Application no. 61496/08
CASE OF BĂRBULESCU v. ROMANIA

Submission
by the
European Trade Union Confederation (ETUC)

under Rule 44(5)

(07/10/2016)

Table of contents

Introduction

1 Referring to the President's decision to grant leave for a third party intervention, the ETUC would like to start its observations by highlighting that it considers this case to be of particular importance for the protection of workers in the digital age, dealing, more specifically, with the very sensitive aspect of the protection of workers' privacy in modern communications systems.

2 Indeed, in its recent Resolution on digitalisation: "Towards fair digital work" the ETUC Executive Committee highlights i.a.:

> The increasing use of new technologies and means of electronic communication in the relation between employers and workers raises many questions concerning workers' privacy and the risks lying in new possibilities of monitoring and surveillance. The ETUC is of the opinion that the use, processing and storage of data in the employment relationship needs principles which avoid infringements of workers' fundamental rights, in particular the right to a private life. This human right is protected under International and European standards. A worker does not give up his or her right to privacy when working.[1]

3 This aspect is becoming crucially important as the normal workplace is more and more characterised not only by the use of computers and the blurring of boundaries between work

[1] Adopted by the Executive Committee on 8-9 June 2016 (https://www.etuc.org/documents/etuc-resolution-digitalisation-towards-fair-digital-work).

and personal use of devices, but also by use of electronic communication. Therefore, employers' and workers' rights have to be balanced in a way which does not undermine workers' privacy. On the contrary, there is an increasing need for the protection of workers' privacy, taking into account their structural dependency in the employment relationship.

4 In relation to the present case the Court, in its Chamber judgment of 12 January 2016, held, by six votes to one, that there has been no violation of Article 8 of the Convention. However, on 3 June 2016 the Grand Chamber Panel accepted the applicant's request that the case be referred to the Grand Chamber.[2]

5 The following observations aim at demonstrating that the approach and findings by the majority in the Chamber Judgment should not be followed. Accordingly, it will mainly follow the line of argumentation as well as the result of the 'Partly Dissenting Opinion of Judge Pinto De Albuquerque' (Dissenting Opinion), but add further information and arguments in this respect.

Relevant international law and material

6 In order to describe the relevant international law and material framework the Chamber judgment refers to Convention No. 108 and to the EU Directive 95/46/EC as well as to Opinions elaborated by the respective Working Party under Article 29 of this Directive (§§ 17 to 22). More extensively, the Dissenting Opinion (in §§ 6 to 8) describes the international and European framework of data protection in general and in the employment relationship in particular. The following references complement those standards in several respects. [3]

United Nations (UN) and International Labour Organisation (ILO)

7 Within the **UN** context the International Covenant on Civil and Political Rights (ICCPR) guarantees the 'Right to privacy' (Article 17 ICCPR). In this respect para. 6 of the Human Rights Committee's General comment[4] states i.a.:

> 'Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited.'

8 Whereas the **ILO** has not yet adopted a legal instrument on the protection of personal data in the employment relationship it did elaborate in 1997 a 'Code of practice on the protection of workers' personal data"[5] dealing i.a. with 'Individual Rights' (11) and 'Collective Rights' (12).

Council of Europe

9 Convention No. 108 on protection of personal data is referred to in the Chamber Judgment (§ 17) whereas the Dissenting Opinion additionally refers to the Committee of Ministers' Recommendation on the processing of personal data in the context of employment (2015)5. The following additional references appear important.

---

[2] See press release ECHR 150 (2016) 03.05.2016.

[3] See also *LÓPEZ RIBALDA v. Spain and GANCEDO GIMÉNEZ and Others v. Spain* (nos. 1874/13 and 8567/13) – Submission by the European Trade Union Confederation (ETUC) under Rule 44(5) (20/07/2015)

[4] General comment No. 16 on Article 17 (Right to privacy) - Thirty second session (1988).

[5] Protection of workers' personal data - An ILO code of practice, 1997.

Convention No. 108 on protection of personal data

10 Besides Articles 2, 3, 5 and 8 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention No. 108)[6] quoted by the Chamber judgment (§ 17), the Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data has elaborated 'Propositions of Modernisation'[7] asking explicitly for 'Transparency of processing':

> '**Article 7bis - Transparency of processing**
> 1 Each Party shall see to it that the controller ensures the transparency of data processing by informing the data subjects, unless they have already been informed, of at least the identity and habitual residence or establishment of the controller, the purposes of the processing carried out, the data processed, the recipients or categories of recipients of the personal data, and the means of exercising the rights set out in Article 8, as well as any other information necessary to ensure fair and lawful data processing.
> 2 …

European Social Charter (ESC)

11 Concerning the Right to Private Life (Article 1§2 ESC) developed by the European Committee of Social Rights, this Committee has elaborated an Interpretative Statement in 2006[8] in which it extended its case-law to the protection of workers with respect to their privacy:

> 'Individuals must be protected from interference in their private or personal lives associated with or arising from their employment situation. Modern electronic communication and data collection techniques have increased the chances of such interference. …'

Handbook on European data protection law (2014)

12 In 2014, the Court, in cooperation with the Fundamental Rights Agency of the European Union (FRA), published a "Handbook on European data protection law" in which information requirements are highlighted. Under the description of the "Rules on transparency of processing" the first of the "Key points" refers to this obligation:

> 'Before starting to process personal data, the controller must, at the very least, inform the data subjects about the identity of the controller and the purpose of the data processing, unless the data subject already has this information.'

13 Under point 4.3.1 the Handbook contains more precise requirements to be fulfilled to be able to qualify the information as sufficient for the purpose of data protection, in particular concerning the content of information and time of providing information. Moreover, the specific issue of 'Employment data' is dealt with under point 8.2.

Committee of Ministers' Recommendation on the processing of personal data in the context of employment (2015)5

14 Recently, the Committee of Ministers has adopted a Recommendation dealing with the specific issue of data protection in the employment relationship[9] (Recommendation (2015)5).

15 In its § 6, the Dissenting Opinion refers mainly to Paragraph 14.1 ('The content, sending and receiving of private electronic communications at work should not be monitored under any

---

[6] CETS No. 108 – 28/01/1981.

[7] 18/12/2012 - T-PD 2012 04 rev4.

[8] CETS No. 35 - 18/10/1961. The same applies to Article 1§2 of the Revised ESC (CETS No. 163 - 03/05/1996).

[9] Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment (Adopted by the Committee of Ministers on 1 April 2015, at the 1224th meeting of the Ministers' Deputies). (It replaces the previous Recommendation (89)2E.)

circumstances'), and paragraph 15.1 ('The introduction and use of information systems and technologies for the direct and principal purpose of monitoring employee's activity and behaviour should not be permitted.'). However, further elements should be taken into account, in particular Principle 21 providing for additional safeguards:

> *'**21. Additional safeguards***
>
> For all particular forms of processing, set out in Part II of the present recommendation, employers should ensure the respect of the following safeguards in particular:
>
> a. inform employees before the introduction of information systems and technologies enabling the monitoring of their activities. The information provided should be kept up to date and should take into account principle 10 of the present recommendation. The information should include the purpose of the operation, the preservation or back-up period, as well as the existence or not of the rights of access and rectification and how those rights may be exercised;
>
> b. take appropriate internal measures relating to the processing of that data and notify employees in advance;
>
> c. consult employees' representatives in accordance with domestic law or practice, before any monitoring system can be introduced or in circumstances where such monitoring may change. Where the consultation procedure reveals a possibility of infringement of employees' right to respect for privacy and human dignity, the agreement of employees' representatives should be obtained; …'

European Union

16 At the level of the European Union the protection of personal data has achieved great importance in primary and secondary legislation. This is supplemented by the respective jurisprudence of the Court of Justice of the European Union (CJEU).

Primary law

17 According to Article 6(1)(1) of the Treaty of the European Union (TEU) the **Charter of Fundamental Rights of the European Union** (CFREU) has 'the same legal value as the Treaties'. Concerning the respect for private life and protection of personal data the relevant provisions (only briefly mentioned in the Dissenting Opinion, § 7) state:

> *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.

18 Moreover, Article 16(1) of the **Treaty on the Functioning of the European Union** (TFEU) provides that everyone has the right to the protection of personal data concerning him or her.

Secondary legislation

19 In its § 18, the Chamber Judgment briefly refers to Articles 2(1) and 8(1) of the **Data Protection Directive** (95/46).[10]

20 Under Article 2 of Directive 95/46:

> '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 one or more factors specific to his physical … identity;
>
> (b) "processing of personal data" ("processing") shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction; …
>
> (d) "controller" shall mean the natural … person … which alone or jointly with others determines the purposes and means of the processing of personal data ...
>
> (h) 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.'

21 Article 3(1) of that Directive provides:

> '1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.'

22 Article 7 of Directive 95/46 is worded as follows:

> 'Member States shall provide that personal data may be processed only if:
>
> (a) the data subject has unambiguously given his consent; 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).'

23 Article 11(1) of Directive 95/46 provides:

> '1. Where the data have not been obtained from the data subject, Member States shall provide that the controller … must at the time of undertaking the recording of personal data … provide the data subject with at least the following information, except where he already has it:
>
> (a) the identity of the controller ...;
>
> (b) the purposes of the processing;
>
> (c) any further information such as
>
> – the categories of data concerned,
>
> – the recipients or categories of recipients,
>
> – the existence of the right of access to and the right to rectify the data concerning him

[10] Directive 95/46/EC of the European Parliament and of the Council of 24/10/1995 Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data - *OJ L 1995, 281 p. 31.* In its § 6, the Dissenting Opinion highlights several further relevant legislative acts (Regulation, Directives).

insofar as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.'

24 The **General Data Protection Regulation (GDPR)**[11] entered into force on 24 May 2016 and shall apply from 25 May 2018[12] thus repealing Directive 95/46.

25 The protection of sensitive data related to the employment relationship was very much discussed. The solution found was that the protection provided generally by the GSPR also applies. Recognising the specific sensitivity of the employment relationship the Member States can, nevertheless, improve this level of protection:

> 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. …

Article 8 of the Convention

General principles

26 Two main elements have to be taken into account. The first relates to the newly developed concept of internet access as a human right. Secondly and more specifically, the term 'correspondence' in Article 8(1) of the Convention requires a specific approach in the digital age.

27 Based on the '**Access to the Internet as a human right**' (§ 3) the Dissenting Opinion draws i.a. the following conclusions (§§ 9 and 11) which are further strengthened by the references mentioned above:

> From this international legal framework, a consolidated, coherent set of principles can be drawn for the creation, implementation and enforcement of an Internet usage policy in the framework of an employment relationship. Any information related to an identified or identifiable employee that is collected, held or used by the employer for employment purposes, including with regard to private electronic communications, must be protected in order to respect the employee's right to privacy and freedom of expression. Consequently, any processing of personal data for the purposes of recruitment, fulfilment or breach of contractual obligations, staff management, work planning and organisation and termination of an employment relationship in both the public and private sectors must be regulated either by law, collective agreement or contract. …
>
> A blanket ban on personal use of the Internet by employees is inadmissible, as is any policy of blanket, automatic, continuous monitoring of Internet usage by employees. Personal data

[11] Regulation (EU) 2016/679 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), OJ 2016, L 119, p. 1 (http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf)

[12] http://ec.europa.eu/justice/data-protection/reform/index_en.htm

relating to racial origin, political opinions or religious or other beliefs, as well as personal data concerning health, sexual life or criminal convictions are considered as "sensitive data" requiring special protection.[13]

28 Apart from these considerations, it appears important to go back to the wording of Article 8 of the Convention itself. It is important to acknowledge the specific character of the term '**correspondence**' in Article 8(1) of the Convention. According to the Court's case law, this is part of the 'private life' also guaranteed under this provision. However, it appears that the Court is not attributing sufficient value to the fact that this notion of communication is expressly mentioned separately. Beyond the level of protection guaranteed by the (general) right to respect for private life, the right to private correspondence requires additional protection. Taking into account the (digital) development of correspondence, email communications must be specifically protected – also at the workplace.

29 An example may illustrate the consequences: Comparing the present case with a case in which a worker would use - admittedly in breach of his obligations - an envelope and a stamp both taken from his office in the employer's premises in order to send a private letter to a private person. Would the employer be permitted to open the letter to see whether it is of private character without asking for the respective consent or even without informing him prior to the search? The answer would have to be negative. The same should apply to the e-mail correspondence.

Procedural safeguards

30 The protection of privacy in general and in the employment relation in particular is a relatively new element in international human rights protection. The risks for privacy deriving from new technologies are increasing. International and in particular European Human Rights protection have developed in the sense that, irrespective of the question of permitted processing of personal data as such, the person(s) concerned have to be informed and, in principle, need to have given their consent. Moreover, the employment relationship requires information (and consultation) of the workers' representatives.

Right of the worker to give their consent or at least to be informed

31 The right to information of the data subject (i.e. the worker) by the controller (i.e. the employer) represents a basic principle and a minimum procedural protection at the same time.

32 Moreover, several European instruments and materials address the protection of privacy, be it in the general form for protection of personal data or in the more specific issue of video surveillance at the workplace. For interpretation purposes, it will be recalled that the Grand Chamber has specifically drawn attention to the importance of international law in the interpretation of the European Convention on Human Rights (Convention):

> The Court, in defining the meaning of terms and notions in the text of the Convention, **can and must** take into account elements of international law other than the Convention, the interpretation of such elements by competent organs, and the practice of European States reflecting their common values.[14] (Emphasis added)

33 At EU level besides the fundamental rights on protection of family life (Article 7 CFREU) and on protection of personal data (Article 8 CFREU, see above para. 17) in primary law, the secondary legislation in the Directive 96/45, see above paras. 19 - 23 refers explicitly to the principle of prior information of the data subject (here the worker) by the controller (here the employer) on the processing of personal data. In its Chapter II Section IV (Information to be

[13] In the view of the ETUC trade union membership and activities should be protected in the same way.

[14] ECtHR 12 November 2008 - no. 34503/97 - *DEMIR AND BAYKARA v. TURKEY*, [2008] ECHR 1345, § 85.

given to the data subject) Article 11 sets out the minimum requirements for the information to make the processing of personal data permissible (see above para. 23).

34 At the level of the Council of Europe, Article 8(a) Convention No. 108 (adopted as early as in 1981[15]) can be considered as the nucleus of the principle of prior information. However, recent developments show more recognition of this right in the context of Convention No. 108. Indeed, the propositions for modernisation contain a new Art. 7bis on "Transparency of processing" requiring again the 'data subjects' (i.e. the worker) to be informed (see above para. 10). Combining EU and CoE law (mainly the ECHR) the Handbook on European data protection law (see above para. 12) refers as a key point to the principle that before starting to process personal data, the controller must, at the very least, inform the data subjects. Most recently and specifically, the Employment Relation Recommendation (2015)5 on the processing of personal data in the context of employment of 1 April 2015 provided for the principle of transparency in general (Principle 10) and highlighted the need for information to be conveyed to the workers as well as to the workers' representatives (Principle 21: Additional safeguards, see above para. 15).

35 In conclusion, the right of the data subject to be informed before the processing of personal data is to be considered as a right derived from Article 8 ECHR as a procedural safeguard.

36 This conclusion is enhanced by a further right, i.a. the principle of prior consent before data processing. In particular Article 7(a) of Directive 95/46 (see above para. 21) requires that 'the data subject has unambiguously given his consent'.[16] Indeed, the right to consent requires prior information.

37 In conclusion and in the words of the Dissenting Opinion (§ 12):

> Employees must be made aware of the existence of an Internet usage policy in force in their workplace, as well as outside the workplace and during out-of-work hours, involving communication facilities owned by the employer, the employee or third parties. All employees should be notified personally of the said policy and consent to it explicitly. Before a monitoring policy is put in place, employees must be aware of the purposes, scope, technical means and time schedule of such monitoring. Furthermore, employees must have the right to be regularly notified of the personal data held about them and the processing of that personal data, the right to access all their personal data, the right to examine and obtain a copy of any records of their own personal data and the right to demand that incorrect or incomplete personal data and personal data collected or processed inconsistently with corporation policy be deleted or rectified. In event of alleged breaches of Internet usage policy by employees, opportunity should be given to them to respond to such claims in a fair procedure, with judicial oversight.

Rights of the workers' representatives to be informed

38 In the present case the question of the involvement of workers' representatives was not mentioned and is therefore not directly relevant. However, the developments in this respect show that normally, individual protection is often seen as insufficient and thus requiring additional procedural protection by workers' representatives.

39 In cases such as the present workers representatives would have to be seen as the ultimate procedural safeguard in order to ensure that the rights and interests of the workers concerned are not violated. Such a right has been developed in recent times in different international material:

40 Generally, several international instruments contain the right to information and consultation of workers' representatives. Besides Convention No. 135 (Workers' Representatives Convention, 1971) the ILO has guaranteed information and consultation rights on specific

[15] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28/01/1981.

[16] Article 7 of Directive 95/46 contains several further grounds of permissible data processing.

issues such as safety and health. More generally, Article 21 of the Revised ESC (The right to information and consultation) and EU Directive 2002/14 on information and consultation.[17]

41 In particular, Principle 21 "Additional safeguards" of the Committee of Ministers' Recommendation Rec (2015)5 (see above para. 15) requires that employers, for all particular forms of processing set out in Part II of this recommendation, should ensure the respect of the safeguards in particular:

> 'c. consult employees' representatives in accordance with domestic law or practice, before any monitoring system can be introduced or in circumstances where such monitoring may change. Where the consultation procedure reveals a possibility of infringement of employees' right to respect for privacy and human dignity, the agreement of employees' representatives should be obtained;'

As consultation requires prior information, this provision strengthens the interpretation of Article 8 ECHR in the sense of additional procedural safeguards at collective level.

42 In conclusion, the ETUC is of the opinion that in cases in which protection by workers' representatives is not available (as in the present case), the need for effective individual protection is even more necessary.

Proportionality requirements

43 Even assuming that the rights derived from Article 8 of the Convention have been prescribed by law and that legitimate aims justify the interference, the sanctions for the breach of the applicant's obligations appear unjustified because they are not proportionate. The Dissenting Opinion (§14) rightly refers to the following proportionality requirements:

> Breaches of the internal usage policy expose both the employer and the employee to sanctions. Penalties for an employee's improper Internet usage should start with a verbal warning, and increase gradually to a written reprimand, a financial penalty, demotion and, for serious repeat offenders, termination of employment. If the employer's Internet monitoring breaches the internal data protection policy or the relevant law or collective agreement, it may entitle the employee to terminate his or her employment and claim constructive dismissal, in addition to pecuniary and non-pecuniary damages.

44 These requirements have not been followed in the present case. The dismissal has not been preceded by other stages of sanctioning the breaches.

Conclusions

45 For the ETUC, it appears worth bearing in mind the following considerations, as expressed in § 15 of the Dissenting Opinion, when deciding on this case:

> Ultimately, without such a policy, Internet surveillance in the workplace runs the risk of being abused by employers acting as a distrustful Big Brother lurking over the shoulders of their employees, as though the latter had sold not only their labour, but also their personal lives to employers. In order to avoid such commodification of the worker, employers are responsible for putting in place and implementing consistently a policy on Internet use along the lines set out above. In so doing, they will be acting in accordance with the principled international-law approach to Internet freedom as a human right.

46 Basing its judgment on the preceding principles the Grand Chamber should make an important step in the direction of better protection of workers in the digital age and hold that Article 8 of the Convention was violated in the present case.

[17] Directive 2002/14/EC of the European Parliament and of the Council of 11 March 2002 establishing a general framework for informing and consulting employees in the European Community, *OJ L 80, 2002, p. 29*.