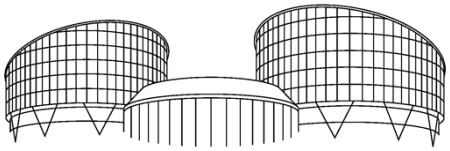

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

FIFTH SECTION

CASE OF LIBERT v. FRANCE

(Application no. 588/13)

JUDGMENT

STRASBOURG

22 February 2018

FINAL

02/07/2018

This judgment has become final under Article 44 § 2 of the Convention. It may be subject to editorial revision.

In the case of Libert v. France,

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

Angelika Nußberger, *President,*
Erik Møse,
André Potocki,
Yonko Grozev,
Síofra O'Leary,
Mārtiņš Mits,
Gabriele Kucsko-Stadlmayer, *judges,*
and Claudia Westerdiek, *Section Registrar,*

Having deliberated in private on 12 December 2017 and on 30 January 2018,

Delivers the following judgment, which was adopted on the last-mentioned date:

PROCEDURE

1. The case originated in an application (no. 588/13) against the French Republic lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by a French national, Mr Eric Libert ("the applicant"), on 27 December 2012.

2. The applicant was represented by Mr Pascal Bibard, a lawyer practising in Amiens. The French Government ("the Government") were represented by their Agent, Mr François Alabrune, Director of Legal Affairs, Ministry of Foreign Affairs.

3. The applicant alleged, in particular, that there had been a violation of Article 8 of the Convention on account of his employer having opened files on the hard disk of his work computer without his being present.

4. On 30 March 2015 the application was communicated to the Government.

5. On 28 June 2016 the Chamber decided to adjourn examination of the case until delivery of the decision or judgment in the Grand Chamber case of *Bărbulescu v. Romania* [GC]. The *Bărbulescu v. Romania* judgment ([GC], no. 61496/08) was delivered on 5 September 2017.

THE FACTS

I. THE CIRCUMSTANCES OF THE CASE

6. The applicant was born in 1958 and lives in Louvencourt.

7. He was hired in 1976 by the French national railway company (*Société nationale des chemins de fer – "the SNCF"*), where he last worked as Deputy Head of the Amiens Regional Surveillance Unit. He stated that in 2007 he had complained to senior management about the conduct of one of his subordinates, who, he alleged, had used extreme language when addressing a colleague. The employee in question had then filed a complaint against him, following which the applicant had been charged with making false accusations. The applicant had subsequently been suspended from duty by the SNCF on grounds of that charge.

8. The proceedings were discontinued a few months later, whereupon the applicant notified his employers of his wish to be reinstated in his former post. He received a reply inviting him to consider appointment to another post, but maintained his original request.

9. On the day of his reinstatement, on 17 March 2008, the applicant found that his work computer had been seized. After being summoned by his superiors, he was informed on 5 April 2008 that the hard disk on the computer had been analysed and that "address change certificates drawn up for third persons and bearing the Lille General Security Service logo" had been found, as well as a large number of files containing pornographic images and films. It can be seen from the judgment of the Amiens Court of Appeal of 15 December 2010 (see paragraphs 14-15 below) that the person who had replaced the applicant during his suspension from post had found "documents which had caught his attention" on the computer, and that he had alerted his superiors in March 2007 and January 2008.

10. A request for a written explanation was sent to the applicant on 7 May 2008. He replied that in 2006, following problems with his personal computer, he had transferred the contents of one of his USB keys to his work computer. He added that the files containing pornographic material had been sent to him by people he did not know, via the SNCF's Intranet.

11. The applicant was summoned to a disciplinary hearing, which took place on 21 May 2008. On 9 June 2008 he was informed by the "resources management director" of Amiens head office that a proposal had been made to dismiss him from the service and that he would be summoned to appear before the disciplinary board. The board convened on 15 July 2008.

12. On 17 July 2008 the SNCF regional director decided to dismiss the applicant from the service. His decision was worded as follows:

> " ... the analysis of the files stored on the hard disk of [the applicant's] work computer, used for his professional duties, contained the following:

i) change of address certificate, signed in his name, certifying the transfer on 01/11/2003 of Ms Catherine [T.] to the Lille General Security Service; the original certificate, sent to ICF North-East enabled the notice period for vacating her flat to be shortened;

ii) change of address certificate, bearing the Ministry of Justice logo, in the name of M. [S.-J.], governor of Fresnes Prison, certifying the transfer of M. [P.] Frédéric to Strasbourg Prison, from 1 November 2006;

iii) draft documents drawn up in the name of Michel [V.], director of the SOCRIF, certifying his financial situation with regard to that company;

iv) a very large number of files containing pornographic images and films (zoophilia and scatophilia).

These facts are in breach of the special obligation of exemplary conduct inherent in the duties formerly performed by him within the General Security Service, and of the following provisions:

i) Article 5.2 of the RH 0006 on the principles governing the conduct of SNCF officials;

ii) the general security database RG 0029 (information systems security policy – user's charter);

iii) the RA 0024 "code of professional conduct" - conduct to be observed with regard to the company's information system;

iv) Article 441-1 of the Criminal Code."

13. On 28 October 2008 the applicant brought proceedings before the Amiens Industrial Tribunal (*conseil des prud'hommes*) seeking a ruling that he had been dismissed without genuine or serious cause. On 10 May 2010 the Industrial Tribunal held that the decision dismissing the applicant from the service had been justified and, accordingly, rejected his claims.

14. On 15 December 2010 the Amiens Court of Appeal upheld the substance of that judgment. It held, in particular, as follows:

" ... [The applicant] submitted that the SNCF had infringed his private life by opening, in his absence, files identified as personal in his computer.

As a matter of policy, documents kept by employees in the company's office, save those identified by them as personal, are presumed to be for professional use, meaning that the employer can have access to them in the employee's absence.

It can be seen from the report drawn up by the SEF that the pornographic photos and videos were found in a file called "fun" stored on a hard disk labelled "D:/personal data".

The SNCF explained, without being challenged, that the "D" drive was called "D:/data" by default and was traditionally used by staff to store their work documents.

An employee cannot use an entire hard disk, which is supposed to record professional data, for his or her private use. The SNCF were therefore entitled to consider that the description "personal data" appearing on the hard disk could not validly prohibit their access to it. In any event, the generic term "personal data" could have referred to work files being personally processed by the employee and did not therefore explicitly designate elements relating to his private life. That had been the

case here, moreover, since the analysis of the hard disk yielded numerous work documents ("LGV photos" file, "warehouse photos" ... .

The term "fun", moreover, does not clearly convey that the file in question is necessarily private. The term can denote exchanges between colleagues at work or work documents kept as "bloopers" by the employee. The employer also rightly pointed out that the user's charter provided that "private information [had to] be clearly identified as such ("private" option in the Outlook criteria)" and that the same was true of the media receiving that information ("private" folder). The lower court was therefore correct in considering that the file had not been identified as personal.

The same applies to the files containing the impugned certificates registered under the names "Fred [P.]", "SOCRIF" and "Catherine"."

15. The Court of Appeal also held that the applicant's dismissal from the service had not been disproportionate. It observed that both the SNCF's Code of Professional Conduct and the internal rules provided that staff were required to use the computers provided to them for exclusively professional ends, with the occasional private use being merely tolerated. It found that the applicant had committed a "massive breach of those rules, going as far as using his work tools to produce a forged document". In the court's view, those acts had been particularly serious because, as an official responsible for general surveillance, he would have been expected to be of exemplary conduct.

16. The applicant appealed on points of law. He submitted, in particular, that there had been a violation of Article 8 of the Convention. The Social Division of the Court of Cassation dismissed the appeal in a judgment of 4 July 2012. It held as follows:

" ... whilst files created by an employee with the assistance of the computer facilities supplied to him by his employer for work purposes are presumed to be professional in nature, meaning that the employer is entitled to open them in the employee's absence, unless they are identified as personal, the description given to the hard disk itself cannot confer privacy on all the data contained in it. The Court of Appeal, which found that labelling the hard disk in the employee's computer "D:/ personal data" could not enable him to use it for purely private purposes and prohibit access by the employer, drew the legitimate conclusion that the files in question, which had not been identified as "private" according to the recommendations of the IT charter, could be lawfully opened by the employer.

The Court of Appeal, which found that the employee had stored 1,562 pornographic files representing a volume of 787 megabytes over a period of four years, and that he had also used his work computer to produce forged certificates, rightly held that such misuse of his office equipment in breach of the rules in force at the SNCF amounted to a breach of his contractual obligations. ...".

...

II. RELEVANT DOMESTIC LAW AND PRACTICE

17. Articles L. 1121-1 and L. 1321-3 of the Labour Code read as follows:

Article L. 1121-1

"No one shall restrict the rights of persons or individual and collective liberties in a manner that is neither justified by the nature of the task to be performed nor proportionate to the aim pursued."

Article L. 1321-3

The internal rules shall not contain: ... 2. Provisions restricting the rights of persons or individual and collective liberties in a manner that is neither justified by the nature of the task to be performed nor proportionate to the aim pursued ... ."

18. In a judgment of 2 October 2001, the Social Division of the Court of Cassation held that employees were entitled, even during working time and at the workplace, to respect for their privacy, which included in particular confidentiality of communications. It concluded, accordingly, that an employer could not read personal messages sent or received by an employee via computer facilities made available to him or her for work purposes, even where the employer had prohibited use of the computer for non-professional purposes (*Bulletin* 2001 V No. 291, p. 233). In a judgment of 17 May 2005, it specified that, "save in a case of serious risk or in exceptional circumstances, an employer c[ould] only open files identified by an employee as personal and stored on the hard disk of his or her work computer in the employee's presence or after he or she had been duly called" (*Bulletin* 2005 V No. 165, p. 143). In a judgment of 18 October 2006, it added that folders and files created by an employee using the computer facilities supplied by his or her employer for work purposes were presumed to be professional documents unless the employee had identified them as personal, and the employer could therefore have access to them in the employee's absence (*Bulletin* 2006 V No. 308, p. 294).

III. USER'S CHARTER REGARDING USE OF THE SNCF'S INFORMATION SYSTEM

19. The user's charter regarding use of the SNCF's information system contains the following provisions:

" ... Access to resources

The resources provided by the SNCF's information system shall be used exclusively for the staff's professional activities, as defined by their job description and within the limits of the tasks assigned to them. Occasional and reasonable use of the electronic mail system and Internet for personal purposes shall nonetheless be tolerated in order to assist practical or family needs provided that this is not liable to affect the quality of the associated service. Private information must be clearly identified as such (*inter alia* "private" option in the Outlook criteria). The same applies to the media receiving this information ("Private" folder). Such use is authorised on a strictly personal basis and cannot in any way be transferred, even temporarily, to a third party without engaging the responsibility of the postholder. Authorisation can be revoked at any

time and shall cease in the event of temporary or definitive suspension of the professional activity justifying it. ...”

THE LAW

I. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

20. The applicant complained of a violation of his right to respect for his private life on the grounds that his employer had opened, in his absence, personal files stored on the hard disk of his work computer. He relied on Article 8 of the Convention, which reads as follows:

“1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”

A. Admissibility

21. The Government submitted that Article 8 of the Convention was inapplicable on the grounds that at the material time or at the time of introduction of the application the SNCF could not be regarded as a public authority within the meaning of the second paragraph of Article 8 and that there had been no interference with the exercise of the applicant’s right to respect for his private life within the meaning of that provision.

22. The question whether or not there had been an “interference by a public authority with the exercise of this right” within the meaning of the second paragraph of Article 8 is distinct, however, from that of the applicability of that provision, as it concerns the merits of the case; the Court will accordingly analyse it in the context of its examination of the complaint on the merits (see paragraphs 37-41 below).

23. That having been established, the Court nonetheless considers it relevant to rule on the applicability of Article 8 in the present case. It observes in this connection that it has previously had the opportunity to rule that telephone calls for non-professional purposes from the workplace could fall within the concepts of “private life” and “correspondence”, within the meaning of Article 8 § 1 of the Convention (see *Halford v. the United Kingdom*, 25 June 1997, §§ 44-46, *Reports of Judgments and Decisions* 1997-III; see also *Amann v. Switzerland* [GC], no. 27798/95, § 44, ECHR 2000-II). In the case of *Halford*, the Court specified that the applicant could have had a reasonable expectation of privacy for such calls, which

expectation was reinforced by the fact that as Assistant Chief Constable she had sole use of her office, where there were two telephones, one of which was specifically designated for her private use. Furthermore, she had been given the assurance, in response to a memorandum she had sent, that she could use her office telephones for the purposes of her sex-discrimination case.

24. Emails sent from the workplace, information derived from the monitoring of personal Internet usage at the workplace (see *Copland v. the United Kingdom,* no. 62617/00, § 41, ECHR 2007-I), and electronic data consisting of emails or computer records (see, *mutatis mutandis*, *Vinci Construction and GTM Génie Civil and Services v. France,* nos. 63629/10 and 60567/10, §§ 69-70, 2 April 2015; the circumstances of that case were different, however, from those of the present case as it concerned companies complaining, in substance, about the search and seizure of electronic data consisting of computer records and emails from a number of their employees, containing, *inter alia*, messages covered by lawyer-client privilege) can also attract the protection of Article 8.

25. The Court can therefore accept that in some circumstances non-professional data, for example data clearly identified as being private and stored by an employee on a computer supplied to him by his employer for professional use, may be deemed to relate to his "private life". In the instant case, as observed in the judgment given on 15 December 2010 by the Amiens Court of Appeal in the applicant's case, the SNCF tolerates the occasional use of work computer facilities by staff for their private use, while specifying the rules to be followed in that regard (see, *mutatis mutandis*, *Bărbulescu*, cited above, § 80).

26. That being said, the Court notes that this complaint is not manifestly ill-founded within the meaning of Article 35 § 3 (a) of the Convention and that it is not inadmissible on any other grounds. It therefore declares it admissible.

B. Merits

1. The parties' submissions

a) The applicant

27. On the question of whether there had been an "interference by a public authority", within the meaning of Article 8 § 2 of the Convention, the applicant submitted at the outset that the SNCF was a group composed of three public bodies of an industrial and commercial nature (*établissement public à caractère industriel et commercial – "EPIC"*). He observed that the description "public body" already indicated that it was a public authority, and added that the three EPIC in question were fully State owned, that the most senior officials of the SNCF were appointed directly by the

Government, and that the SNCF was under State supervision through the General Directorate of Infrastructures, Transport and the Sea of the Ministry of Ecology, Sustainable Development and Energy.

28. The applicant admitted having used his work computer for personal ends, but denied having personalised the entire contents of the hard disk, submitting that he had labelled only part of the contents "D:/personal data". He added that the volume of documents in question was not such as to support a presumption that they were work related as he had taken care to divide the storage space of his hard disk into two parts, only one of which was labelled "D:/personal data". He pointed out that his employer had consulted a file labelled "fun" whereas there was no doubt that this term denoted a non-professional content.

29. The applicant then submitted that the interference of which he complained had not been in accordance with the law, observing, among other things, that Articles L. 1121-1 and L. 1321-3 of the Labour Code, to which the Government referred, were limited to indicating in general terms that such a measure was possible if it was justified by the nature of the task to be performed and proportionate to the aim pursued.

30. The applicant submitted, further, that the measure of which he complained had not been carried out in pursuit of a legitimate aim. In his view, the need to give the employer the possibility of monitoring execution of the employees' work and satisfying themselves that they were adhering to the rules was an irrelevant consideration in his case because his computer had been seized and the contents searched at a time when he had been absent for more than a year and the computer had not therefore been used for a long time. Nor could his employer rely on the need to prevent crime, as the possession of erotic, pornographic or humorous images was not contrary to French law. He submitted, further, that such grounds presupposed the prior existence of a suspicion, whereas his employer could not have been aware of the contents of the files in question until after he had opened them. He challenged the Government's assertion that the existence of the files had been disclosed to his employer by the employee who had been replacing him, as that employee had not been using his computer but other computer facilities. He alleged that his employer had in truth sought a pretext to get rid of a very long-standing management employee cheaply.

31. The applicant submitted that he had suffered a material infringement of his right to respect for his private life. In his view, that infringement could not be regarded as proportionate if the employee did not have the benefit of substantive and formal guarantees. French positive law failed to provide such guarantees.

b) The Government

32. The Government submitted that there had not been an "interference", within the meaning of Article 8 § 2 of the Convention, with the applicant's

right to respect for his private life because he had not properly identified the files opened by his superiors as private. They added that even if there had been an interference, it had not been by a "public authority", within the meaning of that provision, because the SNCF was an EPIC whose employees were subject to private law, the non-regulatory decisions taken in their regard were acts subject to private law and employer-employee disputes fell within the jurisdiction of the ordinary courts.

33. In the alternative, the Government submitted that the interference had been in accordance with the law (Articles L. 1121-1 and L. 1321-3 of the Labour Code, supplemented by the case-law of the Court of Cassation), pursued legitimate aims and been necessary in a democratic society.

34. With regard to the aims pursued, the Government submitted, first, that the interference in question had sought to guarantee the protection of the "rights and freedoms of others": those of the employer, who should be able to monitor execution of the employees' work, satisfy itself that they adhered to the applicable rules, protect the company's electronic networks and prevent risks related to the unauthorised use of work computers. Secondly, they referred to the "prevention of crime", pointing out in that respect that the applicant had been suspended from duty at the beginning of 2007 on account of the criminal charge against him and that it was following the discovery of suspicious documents on his computer by the employee temporarily replacing him that his employer had carried out fuller investigations.

35. The Government then pointed out that the Court had held, in *Copland* (cited above), that it would not exclude that the monitoring of an employee's telephone, email or Internet usage at the workplace may be considered "necessary in a democratic society" in certain situations in pursuit of a legitimate aim. They pointed to the margin of appreciation available to States in the area of labour relations, where two competing private interests had to be weighed up, and the protection offered by French positive law to the effect that the employer could not consult and open, in the absence of the employee concerned, files and folders identified as personal. They submitted, however, that under the employment contract and the relationship of subordination deriving from it, employers were entitled to expect employees to carry out the tasks assigned to them. They specified that the Court of Cassation had thus held – in particular – that employers could find that employees had breached their contractual obligations by misusing computer facilities for private purposes (Cass. Soc. 16 May 2007, no. 05-46.455) or immoral purposes liable to harm the company's interests (Cass. Soc. 2 June 2004, no. 03-45.269). In their submission, as the applicant had been attached to the department responsible for rail safety, his employer had to be able to access the work documents contained in his work computer. As the applicant had put his entire hard disk in the file marked "personal data", his employer had had no alternative but to access

that file. The SNCF had had a duty to investigate because it had been informed by the employee replacing the applicant of the presence "of [the] files in question" on the hard disk of his computer.

36. The Government observed that the SNCF's Code of Professional Conduct and the internal rules stipulated that staff must use the company's computer facilities exclusively for work purposes, and that their use for private purposes was authorised only exceptionally, occasionally and reasonably, and in the context of everyday and family life; any use resulting in substantial use of storage space and any access to sites whose content infringed public order, dignity of persons or morals was proscribed. They concluded that the applicant could not have been unaware that the storage of 1,562 pornographic files corresponding to 787 megabytes on his hard disk over a period of four years was liable to contravene the user's charter, the Professional Code of Conduct and the SNCF's internal rules. Adding that the presence of those files "could have caused problems for the employer, who could subsequently have been sued for passive collusion", the Government concluded that the measure complained of had been fully justified and proportionate.

2. The Court's assessment

a) Whether there was an "interference by a public authority" and whether the case concerned a negative or a positive obligation

37. The Court is not convinced by the Government's submission that there had been no "interference" with the right to respect for the applicant's private life because he had not properly labelled as private the files opened by his superiors. It observes that the Government did not deny that the applicant's files had been opened on his work computer without his knowledge and in his absence. Having regard to the special circumstances of the case, the Court is willing to accept that there was an interference with his right to respect for private life.

38. Nor is the Court convinced by the Government's submission that the SNCF was not a public authority within the meaning of Article 8 § 1 of the Convention. Admittedly, as they observed, the SNCF carries on an "industrial and commercial" activity, its staff are subject to private law, the non-regulatory decisions it takes in their regard are acts subject to private law and employment disputes to which it is a party are tried by the ordinary courts. It is, however, a public-law entity (a "public body of an industrial and commercial nature"), placed under State supervision, and with State-appointed directors, which provides a public service, holds a monopoly and enjoys an implicit State guarantee. In the light of the Court's case-law on the concept of "public authority" (see, in particular, *Kotov v. Russia* [GC], no. 54522/00, § 92-107, 3 April 2012; *Liseytseva and Maslov v. Russia*, nos. 39483/05 and 40527/10, § 183-192, 9 October 2014; and *Samsonov*

v. Russia ((dec.) no. 2880/10, §§ 63-66, 16 September 2014), those factors substantiate the description of the SNCF as a public authority for the purposes of Article 8 of the Convention.

39. The present case must also be compared with the cases of *RENFE v. Spain* (dec.) no. 35216/97, 8 September 1997) and *Copland* (cited above, §§ 43-44). In the former case the European Commission of Human Rights held that the Spanish national railway company was a "governmental organisation" because it was answerable to the government and held a monopoly (without disregarding the differences between the concepts of "governmental organisation" and "public authority", the pattern of analysis used by the Court in these two situations is similar; see, for example, *Kotov*, cited above, § 95). In the latter case the Court held that a measure taken by a State employer against one of its employees could amount to an interference by a public authority with the right to respect for the latter's private and family life (the case concerned the monitoring of correspondence of an employee of a State college by the establishment's authorities).

40. The present case is therefore distinguishable from the case of *Bărbulescu,* cited above (§§ 108-11), in which the right to respect for private life and private correspondence had been infringed by a strictly private-sector employer.

41. Since the interference was by a public authority, the complaint must be analysed from the angle not of the State's positive obligations, as in the case of *Bărbulescu,* cited above, but of its negative obligations.

42. Such interference violates Article 8, unless it is "in accordance with the law", pursues one or more of the legitimate aims referred to in paragraph 2 and is "necessary in a democratic society" to achieve the aim or aims concerned.

b) In accordance with the law

43. The Court observes that it is well established in the case-law that the term "in accordance with the law" implies – and this follows from the object and purpose of Article 8 – that there must be a measure of legal protection in domestic law against arbitrary interferences by public authorities with the rights safeguarded by Article 8 § 1. This expression not only requires compliance with domestic law, but also relates to the quality of that law, requiring it to be compatible with the rule of law. In order to fulfil the requirement of foreseeability, the law must be sufficiently clear in its terms to give individuals an adequate indication as to the circumstances and conditions in which the authorities are empowered to resort to any such measures (see, for example, *Copland*, cited above §§ 45-46).

44. The Government referred to Articles L. 1121-1 and L. 1321-3 of the Labour Code, which merely indicate, however, in general terms, that within a company no one may restrict the rights of persons or individual and

collective liberties in a manner that is neither justified by the nature of the task to be performed nor proportionate to the aim pursued, and that the internal rules laid down by the employer cannot contain provisions restricting the rights of persons or individual and collective liberties in a manner that is neither justified by the nature of the task to be performed nor proportionate to the aim pursued (see paragraph 17 above). The Court observes, however, that the Court of Cassation – examining a complaint under Article 8 – had already held at the material time that, save in a case of serious risk or in exceptional circumstances, an employer could only open files identified by an employee as personal and stored on the hard disk of his or her work computer in the employee's presence or after he or she had been duly called. It had added that folders and files created by an employee using the computer supplied by his or her employer for work purposes were presumed to be professional documents, unless the employee had identified them as personal, and the employer could therefore have access to them in the employee's absence (see paragraph 18 above). The Court concludes that, at the material time, positive law had already allowed the employer, within the said limits, to open files stored on an employee's work computer. It therefore accepts that the interference complained of by the applicant had a legal basis and that positive law contained adequate provisions specifying the circumstances and conditions in which such a measure could validly be regarded as "in accordance with the law".

c) Legitimate aim

45. Whilst an interference with files stored on an employee's computer can have the legitimate aim of "prevent[ing] crime", the Court cannot agree with the Government's assertion that this was the case here. It notes the Government's submission in this regard that the applicant had been suspended from duty at the beginning of 2007 on account of the criminal charge against him and that it was following the discovery of suspicious documents on his computer by the employee temporarily replacing him that the SNCF had carried out more thorough investigations. The Court observes, however, that the opening of the files in question was not done in the context of the criminal proceedings brought against the applicant and that neither the domestic decisions nor the other documents in the case showed that it had been considered at any stage of the domestic proceedings that the contents of the files might constitute a criminal offence.

46. The Court acknowledges, however, that, as also submitted by the Government, the interference was intended to safeguard the protection of the "rights of others", that is to say, in this case, those of the employer, who may legitimately wish to ensure that the employees are using the computer facilities placed at their disposal for the purpose of carrying out their duties in line with their contractual obligations and the applicable regulations. It reiterates in this connection its observation in *Bărbulescu*, cited above

(§ 127), 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.

d) Necessary in a democratic society

47. The notion of necessity implies that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued. Whilst, in ruling on the "necessity" of an interference "in a democratic society", the Court must have regard to the margin of appreciation afforded to the Contracting States, it does not, however, confine itself to ascertaining whether the respondent State exercised its discretion reasonably, carefully and in good faith. In exercising its supervisory jurisdiction, the Court must consider the impugned decisions in the light of the case as a whole and determine whether the reasons adduced to justify the interference at issue are relevant and sufficient. It must also examine whether domestic law and practice afforded adequate and effective safeguards against any abuse and arbitrariness. For that purpose, it refers, *mutatis mutandis* to the recent judgment *Bărbulescu* (cited above, §§ 120-21), in which it held, in the context of the application of Article 8 to the relationship between private employers and their employees, that the domestic courts had to ensure that the introduction by an employer of measures to monitor correspondence and other communications, irrespective of the extent and duration of such measures, was accompanied by adequate and sufficient safeguards against abuse. It stressed, in this context, that proportionality and procedural guarantees against arbitrariness were essential.

48. Having pointed that out, the Court observes that French positive law contains provisions for the protection of private life. The principle is that, whilst the employer can open any professional files stored on the hard disks of the computers placed at the employees' disposal for the purposes of their duties, it cannot surreptitiously open files identified as being personal "save in a case of serious risk or in exceptional circumstances". It can only open such files in the presence of the employee concerned or after the latter has been duly called.

49. The Court observes that the domestic courts applied that principle in the present case. Both the Amiens Court of Appeal (see paragraph 14 above) and the Court of Cassation (see paragraph 16 above) explicitly reiterated it, with the Court of Cassation observing in particular that "files created by the employee with the assistance of the computer facilities supplied to him by his employer for work purposes [were] presumed to be professional in nature, meaning that the employer [was] entitled to open them without the employee being present, unless they [were] identified as personal".

50. Addressing the applicant's submission that there had been a violation of his right to respect for his private life, they held that, in the circumstances of the case, that principle did not preclude his employer from opening the files in question, as these had not been duly identified as private.

51. The Court reiterates at the outset that it is primarily for the national authorities, notably the courts, to resolve problems of interpretation of domestic legislation; save in cases of arbitrary or manifestly unreasonable interpretation (see, for example, *Anheuser-Busch Inc. v. Portugal* [GC], no. 73049/01, § 86, ECHR 2007-I), its role is confined to ascertaining whether the effects of such an interpretation are compatible with the Convention (see, for example, *Waite and Kennedy v. Germany* [GC], no. 26083/94, § 54, ECHR 1999-I, and *Rohlena v. the Czech Republic* [GC], no. 59552/08, § 51, ECHR 2015). It observes next that, in reaching the conclusion summarised above, the Amiens Court of Appeal (see paragraphs 14-15 above) based itself on the finding that the pornographic photographs and videos in question were stored in a file labelled "fun" contained in a hard disk called "D:/personal data", and on the SNCF's explanation that "the 'D' drive [was] called 'D:/data' by default and [was] traditionally used by staff to store their work documents". It went on to consider that an employee could not "use a whole hard disk, which was supposed to record professional data, for private use and that "in any event the generic term "personal data" could have referred to work files being processed personally by the employee and did not therefore explicitly designate elements related to private life". More specifically, the Court of Appeal found that the term "fun" did not clearly confer a necessarily private designation on the file, as the term [could] refer to exchanges between colleagues at work or professional documents kept by the employee as "bloopers". The Court of Appeal had, furthermore, accepted the SNCF's argument that the "user's charter provided that private information should be clearly identified as such ('private' option in the Outlook criteria)", and that the same applied to the "media receiving that information ('private' folder)". It also considered that the measure taken against the applicant – his dismissal from the service – was not disproportionate, given that the applicant had committed a "massive breach" of the SNCF's Code of Professional Conduct and its internal rules, which provided that staff were required to use the computer facilities supplied to them for exclusively professional purposes, with the occasional private use being merely tolerated. According to the Court of Appeal, his actions were particularly serious because, as an official responsible for general surveillance, he would have been expected to be of exemplary conduct.

52. The Court, which observes that the domestic courts thus properly assessed the applicant's allegation of a violation of his right to respect for his private life, finds their decisions to have been based on relevant and

sufficient grounds. Admittedly, in using the word "personal" rather than "private", the applicant used the same word as that found in the Court of Cassation's case-law to the effect that an employer cannot, in principle, open files identified as "personal" by the employee (see paragraph 18 above). However, in terms of the Court's task of assessing the compatibility of the impugned measures with Article 8 of the Convention, that is insufficient to call into question the relevance or adequacy of the grounds on which the domestic courts based their decisions, having regard to the fact that the user's charter for use of the SNCF's information system specifically states that "private data must be clearly identified as such (*inter alia* 'private' option in the Outlook criteria) [and that] the same is true of the media receiving that information ('private' folder)". The Court also accepts that, having noted that the applicant had used a substantial amount of the storage space on his work computer to store the files in question (1,562 files representing a volume of 787 megabytes), the SNCF and the domestic courts deemed it necessary to examine his case thoroughly.

53. Consequently, the Court, observing, moreover, that it is required to consider the impugned decisions in the light of the case in its entirety, considers that the domestic authorities did not exceed their margin of appreciation, and that there has therefore been no violation of Article 8 of the Convention.

II. ALLEGED VIOLATION OF ARTICLE 6 § 1 OF THE CONVENTION

54. The applicant submitted that, in the light of the Court of Cassation's previous case-law, he could not have expected it to conclude in his case that the opening of the files by his employer was compatible with his right to respect for his private life. In his view, by transforming conduct which had hitherto been lawful into wrongful conduct, it had "limited" its established case-law and, applying it retroactively, had "undermined legal certainty and the expectations of defendants". He also submitted that the fact that a former legal director of the SNCF had been an advocate-general at the Court of Cassation since 2000 cast a "real doubt" on the impartiality of that court. He relied on Article 6 § 1 of the Convention, which provides:

> "In the determination of his civil rights and obligations ... everyone is entitled to a fair ... hearing ... by [a] ... tribunal ..."

55. As the Court has already noted (see paragraph 44 above), the Court of Cassation – on examining a complaint under Article 8 – had held prior to the facts of the present case that, save in a case of serious risk or in exceptional circumstances, an employer could only open files identified as personal by the employee and contained in the hard disk of his work computer in the presence of the employee concerned or after the latter had been duly called. It had added, however, that files and folders created by an

employee with the computer facilities supplied by his or her employer for professional use were presumed to be professional in nature unless the employee identified them as personal, which meant that the employer could access them in the employee's absence. Accordingly, at the material time positive law, as then established, allowed the employer, within those limits, to open files stored on an employee's work computer. The Court observes, further, that the complaint that the Court of Cassation's impartiality had been affected by the fact that a former legal director of the SNCF was now an advocate-general is not substantiated as the applicant did not even claim that the advocate-general had sat on the bench examining his appeal.

56. The Court consequently concludes that this part of the application is manifestly ill-founded and accordingly declares it inadmissible and rejects it under Article 35 §§ 3 a) and 4 of the Convention.

FOR THESE REASONS, THE COURT

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

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

Done in French, and notified in writing on 22 February 2018, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

Claudia Westerdiek
Registrar

Angelika Nußberger
President