applicant had created the Yahoo Messenger account in issue on his employer's instructions to answer customers' enquiries (see paragraph 11 above), and the employer had access to it.

80. It is open to question whether – and if so, to what extent – the employer's restrictive regulations left the applicant with a reasonable expectation of privacy. Be that as it may, an employer's instructions cannot reduce private social life in the workplace to zero. Respect for private life and for the privacy of correspondence continues to exist, even if these may be restricted in so far as necessary.

81. In the light of all the above considerations, the Court concludes that the applicant's communications in the workplace were covered by the concepts of "private life" and "correspondence". Accordingly, in the circumstances of the present case, Article 8 of the Convention is applicable.

D. Compliance with Article 8 of the Convention

1. The parties' submissions and third-party comments

(a) The applicant

82. In his written observations before the Grand Chamber, the applicant submitted that the Chamber had not taken sufficient account of certain factual aspects of the case. Firstly, he emphasised the specific features of Yahoo Messenger, which was designed for personal use. His employer's decision to use this tool in a work context did not alter the fact that it was essentially intended to be used for personal purposes. He thus considered himself to be the sole owner of the Yahoo Messenger account that he had opened at his employer's request.

83. Secondly, the applicant argued that his employer had not introduced any policy on internet use. He had not had any warning of the possibility that his communications might be monitored or read; nor had he given any consent in that regard. If such a policy had been in place and he had been informed of it, he would have refrained from disclosing certain aspects of his private life on Yahoo Messenger.

84. Thirdly, the applicant contended that a distinction should be drawn between personal internet use having a profit-making purpose and "a small harmless private conversation" which had not sought to derive any profit and had not caused any damage to his employer; he pointed out in that connection that during the disciplinary proceedings against him, the employer had not accused him of having caused any damage to the company. The applicant highlighted developments in information and communication technologies, as well as in the social customs and habits linked to their use. He submitted that contemporary working conditions made it impossible to draw a clear dividing line between private and professional life, and disputed the legitimacy of any management policy prohibiting personal use of the internet and of any connected devices.

85. From a legal standpoint, the applicant submitted that the Romanian State had not fulfilled its positive obligations under Article 8 of the Convention. More specifically, the domestic courts had not overturned his dismissal despite having acknowledged that there had been a violation of his right to respect for his private communications.

86. Firstly, he submitted that the Chamber had incorrectly distinguished the present case from *Copland* (cited above, § 42). In his view, the decisive factor in analysing the case was not whether the employer had tolerated personal internet use, but the fact that the employer had not warned the employee that his communications could be monitored. In that connection, he contended that his employer had first placed him under surveillance and had only afterwards given him the opportunity to specify whether his communications were private or work-related. The Court had to examine both whether an outright ban on personal internet use entitled the employer to monitor its employees, and whether the employer had to give reasons for such monitoring.

87. Secondly, the applicant submitted that the Chamber's analysis in relation to the second paragraph of Article 8 was not consistent with the Court's case-law in that it had not sought to ascertain whether the interference with his right to respect for his private life and correspondence had been in accordance with the law, had pursued a legitimate aim and had been necessary in a democratic society.

88. With regard to the jurisdiction of the labour courts, the applicant contended that they were competent to carry out a full review of the lawfulness and justification of the measure referred to them. It was for the courts to request the production of the necessary evidence and to raise any relevant factual or legal issues, even where they had not been mentioned by the parties. Accordingly, the labour courts had extensive jurisdiction to examine any issues relating to a labour-law dispute, including those linked to respect for employees' private life and correspondence.

89. However, in the applicant's case the domestic courts had pursued a rigid approach, aimed simply at upholding his employer's decision. They had performed an incorrect analysis of the factual aspects of the case and had failed to take into account the specific features of communications in cyberspace. The violation of the applicant's right to respect for his private life and correspondence had thus been intentional and illegal and its aim had been to gather evidence enabling his contract to be terminated.

90. Lastly, the applicant complained for the first time in the proceedings before the Grand Chamber of the outcome of the criminal complaint he had lodged in 2007: in 2012 the department of the prosecutor's office with responsibility for investigating organised crime and terrorism (DIICOT) had rejected the complaint without properly establishing the facts of the case.

91. At the hearing before the Grand Chamber the applicant stated, in reply to a question from the judges, that because his employer had only made a single printer available to employees, all his colleagues had been able to see the contents of the forty-five-page transcript of his Yahoo Messenger communications.

92. The applicant urged the Grand Chamber to find a violation of Article 8 of the Convention and to take the opportunity to confirm that monitoring of employees' correspondence could only be carried out in compliance with the applicable legislation, in a transparent manner and on grounds provided for by law, and that employers did not have discretion to monitor their employees' correspondence.

(b) The Government

93. The Government stated that the employer had recorded the applicant's communications from 5 to 13 July 2007 and had then given him an opportunity to account for his internet use, which was more substantial than that of his colleagues. They pointed out that since the applicant had maintained that the contents of his communications were work-related, the employer had investigated his explanations.

94. The Government argued that in his appeal against the decision of the first-instance court the applicant had not challenged the court's finding that he had been informed that his employer was monitoring internet use. In that connection, they produced a copy of the information notice issued by the employer and signed by the applicant. On the basis of the employer's attendance register, they observed that the applicant had signed the notice between 3 and 13 July 2007.

95. The Government further submitted that the employer had recorded the applicant's communications in real time. There was no evidence that the employer had accessed the applicant's previous communications or his private email.

96. The Government indicated their agreement with the Chamber's conclusions and submitted that the Romanian State had satisfied its positive obligations under Article 8 of the Convention.

97. They observed firstly that the applicant had chosen to raise his complaints in the domestic courts in the context of a labour-law dispute. The courts had examined all his complaints and weighed up the various interests at stake, but the main focus of their analysis had been whether the disciplinary proceedings against the applicant had been compliant with domestic law. The applicant had had the option of raising before the domestic courts his specific complaint of a violation of his right to respect for his private life, for example by means of an action under Law no. 677/2001 or an action in tort, but he had chosen not to do so. He had also filed a criminal complaint, which had given rise to a decision by the prosecuting authorities to take no further action on the grounds that the monitoring by the employer of employees' communications had not been unlawful.

98. Referring more specifically to the State's positive obligations, the Government submitted that approaches among Council of Europe member States varied greatly as regards the regulation of employee monitoring by employers. Some States included this matter within the wider scope of personal data processing, while others had passed specific legislation in this sphere. Even among the latter group of States, there were no uniform solutions regarding the scope and purpose of monitoring by the employer, prior notification of employees or personal internet use.

99. Relying on *K ö pke* (cited above), the Government maintained that the domestic courts had performed an appropriate balancing exercise between the applicant's right to respect for his private life and correspondence and his employer's right to organise and supervise work within the company. In the Government's submission, where communications were monitored by a private entity, an appropriate examination by the domestic courts was sufficient for the purposes of Article 8 and there was no need for specific protection by means of a legislative framework.

100. The Government further submitted that the domestic courts had reviewed the lawfulness and the necessity of the employer's decision and had concluded that the disciplinary proceedings had been conducted in accordance with the legislation in force. They attached particular importance to the manner in which the proceedings had been conducted, especially the opportunity given to the applicant to indicate whether the communications in question had been private. If he had made use of that opportunity, the domestic courts would have weighed up the interests at stake differently.

101. In that connection, the Government noted that in the proceedings before the domestic authorities the applicant himself had produced the full transcripts of his communications, without taking any precautions; he could instead have disclosed only the names of the relevant accounts or submitted extracts of his communications, for example those that did not contain any intimate information. The Government also disputed the applicant's allegations that his communications had been disclosed to his colleagues and pointed out that only the three-member disciplinary board had had access to them.

102. The Government further contended that the employer's decision had been necessary, since it had had to investigate the arguments raised by the applicant in the disciplinary proceedings in order to determine whether he had complied with the internal regulations.

103. Lastly, the Government argued that a distinction should be made between the nature of the communications and their content. They observed, as the Chamber had, that the domestic courts had not taken the content of the applicant's communications into account at all but had simply examined their nature and found that they were personal.

104. The Government thus concluded that the applicant's complaint under Article 8 of the Convention was ill-founded.

(c) Third parties

(i) The French Government

105. The French Government referred, in particular, to their conception of the scope of the national authorities' positive

obligation to ensure respect for employees' private life and correspondence. They provided a comprehensive overview of the applicable provisions of French civil law, labour law and criminal law in this sphere. In their submission, Article 8 of the Convention was only applicable to strictly personal data, correspondence and electronic activities. In that connection, they referred to settled case-law of the French Court of Cassation to the effect that any data processed, sent and received by means of the employer's electronic equipment were presumed to be professional in nature unless the employee designated them clearly and precisely as personal.

106. The French Government submitted that States had to enjoy a wide margin of appreciation in this sphere since the aim was to strike a balance between competing private interests. The employer could monitor employees' professional data and correspondence to a reasonable degree, provided that a legitimate aim was pursued, and could use the results of the monitoring operation in disciplinary proceedings. They emphasised that employees had to be given advance notice of such monitoring. In addition, where data clearly designated as personal by the employee were involved, the employer could ask the courts to order investigative measures and to instruct a bailiff to access the relevant data and record their content.

(ii) The European Trade Union Confederation

107. The European Trade Union Confederation submitted that it was crucial to protect privacy in the working environment, taking into account in particular the fact that employees were structurally dependent on employers in this context. After summarising the applicable principles of international and European law, it stated that internet access should be regarded as a human right and that the right to respect for correspondence should be strengthened. The consent, or at least prior notification, of employees was required, and staff representatives had to be informed, before the employer could process employees' personal data.

2. The Court's assessment

(a) Whether the case concerns a negative or a positive obligation

108. The Court must determine whether the present case should be examined in terms of the State's negative or positive obligations. It reiterates that by Article 1 of the Convention, the Contracting Parties "shall secure to everyone within their jurisdiction the rights and freedoms defined in ... [the] Convention". While the essential object of Article 8 of the Convention is to protect individuals against arbitrary interference by public authorities, it may also impose on the State certain positive obligations to ensure effective respect for the rights protected by Article 8 (see, among other authorities, *X and Y v. the Netherlands* , 26 March 1985, § 23, Series A no. 91; *Von Hannover (no. 2)* , cited above, § 98; and *Hämäläinen v. Finland* [GC], no. 37359/09, § 62, ECHR 2014).

109. In the present case the Court observes that the measure complained of by the applicant, namely the monitoring of Yahoo Messenger communications, which resulted in disciplinary proceedings against him followed by his dismissal for infringing his employer's internal regulations prohibiting the personal use of company resources, was not taken by a State authority but by a private commercial company. The monitoring of the applicant's communications and the inspection of their content by his employer in order to justify his dismissal cannot therefore be regarded as "interference" with his right by a State authority.

110. Nevertheless, the Court notes that the measure taken by the employer was accepted by the national courts. It is true that the monitoring of the applicant's communications was not the result of direct intervention by the national authorities; however, their responsibility would be engaged if the facts complained of stemmed from a failure on their part to secure to the applicant the enjoyment of a right enshrined in Article 8 of the Convention (see, *mutatis mutandis* , *Obst v. Germany* , no. 425/03, §§ 40 and 43, 23 September 2010, and *Schüth v. Germany* , no. 1620/03, §§ 54 and 57, ECHR 2010).

111. In the light of the particular circumstances of the case as described in paragraph 109 above, the Court considers, having regard to its conclusion concerning the applicability of Article 8 of the Convention (see paragraph 81 above) and to the fact that the applicant's enjoyment of his right to respect for his private life and correspondence was impaired by the actions of a private employer, that the complaint should be examined from the standpoint of the State's positive obligations.

112. While the boundaries between the State's positive and negative obligations under the Convention do not lend themselves to precise definition, the applicable principles are nonetheless similar. In both contexts regard must be had in particular to the fair balance that has to be struck between the competing interests of the individual and of the community as a whole, subject in any event to the margin of appreciation enjoyed by the State (see *Palomo Sánchez and Others v. Spain* [GC], nos. 28955/06 and 3 others, § 62, ECHR 2011).

(b) General principles applicable to the assessment of the State's positive obligation to ensure respect for private life and correspondence in an employment context

113. The Court reiterates that the choice of the means calculated to secure compliance with Article 8 of the Convention in the sphere of the relations of individuals between themselves is in principle a matter that falls within

the Contracting States' margin of appreciation. There are different ways of ensuring respect for private life, and the nature of the State's obligation will depend on the particular aspect of private life that is at issue (see *Söderman v. Sweden* [GC], no. 5786/08, § 79, ECHR 2013, with further references).

114. The Court's task in the present case is therefore to clarify the nature and scope of the positive obligations that the respondent State was required to comply with in protecting the applicant's right to respect for his private life and correspondence in the context of his employment.

115. The Court observes that it has held that in certain circumstances, the State's positive obligations under Article 8 of the Convention are not adequately fulfilled unless it secures respect for private life in the relations between individuals by setting up a legislative framework taking into consideration the various interests to be protected in a particular context (see *X and Y v. the Netherlands* , cited above, §§ 23, 24 and 27, and *M.C. v. Bulgaria* , no. 39272/98, § 150, ECHR 2003XII, both concerning sexual assaults of minors; see also *K.U. v. Finland* , no. 2872/02, §§ 43 and 49, ECHR 2008, concerning an advertisement of a sexual nature placed on an internet dating site in the name of a minor; *Söderman* , cited above, § 85, concerning the effectiveness of remedies in respect of an alleged violation of personal integrity committed by a close relative; and *Codarcea v. Romania* , no. 31675/04, §§ 102-04, 2 June 2009, concerning medical negligence).

116. The Court accepts that protective measures are not only to be found in labour law, but also in civil and criminal law. As far as labour law is concerned, it must ascertain whether in the present case the respondent State was required to set up a legislative framework to protect the applicant's right to respect for his private life and correspondence in the context of his professional relationship with a private employer.

117. In this connection it considers at the outset that labour law has specific features that must be taken into account. The employer-employee relationship is contractual, with particular rights and obligations on either side, and is characterised by legal subordination. It is governed by its own legal rules, which differ considerably from those generally applicable to relations between individuals (see *Saumier v. France* , no. 74734/14, § 60, 12 January 2017).

118. From a regulatory perspective, labour law leaves room for negotiation between the parties to the contract of employment. Thus, it is generally for the parties themselves to regulate a significant part of the content of their relations (see, *mutatis mutandis* , *Wretlund v. Sweden* (dec.), no. 46210/99, 9 March 2004, concerning the compatibility with Article 8 of the Convention of the obligation for the applicant, an employee at a nuclear plant, to undergo drug tests; with regard to trade-union action from the standpoint of Article 11, see *Gustafsson v. Sweden* , 25 April 1996, § 45, *Reports* 1996II, and, *mutatis mutandis* , *Demir and Baykara v. Turkey* [GC], no. 34503/97, §§ 14046, ECHR 2008, for the specific case of civil servants). It also appears from the comparative-law material at the Court's disposal that there is no European consensus on this issue. Few member States have explicitly regulated the question of the exercise by employees of their right to respect for their private life and correspondence in the workplace (see paragraph 52 above).

119. In the light of the above considerations, the Court takes the view that the Contracting States must be granted a wide margin of appreciation in assessing the need to establish a legal framework governing the conditions in which an employer may regulate electronic or other communications of a non-professional nature by its employees in the workplace.

120. Nevertheless, the discretion enjoyed by States in this field cannot be unlimited. The domestic authorities should ensure that the introduction by an employer of measures to monitor correspondence and other communications, irrespective of the extent and duration of such measures, is accompanied by adequate and sufficient safeguards against abuse (see, *mutatis mutandis* , *Klass and Others v. Germany* , 6 September 1978, § 50, Series A no. 28, and *Roman Zakharov* , cited above, §§ 232-34).

121. The Court is aware of the rapid developments in this area. Nevertheless, it considers that proportionality and procedural guarantees against arbitrariness are essential. In this context, the domestic authorities should treat the following factors as relevant:

(*i*) whether the employee has been notified of the possibility that the employer might take measures to monitor correspondence and other communications, and of the implementation of such measures. While in practice employees may be notified in various ways depending on the particular factual circumstances of each case, the Court considers that for the measures to be deemed compatible with the requirements of Article 8 of the Convention, the notification should normally be clear about the nature of the monitoring and be given in advance;

(*ii*) the extent of the monitoring by the employer and the degree of intrusion into the employee's privacy. In this regard, a distinction should be made between monitoring of the flow of communications and of their content. Whether all communications or only part of them have been monitored should also be taken into account, as should the question whether the monitoring was limited in time and the number of people who had access to the results (see *Köpke* , cited above). The same applies to the spatial limits to the monitoring;

(*iii*) whether the employer has provided legitimate reasons

to justify monitoring the communications and accessing their actual content (see paragraphs 38, 43 and 45 above for an overview of international and European law in this area). Since monitoring of the content of communications is by nature a distinctly more invasive method, it requires weightier justification;

(*iv*) whether it would have been possible to establish a monitoring system based on less intrusive methods and measures than directly accessing the content of the employee's communications. In this connection, there should be an assessment in the light of the particular circumstances of each case of whether the aim pursued by the employer could have been achieved without directly accessing the full contents of the employee's communications;

(*v*) the consequences of the monitoring for the employee subjected to it (see, *mutatis mutandis* , the similar criterion applied in the assessment of the proportionality of an interference with the exercise of freedom of expression as protected by Article 10 of the Convention in Axel Springer AG v. Germany [GC], no. 39954/08, § 95, 7 February 2012, with further references); and the use made by the employer of the results of the monitoring operation, in particular whether the results were used to achieve the declared aim of the measure (see *Köpke* , cited above);

(*vi*) whether the employee had been provided with adequate safeguards, especially when the employer's monitoring operations were of an intrusive nature. Such safeguards should in particular ensure that the employer cannot access the actual content of the communications concerned unless the employee has been notified in advance of that eventuality.

In this context, it is worth reiterating that in order to be fruitful, labour relations must be based on mutual trust (see *Palomo Sánchez and Others* , cited above, § 76).

122. Lastly, the domestic authorities should ensure that an employee whose communications have been monitored has access to a remedy before a judicial body with jurisdiction to determine, at least in substance, how the criteria outlined above were observed and whether the impugned measures were lawful (see *Obst* , cited above, § 45, and *Köpke* , cited above).

123. In the present case the Court will assess how the domestic courts to which the applicant applied dealt with his complaint of an infringement by his employer of his right to respect for his private life and correspondence in an employment context.

(c) Application of the above general principles in the present case

124. The Court observes that the domestic courts held that the interests at stake in the present case were, on the one hand, the applicant's right to respect for his private life, and on the other hand, the employer's right to engage in monitoring, including the corresponding disciplinary powers, in order to ensure the smooth running of the company (see paragraphs 28 and 30 above). It considers that, by virtue of the State's positive obligations under Article 8 of the Convention, the national authorities were required to carry out a balancing exercise between these competing interests.

125. The Court observes that the precise subject of the complaint brought before it is the alleged failure of the national courts, in the context of a labour-law dispute, to protect the applicant's right under Article 8 of the Convention to respect for his private life and correspondence in an employment context. Throughout the proceedings the applicant complained in particular, both before the domestic courts and before the Court, about his employer's monitoring of his communications via the Yahoo Messenger accounts in question and the use of their contents in the subsequent disciplinary proceedings against him.

126. As to whether the employer disclosed the contents of the communications to the applicant's colleagues (see paragraph 26 above), the Court observes that this argument is not sufficiently substantiated by the material in the case file and that the applicant did not produce any further evidence at the hearing before the Grand Chamber (see paragraph 91 above).

127. It therefore considers that the complaint before it concerns the applicant's dismissal based on the monitoring carried out by his employer. More specifically, it must ascertain in the present case whether the national authorities performed a balancing exercise, in accordance with the requirements of Article 8 of the Convention, between the applicant's right to respect for his private life and correspondence and the employer's interests. Its task is therefore to determine whether, in the light of all the circumstances of the case, the competent national authorities struck a fair balance between the competing interests at stake when accepting the monitoring measures to which the applicant was subjected (see, *mutatis mutandis* , *Palomo S á nchez and Others* , cited above, § 62). It acknowledges that the employer has a legitimate interest in ensuring the smooth running of the company, and that this can be done by establishing mechanisms for checking that its employees are performing their professional duties adequately and with the necessary diligence.

128. In the light of the above considerations, the Court will first examine the manner in which the domestic courts established the relevant facts in the present case. Both the County Court and the Court of Appeal held that the applicant had had prior notification from his employer (see

paragraphs 28 and 30 above). The Court must then ascertain whether the domestic courts observed the requirements of the Convention when considering the case.

129. At this stage, the Court considers it useful to reiterate that when it comes to establishing the facts, it is sensitive to the subsidiary nature of its task and must be cautious in taking on the role of a first-instance tribunal of fact, where this is not rendered unavoidable by the circumstances of a particular case (see *Mustafa Tunç and Fecire Tunç v. Turkey* [GC], no. 24014/05, § 182, 14 April 2015). Where domestic proceedings have taken place, it is not the Court's task to substitute its own assessment of the facts for that of the domestic courts and it is for the latter to establish the facts on the basis of the evidence before them (see, among other authorities, *Edwards v. the United Kingdom* , 16 December 1992, § 34, Series A no. 247B). Though the Court is not bound by the findings of domestic courts and remains free to make its own assessment in the light of all the material before it, in normal circumstances it requires cogent elements to lead it to depart from the findings of fact reached by the domestic courts (see *Giuliani and Gaggio v. Italy* [GC], no. 23458/02, § 180, ECHR 2011 (extracts), and *Aydan v. Turkey* , no. 16281/10, § 69, 12 March 2013).

130. The evidence produced before the Court indicates that the applicant had been informed of his employer's internal regulations, which prohibited the personal use of company resources (see paragraph 12 above). He had acknowledged the contents of the document in question and had signed a copy of it on 20 December 2006 (see paragraph 14 above). In addition, the employer had sent all employees an information notice dated 26 June 2007 reminding them that personal use of company resources was prohibited and explaining that an employee had been dismissed for breaching this rule (see paragraph 15 above). The applicant acquainted himself with the notice and signed a copy of it on an unspecified date between 3 and 13 July 2007 (see paragraph 16 above). The Court notes lastly that on 13 July 2007 the applicant was twice summoned by his employer to provide explanations as to his personal use of the internet (see paragraphs 18 and 20 above). Initially, after being shown the charts indicating his internet activity and that of his colleagues, he argued that his use of his Yahoo Messenger account had been purely work-related (see paragraphs 18 and 19 above). Subsequently, on being presented fifty minutes later with a forty-five-page transcript of his communications with his brother and fiancée, he informed his employer that in his view it had committed the criminal offence of breaching the secrecy of correspondence (see paragraph 22 above).

131. The Court notes that the domestic courts correctly identified the interests at stake – by referring explicitly to the applicant's right to respect for his private life – and also the applicable legal principles (see paragraphs 28 and 30 above). In particular, the Court of Appeal made express reference to the principles of necessity, purpose specification, transparency, legitimacy, proportionality and security set forth in Directive 95/46/EC, and pointed out that the monitoring of internet use and of electronic communications in the workplace was governed by those principles (see paragraph 30 above). The domestic courts also examined whether the disciplinary proceedings had been conducted in an adversarial manner and whether the applicant had been given the opportunity to put forward his arguments.

132. It remains to be determined how the national authorities took the criteria set out above (see paragraph 121) into account in their reasoning when weighing the applicant's right to respect for his private life and correspondence against the employer's right to engage in monitoring, including the corresponding disciplinary powers, in order to ensure the smooth running of the company.

133. As to whether the applicant had received prior notification from his employer, the Court observes that it has already concluded that he did not appear to have been informed in advance of the extent and nature of his employer's monitoring activities, or of the possibility that the employer might have access to the actual content of his messages (see paragraph 78 above). With regard to the possibility of monitoring, it notes that the County Court simply observed that "the employees' attention had been drawn to the fact that, shortly before the applicant's disciplinary sanction, another employee had been dismissed" (see paragraph 28 above) and that the Court of Appeal found that the applicant had been warned that he should not use company resources for personal purposes (see paragraph 30 above). Accordingly, the domestic courts omitted to determine whether the applicant had been notified in advance of the possibility that the employer might introduce monitoring measures, and of the scope and nature of such measures. The Court considers that to qualify as prior notice, the warning from the employer must be given before the monitoring activities are initiated, especially where they also entail accessing the contents of employees' communications. International and European standards point in this direction, requiring the data subject to be informed before any monitoring activities are carried out (see paragraphs 38 and 43 above; see also, for a comparative-law perspective, paragraph 53 above).

134. As regards the scope of the monitoring and the degree of intrusion into the applicant's privacy, the Court observes that this question was not examined by either the County Court or the Court of Appeal (see paragraphs 28 and 30 above), even though it appears that the employer recorded all the applicant's communications during the monitoring period in real time, accessed them and printed out their contents (see paragraphs 17 and 21 above).

135. Nor does it appear that the domestic courts carried out a sufficient assessment of whether there were legitimate reasons to justify monitoring the applicant's communications. The Court is compelled to observe that the Court of Appeal did not identify what specific aim in the present case could have justified such strict monitoring. Admittedly, this question had been touched upon by the County Court, which had mentioned the need to avoid the company's IT systems being damaged, liability being incurred by the company in the event of illegal activities in cyberspace, and the company's trade secrets being disclosed (see paragraph 28 above). However, in the Court's view, these examples can only be seen as theoretical, since there was no suggestion that the applicant had actually exposed the company to any of those risks. Furthermore, the Court of Appeal did not address this question at all.

136. In addition, neither the County Court nor the Court of Appeal sufficiently examined whether the aim pursued by the employer could have been achieved by less intrusive methods than accessing the actual contents of the applicant's communications.

137. Moreover, neither court considered the seriousness of the consequences of the monitoring and the subsequent disciplinary proceedings. In this respect the Court notes that the applicant had received the most severe disciplinary sanction, namely dismissal.

138. Lastly, the Court observes that the domestic courts did not determine whether, when the employer summoned the applicant to give an explanation for his use of company resources, in particular the internet (see paragraphs 18 and 20 above), it had in fact already accessed the contents of the communications in issue. It notes that the national authorities did not establish at what point during the disciplinary proceedings the employer had accessed the relevant content. In the Court's view, accepting that the content of communications may be accessed at any stage of the disciplinary proceedings runs counter to the principle of transparency (see, to this effect, Recommendation CM/Rec(2015)5, cited in paragraph 43 above; for a comparative-law perspective, see paragraph 54 above).

139. Having regard to the foregoing, the Court finds that the Court of Appeal's conclusion that a fair balance was struck between the interests at stake (see paragraph 30 above) is questionable. Such an assertion appears somewhat formal and theoretical. The Court of Appeal did not explain the specific reasons linked to the particular circumstances of the applicant and his employer that led it to reach that finding.

140. That being so, it appears that the domestic courts failed to determine, in particular, whether the applicant had received prior notice from his employer of the possibility that his communications on Yahoo Messenger might be monitored; nor did they have regard either to the fact that he had not been informed of the nature or the extent of the monitoring, or to the degree of intrusion into his private life and correspondence. In addition, they failed to determine, firstly, the specific reasons justifying the introduction of the monitoring measures; secondly, whether the employer could have used measures entailing less intrusion into the applicant's private life and correspondence; and thirdly, whether the communications might have been accessed without his knowledge (see paragraphs 120 and 121 above).

141. Having regard to all the above considerations, and notwithstanding the respondent State's margin of appreciation, the Court considers that the domestic authorities did not afford adequate protection of the applicant's right to respect for his private life and correspondence and that they consequently failed to strike a fair balance between the interests at stake. There has therefore been a violation of Article 8 of the Convention.

II. APPLICATION OF ARTICLE 41 OF THE CONVENTION

142. Article 41 of the Convention provides:

"If the Court finds that there has been a violation of the Convention or the Protocols thereto, and if the internal law of the High Contracting Party concerned allows only partial reparation to be made, the Court shall, if necessary, afford just satisfaction to the injured party."

A. Damage

1. Pecuniary damage

143. Before the Chamber, the applicant claimed 59,976.12 euros (EUR) in respect of the pecuniary damage he had allegedly sustained. He explained that this amount represented the current value of the wages to which he would have been entitled if he had not been dismissed. At the hearing before the Grand Chamber, the applicant's representatives stated that they maintained their claim for just satisfaction.

144. In their observations before the Chamber, the Government stated that they were opposed to any award in respect of the pecuniary damage alleged to have been sustained. In their submission, the sum claimed was based on mere speculation and there was no link between the applicant's dismissal and the damage alleged.

145. The Court observes that it has found a violation of Article 8 of the Convention in that the national courts failed to establish the relevant facts and to perform an adequate balancing exercise between the applicant's right to respect for his private life and correspondence and the employer's interests. It does not discern any causal link between the violation found and the pecuniary damage alleged, and therefore dismisses this claim.

2. Non-pecuniary damage

146. Before the Chamber, the applicant also claimed EUR 200,000 in respect of the non-pecuniary damage he had allegedly sustained as a result of his dismissal. He stated that because of the disciplinary nature of the dismissal, he had been unable to find another job, that his standard of living had consequently deteriorated, that he had lost his social standing and that as a result, his fiancée had decided in 2010 to end their relationship.

147. The Government submitted in reply that the finding of a violation could in itself constitute sufficient just satisfaction. In any event, they submitted that the sum claimed by the applicant was excessive in the light of the Court's case-law in this area.

148. The Court considers that the finding of a violation constitutes sufficient just satisfaction for any non-pecuniary damage that may have been sustained by the applicant.

B. Costs and expenses

149. Before the Chamber, the applicant also claimed 3,310 Romanian lei (RON) (approximately EUR 750) in respect of the costs and expenses incurred in the domestic courts, and RON 500 (approximately EUR 115) for the fees of the lawyer who had represented him in the domestic proceedings. He claimed a further EUR 500 for the fees of the lawyers who had represented him before the Court. He produced the following in support of his claim:

- copies of the legal-aid agreement and of the receipt for payment of the sum of RON 500, corresponding to his lawyer's fees in the domestic proceedings;

- documents proving that he had paid his employer the sums of RON 2,700 and RON 610.30 in respect of costs and expenses;

- a copy of the receipt for payment of the sum of RON 2,218.64, corresponding to the fees of one of the lawyers who had represented him before the Court.

The applicant did not seek the reimbursement of the expenses incurred in connection with the proceedings before the Grand Chamber.

150. In their observations before the Chamber, the Government requested the Court to award the applicant only those sums that were necessary and corresponded to duly substantiated claims. In that connection, they submitted that the applicant had not proved that he had paid EUR 500 in fees to the lawyers who had represented him before the Court, and that the receipt for payment of a sum of RON 500 in fees to the lawyer who had represented him in the domestic courts had not been accompanied by any supporting documents detailing the hours worked.

151. According to the Court's case-law, an applicant is entitled to the reimbursement of costs and expenses only in so far as it has been shown that these have been actually and necessarily incurred and are reasonable as to quantum (see *Lupeni Greek Catholic Parish and Others v. Romania* [GC], no. 76943/11, § 187, ECHR 2016 (extracts)). In the present case, having regard to the documents in its possession and to its case-law, the Court considers it reasonable to award the applicant the sum of EUR 1,365 covering costs under all heads.

C. Default interest

152. The Court considers it appropriate that the default interest rate should be based on the marginal lending rate of the European Central Bank, to which should be added three percentage points.

FOR THESE REASONS, THE COURT

1. *Holds* , by eleven votes to six, that there has been a violation of Article 8 of the Convention;

2. *Holds* , by sixteen votes to one, that the finding of a violation constitutes in itself sufficient just satisfaction for the non-pecuniary damage sustained by the applicant;

3. *Holds* , by fourteen votes to three,

(a) that the respondent State is to pay the applicant, within three months, EUR 1,365 (one thousand three hundred and sixty-five euros) in respect of costs and expenses, to be converted into the currency of the respondent State at the rate applicable at the date of settlement, plus any tax that may be chargeable to the applicant;

(b) that from the expiry of the above-mentioned three months until settlement simple interest shall be payable on the above amount at a rate equal to the marginal lending rate of the European Central Bank during the default period plus three percentage points;

4. *Dismisses* , unanimously, the remainder of the applicant's claim for just satisfaction.

Done in English and French, and delivered at a public hearing in the Human Rights Building, Strasbourg, on 5 September 2017.

Søren Prebensen
Deputy to the Registrar

Guido Raimondi
President

In accordance with Article 45 § 2 of the Convention and Rule 74 § 2 of the Rules of Court, the following separate opinions are annexed to this judgment:

(a) partly dissenting opinion of Judge Karakaş;

(b) joint dissenting opinion of Judges Raimondi, Dedov, Kjølbro, Mits, Mourou-Vikström and Eicke.

G.R. S.C.P.

PARTLY DISSENTING OPINION OF JUDGE KARAKAŞ

(Translation)

I agree entirely with the majority's finding of a violation of Article 8 of the Convention.

However, I do not share the majority's opinion that the finding of a violation constitutes sufficient just satisfaction for the non-pecuniary damage sustained by the applicant.

It is obvious that under Article 41 the Court decides to award a certain amount in respect of non-pecuniary damage if it considers it "necessary" to afford redress. As it has considerable latitude to determine in which cases such an award should be made to the applicants, the Court sometimes concludes that the finding of a violation constitutes sufficient just satisfaction and that no monetary award is required (see, among many other authorities, *Nikolova v. Bulgaria* , no. 31195/96, § 76, ECHR 1999-II; *Vinter and Others v. the United Kingdom* [GC], nos. 66069/09 and 2 others, ECHR 2013 (extracts); and *Murray v. the Netherlands* [GC], no. 10511/10, ECHR 2016). In order to arrive at that conclusion, the Court will have regard to all the facts of the case, including the nature of the violations found and any special circumstances pertaining to the context of the case (see, for example, *Vinter and Others* , cited above, and the joint partly dissenting opinion of Judges Spielmann, Sajó, Karakaş and Pinto de Albuquerque in the case of *Murray* , cited above). Where this is warranted by the circumstances of the case, as in *McCann and Others v. the United Kingdom* (27 September 1995, § 219, Series A no. 324), in which the Court declined to make any award in respect of nonpecuniary damage in view of the fact that the three terrorist suspects who had been killed had been intending to plant a bomb in Gibraltar, or by the nature of the violation found, as in the case of *Tarakhel v. Switzerland* ([GC], no. 29217/12, ECHR 2014 (extracts)), the Court rules that the finding of a violation in itself affords sufficient just satisfaction for any non-pecuniary damage. In other words, it is only in very exceptional cases that the Court decides not to make any award in respect of non-pecuniary damage.

There may also be instances in which the Court decides to award a lower sum than that awarded in other cases relating to the Article concerned, again taking into consideration the particular features of the context. For example, in *A. and Others v. the United Kingdom* ([GC], no. 3455/05, ECHR 2009), in the context of terrorism, the Court gave detailed reasons (§ 252; see also *Del Río Prada v. Spain* [GC], no. 42750/09, § 145, ECHR 2013) explaining why it had awarded a significantly lower sum than in other previous cases concerning unlawful detention.

In the present case, the domestic courts did not ensure adequate protection of the applicant's right to respect for his private life and correspondence: the applicant was seriously affected by the disciplinary proceedings against him, since he was dismissed from his post.

This violation of Article 8 undoubtedly caused non-pecuniary damage to the applicant, who cannot be satisfied with the mere finding that such damage was sustained. For that reason, I was in favour of granting an award, even of a modest amount, by way of just satisfaction for the non-pecuniary damage sustained by the applicant.

JOINT DISSENTING OPINION OF JUDGES RAIMONDI, DEDOV, KJØLBRO, MITS, MOUROU-VIKSTRÖM AND EICKE

Introduction

1. We agree with the majority, some of us with some hesitation, that, even in a context where on the facts before the Court it is difficult to see how the applicant could have had a "reasonable expectation of privacy" (see below), Article 8 is applicable in the circumstances of this case (see paragraphs 69 to 81 of the judgment). With Article 8 having been found to be applicable, we also agree that this applicant's complaint falls to be examined from the standpoint of the State's positive obligations (see paragraph 111 of the judgment). Subject to what follows, we also agree with the general principles applicable to the assessment of the State's positive obligation, as set out in paragraphs 113 to 122 of the judgment.

2. However, for the reasons set out below, we respectfully disagree with the majority in relation to the correct approach to the State's positive obligation in the context of this case and their ultimate conclusion that the "domestic authorities", by which the majority means only the employment courts, "did not afford adequate protection of the applicant's right to respect for his private life and correspondence and that they consequently failed to strike a fair balance between the interests at stake" (see paragraph 141 of the judgment).

Principle

3. In light of the fact that there is common ground that the present application is to be considered by reference to the State's positive obligation under Article 8, the appropriate starting point is provided by the Court's case-law defining the content and reach of the concept of "positive obligations" under Article 8. The relevant principles were most recently summarised by the Grand Chamber, in the context of the positive obligation to protect the applicant's physical and psychological integrity from other persons, in

Söderman v. Sweden ([GC], no. 5786/08, §§ 78-85, ECHR 2013). There the Court made clear that:

(a) the object of Article 8 is essentially that of protecting the individual against arbitrary interference by the public authorities. However, this provision does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there are positive obligations inherent in an effective respect for private or family 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, *inter alia* , *Airey v. Ireland* , 9 October 1979, § 32, Series A no. 32) (*Söderman* , cited above, § 78);

(b) the choice of the means calculated to secure compliance with Article 8 of the Convention in the sphere of the relations of individuals between themselves is in principle a matter that falls within the Contracting States' margin of appreciation, whether the obligations on the State are positive or negative. There are different ways of ensuring respect for private life and the nature of the State's obligation will depend on the particular aspect of private life that is in issue (see, for example, *Von Hannover v. Germany (no. 2)* [GC], nos. 40660/08 and 60641/08, § 104, ECHR 2012; *Odièvre v. France* [GC], no. 42326/98, § 46, ECHR 2003 III; *Evans v. the United Kingdom* [GC], no. 6339/05, § 77, ECHR 2007 I; and *Mosley v. the United Kingdom* , no. 48009/08, § 109, 10 May 2011) (*Söderman* , cited above, § 79); and

(c) in respect of less serious acts between individuals, which may violate psychological integrity, the obligation of the State under Article 8 to maintain and apply in practice an adequate legal framework affording protection does not always require that an efficient criminal-law provision covering the specific act be in place. The legal framework could also consist of civil-law remedies capable of affording sufficient protection (see, *mutatis mutandis* , *X and Y v. the Netherlands* , 26 March 1985, §§ 24 and 27, Series A no. 91, and *K.U. v. Finland* , no. 2872/02, § 47, ECHR 2008). The Court notes, for example, that in some previous cases concerning the protection of a person's picture against abuse by others, the remedies available in the member States have been of a civil-law nature, possibly combined with procedural remedies such as the granting of an injunction (see, *inter alia* , *Von Hannover* , cited above; *Reklos and Davourlis v. Greece* , no. 1234/05, 15 January 2009; and *Schüssel v. Austria* (dec.), no. 42409/98, 21 February 2002) (*Söderman* , cited above, § 85).

4. The facts of this case, as the majority at least implicitly accepts (see paragraph 80 of the judgment), are, of course, a million miles away from the seriousness of the cases considered in *Söderman* . After all, in that case the Court was concerned with allegations of the violation of a person's physical or psychological integrity by another person.

5. Nevertheless, even in that context, it is clear, firstly, that the choice of measures designed to secure respect for private life under Article 8, even in the sphere of the relations of individuals between themselves, is primarily for the Contracting States; a choice in relation to which they enjoy a wide margin of appreciation (see paragraph 119 of the judgment; narrowing where, unlike in the present case, a particularly important facet of an individual's existence or identity is at stake, or where the activities at stake involve a most intimate aspect of private life). This conclusion is underlined by the fact that there is no European consensus on this matter and only six out of thirty-four surveyed Council of Europe member States have explicitly regulated the issue of the workplace privacy (see paragraphs 52 and 118 of the judgment). Secondly, the "measures" adopted by the State under Article 8 should in principle take the form of an adequate "legal framework" affording protection to the victim. Article 8 does not necessarily require that an efficient criminal-law provision covering the specific act be in place. The legal framework could also consist of civil-law remedies capable of affording sufficient protection.

6. This, of course, applies *mutatis mutandis* in the present case where, as the majority identify, the Court is at best concerned with the protection of a core or minimum level of private life and correspondence in the work place against interference by a private law employer.

The focus of the enquiry

7. Having identified some of the principles set out above, the majority, in paragraph 123, unjustifiably in our view, narrowed its enquiry to the question "how the domestic courts to which the applicant applied dealt with his complaint of an infringement by his employer of his right to respect for private life and correspondence in an employment context".

8. Although recognising that "protective measures are not only to be found in labour law, but also in civil and criminal law" (see paragraph 116 of the judgment), the majority in fact sidelined and avoided the real question that falls to be answered, namely: did the High Contracting Party maintain and apply an adequate "legal framework" providing at least civil-law remedies capable of affording sufficient protection to the applicant?

9. As the respondent Government submitted, and the majority accepts, the relevant "legal framework" in Romania consisted not only of the employment courts, before which the applicant raised his complaint, but also included *inter alia* :

(a) the criminal offence of "breach of secrecy of correspondence" under Article 195 of the Criminal Code (see paragraph 33 of the judgment); incidentally, a remedy

which the applicant engaged by lodging a criminal complaint but, following a decision by the prosecutor that there was no case to answer, failed to exhaust by not challenging that decision in the domestic courts: paragraph 31 of the judgment;

(b) the provisions of Law no. 677/2001 "on the protection of individuals with regard to the processing of personal data and on the free movement of such data" (see paragraph 36 of the judgment), which, in anticipation of Romania's accession to the EU, reproduces certain provisions of 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. This Law expressly provides, in Article 18, for a right to (i) lodge a complaint with the supervisory authority and, in the alternative or subsequently, (ii) apply to the competent courts for protection of the data protection rights safeguarded by the Act, including a right to seek compensation in relation to any damage suffered; and

(c) the provisions of the Civil Code (Articles 998 and 999; paragraph 34 of the judgment) enabling a claim in tort to be brought with a view to obtaining reparation for the damage caused, whether deliberately or through negligence.

10. Other than the criminal complaint which was not pursued any further, none of the domestic remedies was ever engaged by the applicant. Instead, the applicant only applied to the employment courts to challenge not primarily the interference by his employer with his private life/correspondence but his dismissal. As the majority note in paragraph 24:

"He asked the court, firstly, to set aside the dismissal; secondly, to order his employer to pay him the amounts he was owed in respect of wages and any other entitlements and to reinstate him in his post; and thirdly, to order the employer to pay him 100,000 Romanian lei (approximately 30,000 euros) in damages for the harm resulting from the manner of his dismissal, and to reimburse his costs and expenses."

11. It was only in the context of these dismissal proceedings that, relying on the judgment of this Court in *Copland v. the United Kingdom* (no. 62617/00, §§ 43-44, ECHR 2007-I), he argued that the decision to dismiss him was unlawful and that by monitoring his communications and accessing their contents his employer had infringed criminal law.

12. The fact that the applicant's focus was primarily, if not exclusively, on the legality of his dismissal, rather than the interference by his employer with his right to respect for private life/correspondence, is also reflected in the way his case was presented before this Court. As the judgment notes at paragraph 55, the applicant's complaint was that "his dismissal by his employer had been based on a breach of his right to respect for his private life and correspondence and that, by not revoking that measure, the domestic courts had failed to comply with their obligation to protect the right in question".

13. As a consequence, one cannot help but note (if only in passing) that, if the respondent Government had raised this as a preliminary objection, there might have been some question as to whether, by applying to the employment courts on the basis he did, the applicant had, in fact, exhausted those domestic remedies "that relate to the breaches alleged and which are at the same time available and sufficient" (see *Aquilina v. Malta* [GC], no. 25642/94, § 39, ECHR 1999-III). After all, there is no material before the Court to suggest that any of the three remedies identified above, and, in particular, a complaint to the specialist data protection supervisory authority and/or an action for damages under Law no. 677/2001 before the competent courts were "bound to fail" (see *Davydov and Others v. Russia* , no. 75947/11, § 233, 30 May 2017).

14. Our doubts about the effectiveness of the employment courts in this context (and the appropriateness of the Court restricting its analysis to the adequacy of the analysis by those employment courts) is further underlined by the fact that, in line with this Court's jurisprudence under Article 6 of the Convention, regardless of whether or not the employer's actions were illegal that fact could not *per se* undermine the validity of the disciplinary proceedings in the instant case. After all, as this Court confirmed most recently in *Vukota-Bojić v. Switzerland* (no. 61838/10, §§ 94-95, 18 October 2016):

"... the question whether the use as evidence of information obtained in violation of Article 8 rendered a trial as a whole unfair contrary to Article 6 has to be determined with regard to all the circumstances of the case, including respect for the applicant's defence rights and the quality and importance of the evidence in question (compare, *inter alia* , *Khan* , cited above, §§ 35-40; *P.G. and J.H. v. the United Kingdom* , cited above, §§ 77-79; and *Bykov v. Russia* [GC], no. 4378/02, §§ 94-98, 10 March 2009, in which no violation of Article 6 was found).

In particular, it must be examined whether the applicant was given an opportunity to challenge the authenticity of the evidence and to oppose its use. In addition, the quality of the evidence must be taken into consideration, as must the circumstances in which it was obtained and whether these circumstances cast doubts on its reliability or accuracy. Finally, the Court will attach weight to whether the evidence in question was or was not decisive for the outcome of the proceedings (compare, in particular, *Khan* , cited above, §§ 35 and 37)."

15. In any event, the above alternative domestic remedies, some of which are more obviously suitable to the protection

of an individual's private life/correspondence in the private workplace, were plainly relevant to the assessment whether the "legal framework" created by Romania was capable of providing "adequate" protection to the applicant against an unlawful interference with his right to respect for private life/correspondence under Article 8 by another private individual (in this case, his employer).

16. By not including them, sufficiently or at all, in their analysis, the majority failed to have regard to important factors relevant to the question posed by this case and failed to give due weight to the acknowledged wide margin of appreciation enjoyed by High Contracting Parties in determining what measures to take and what remedies to provide for in compliance with their positive obligation under Article 8 to put in place an adequate "legal framework". Absent any evidence to suggest that the domestic remedies either individually or cumulatively were not sufficiently available or effective to provide the protection required under Article 8, it seems to us that there is no basis on which the Court could find a violation of Article 8 in the circumstances of the present case.

17. Before leaving this question of the appropriate focus for the enquiry, we would want to express our sincere hope that the majority judgment should not be read as a blanket requirement under the Convention that, where more appropriate remedies are available within the domestic legal framework (such as e.g. those required to be put in place under the relevant EU data protection legislation), the domestic employment courts, when confronted with a case such as that brought by the applicant, are required to duplicate the functions of any such, more appropriate, specialist remedy.

The analysis by the domestic employment courts

18. However, even if, contrary to the above, the majority's focus only on the analysis by the domestic employment courts were the appropriate approach, we also do not agree that, in fact, that analysis is defective so as to lead to a finding of a violation under Article 8.

19. In considering the judgments of the County Court and the Bucharest Court of Appeal, we note that both domestic courts took into consideration the employer's internal regulations, which prohibited the use of company resources for personal purposes (see paragraphs 12, 28 and 30 of the judgment). We further observe that the applicant had been informed of the internal regulations, since he had acquainted himself with them and signed a copy of them on 20 December 2006 (see paragraph 14 of the judgment). The domestic courts interpreted the provisions of that instrument as implying that it was possible that measures might be taken to monitor communications, an eventuality that was likely to reduce significantly the likelihood of any reasonable expectation on the applicant's part that the privacy of his correspondence would be respected (contrast *Halford v. the United Kingdom* , 25 June 1997, § 45, *Reports of Judgments and Decisions* 1997III, and *Copland* , cited above, § 42). We therefore consider that the question of prior notification should have been examined against this background.

20. In this context, it is clear on the evidence before the Court that the domestic courts did indeed consider this question. Both the County Court and the Court of Appeal attached a certain weight to the information notice which the applicant had signed, and their decisions indicate that a signed copy of the notice was produced in the proceedings before them (see paragraphs 28 and 30 of the judgment). The County Court observed, among other things, that the employer had warned its employees that their activities, including their computer use, were being monitored, and that the applicant himself had acknowledged the information notice (see paragraph 28 of the judgment). The Court of Appeal further confirmed that "personal use [of company resources could] be refused ... in accordance with the provisions of the internal regulations", of which the employees had been duly informed (see paragraph 30 of the judgment). Accordingly, the domestic courts found, on the basis of the documents in their possession, that the applicant had received sufficient warning that his activities, including his use of the computer made available to him by his employer, could be monitored. We can see no basis for departing from their decisions, and consider that the applicant could reasonably have expected his activities to be monitored.

21. Next, we note that the national authorities carried out a careful balancing exercise between the interests at stake, taking into account both the applicant's right to respect for his private life and the employer's right to engage in monitoring, including the corresponding disciplinary powers, in order to ensure the smooth running of the company (see paragraphs 28 and 30 of the judgment; see also, *mutatis mutandis* , *Obst v. Germany* , no. 425/03, § 49, 23 September 2010, and *Fernández Martínez v. Spain* [GC], no. 56030/07, § 151, ECHR 2014 (extracts). The Court of Appeal, in particular, citing the provisions of Directive 95/46/EC, noted that there had been a conflict in the present case between "the employer's right to engage in monitoring and the employees' right to protection of their privacy" (see paragraph 30 of the judgment).

22. We also note that, on the basis of the material in their possession, the domestic courts found that the legitimate aim pursued by the employer in engaging in the monitoring of the applicant's communications had been to exercise "the right and the duty to ensure the smooth running of the company" (see the Court of Appeal as quoted at paragraph 30 of the judgment). While the domestic courts attached greater weight to the employer's right to ensure the smooth running of the company and to supervise how employees performed their tasks in the context of their employment

relationship than to the applicant's right to respect for his private life and correspondence, we consider that it is not unreasonable for an employer to wish to check that its employees are carrying out their professional duties when making use in the workplace and during working hours of the equipment which it has made available to them. The Court of Appeal found that the monitoring of the applicant's communications was the only way for the employer to achieve this legitimate aim, prompting it to conclude that a fair balance had been struck between the need to protect the applicant's private life and the employer's right to supervise the operation of its business (see paragraph 30 of the judgment).

23. In our view, the choice of the national authorities to give the employer's interests precedence over those of the employee is not capable in itself of raising an issue under the Convention (see, *mutatis mutandis* , *Obst* , cited above, § 49). We would reiterate that where they are required to strike a balance between several competing private interests, the authorities enjoy a certain discretion (see *Hämäläinen v. Finland* [GC], no. 37359/09, § 67 in fine, ECHR 2014, and further references). In the present case, therefore, it is our view that the domestic courts acted within Romania's margin of appreciation.

24. We further note that the monitoring to which the applicant was subjected was limited in time, and that the evidence before the Court indicates that the employer only monitored the applicant's electronic communications and internet activity. Indeed, the applicant did not allege that any other aspect of his private life, as enjoyed in a professional context, had been monitored by his employer. Furthermore, on the evidence before the Court, the results of the monitoring operation were used solely for the purposes of the disciplinary proceedings against the applicant and only the persons involved in those proceedings had access to the content of the applicant's communications (for a similar approach see *Köpke v. Germany* (dec.), no. 420/07, 5 October 2010). In this connection, it is observed that the majority agree that the applicant did not substantiate his allegations that the content in question had been disclosed to other colleagues (see paragraph 126 of the judgment).

25. Lastly, we note that in their examination of the case, the national authorities took into account the attitude displayed by the applicant in the course of his professional activities in general, and during the disciplinary proceedings against him in particular. Thus, the County Court found that he had committed a disciplinary offence by breaching his employer's internal regulations, which prohibited the use of computers for personal purposes (see paragraph 28 of the judgment). The domestic authorities attached significant weight in their analysis to the applicant's attitude in the disciplinary proceedings, during which he had denied using his employer's resources for personal purposes and had maintained that he had used them solely for work-related purposes, which was incorrect (see paragraphs 28 and 30 of the judgment). They were plainly entitled to do so. This was confirmed when the applicant asserted before this Court that, despite the fact that he knew that private use of his work computer was prohibited, it would only have been an awareness of monitoring by the employer which would have led him not to engage in private use of the employer's computer; he did not deny that he was informed about the monitoring, but could not remember when he had received the information notice alerting him to the monitoring.

26. After all, as the majority also stress (see paragraph 121 of the judgment), in order to be fruitful, employment relations must be based on mutual trust (see *Palomo Sánchez and Others v. Spain* [GC], nos. 28955/06 and 3 others, § 76, ECHR 2011). Accordingly, it is our view that within their margin of appreciation, the domestic (employment) courts were entitled, when weighing up the interests at stake, to take into account the attitude displayed by the applicant, who had broken the bond of trust with his employer.

27. Having regard to all the foregoing considerations and in contrast to the majority, we conclude that there has been no failure to protect the applicant's right to respect for his private life and correspondence and that there has, therefore, been no violation of Article 8 of the Convention.